
CyberPower
2024
SUSTAINABILITY REPORT

Foreword 3
- Message from the Chair 3
- Message from the President 4
- About This Report 5

01 Sustainability Governance 6
- Honors and Recognition 7
- Sustainability Roadmap 9
- Sustainability Governance Framework 12
- Material Topics and Stakeholders 13

02 About Us 19
- About CyberPower 20
- Business Operations 22
- Economic Performance 24
- External Engagement 27

03 Corporate Governance 28
- Governance Structure 29
- Functional Committees 34
- Ethical Management 35
- Legal Compliance 37
- Risk Management 38
- Information Security 40

04 Product Innovation and Service 46
- Innovation and Research 47
- Product Quality 54
- Customer Service 58

05 Supply Chain Management 60
- Sustainable Value Chain 61
- Supplier Risk Assessment 63
- Supplier Evaluation and Audit 64

06 Environmental Protection 65
- Climate Change Adaptation 66
- Climate-related Risks and Opportunities 67
- Greenhouse Gas and Energy Management 74
- Water Resource Management 76
- Waste Management 76
- Energy Saving and Carbon Reduction 77

07 Social Inclusion 80
- Human Resources Overview 81
- Employee Turnover 83
- Employee Rights and Compensation 86
- Talent Attraction and Retention 92
- Safe and Secure Workplace Environment 94
- Workplace Health Services 99
- Social Care for the Common Good 101

Appendix 102
- GRI Sustainability Reporting Standards Index 103
- Sustainability Accounting Standards Board Index 108
- Task Force on Climate-related Financial Disclosures Index 109
- Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies / Other Electronic Industries 110
- Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies / Climate-Related Information of Listed Company 111
- Independent Assurance Statement 112

Message from the Chair

CyberPower was founded in 1997 with a strong commitment to branding in the power management industry. Supported by our global team of experts, we have developed comprehensive capabilities in brand management, encompassing product design, manufacturing, sales, and service. In 2024, we were honored with several international brand and product awards, reflecting widespread recognition of our achievements in brand management. We value our employees, prioritizing their well-being with ongoing care and support to foster a strong sense of belonging. The interdependence between our global team and the culture of our company has contributed to CyberPower's positive impact in the power management field.

Looking back at 2024, despite global economic uncertainties and geopolitical risks, CyberPower remained solid and steady growth. The company achieved consolidated annual revenue of NT$12.492 billion, a gross margin of 50.95%, and earnings per share of NT$24.75. Our performance outpaced that of the prior year, maintaining steady and sustainable growth, which clearly demonstrates the effectiveness of our product portfolio optimization and value creation strategies.

From the very beginning, CyberPower has been mindful of climate change and the energy crisis. While pursuing corporate growth, we also fulfill our social responsibilities and stay aligned with evolving sustainability standards and trends. To further strengthen our corporate social responsibility (CSR) efforts, a Sustainability Task Force was established in early 2022, focusing on five key areas, including Corporate Governance, Environmental Sustainability, Social Contribution, Employee Care, and Responsible Supply Chain. In 2024, we released the first edition of our “Sustainable Development Best Practice Principles”, which serves as an internal framework for embedding CSR principles into our business operations.

In terms of products and research & development, the company continuously integrates green design thinking to enhance product intelligence and energy efficiency. We have adopted circular packaging and digitalized product manuals, effectively reducing resource consumption. At the same time, we actively promote international research & development collaborations and innovation, securing multiple patents that demonstrate the strength and depth of our technological capabilities.

Today, as global companies face multiple challenges including climate impacts, human rights issues, and supply chain responsibilities, CyberPower is proactively addressing these critical international concerns. Through our Sustainability Reports, we respond to stakeholder expectations with greater openness and transparency. Looking ahead, we will continue to strengthen corporate governance, deepen our brand value, and implement climate action with unwavering commitment—advancing toward our vision of becoming a global brand recognized for sustainable value.

Chair Chin Kuo



Message from the President

CyberPower's commitment to "Establish ideal power quality to foster technological advancement and better life" has remained unchanged since the beginning. Through years of diligent efforts, we have solidified our sales and service capabilities, establishing a strong foothold in the global market by leveraging our comprehensive resource structure and rich experience.

The global landscape has become increasingly complex, with economic, trade, and energy challenges, the external environment is filled with substantial uncertainties. As CyberPower continues to expand its market presence since its inception, the company is in the process of establishing a real-time data analysis platform to enhance operational resilience and adaptability. By leveraging data-driven insights, we can swiftly respond to market fluctuations, optimize strategies, and drive sustainable growth and profitability.

In terms of operations, CyberPower remains firmly committed to its core values of in-depth research & development and in-house manufacturing. Our products are developed with a focus on user experience and market orientation. In addition to providing standardized solutions, we offer customized services tailored to the specific needs of various industries and application scenarios. In 2024, we were once again recognized by CRN Magazine in the US as one of the Top 100 Edge Computing companies, reaffirming that we deliver not just products, but comprehensive and integrated power solutions.

In response to climate challenges, CyberPower conducts organizational greenhouse gas (GHG) inventory and verification in accordance with ISO 14064-1. In 2024, we expanded our inventory boundaries beyond Taiwan to include our major production sites in China and the Philippines. By adopting the framework of the Task Force on Climate-related Financial Disclosures (TCFD), we have enhanced our assessment of both transition and physical risks and are progressively implementing emission reduction measures to strengthen our resilience and adaptive capacity in the face of climate change. To further improve the quality and relevance of our sustainability disclosures, we have also adopted the industry-specific disclosure standards published by the Sustainability Accounting Standards Board (SASB). This approach enables us to focus on key material issues within our sector, enhancing both the transparency and consistency of our reporting to meet the expectations of international investors.

CyberPower has long been committed to developing energy-saving and intelligent power management technologies. We have integrated our patented GreenPower UPS™ technology along with a Building Management System (BMS) to help users effectively reduce energy consumption and carbon emissions. This system monitors building temperature and humidity and automatically adjusts air conditioning settings, making it widely applicable across corporate and consumer environments. This reflects our dedication to balancing product functionality with environmental responsibility. Looking ahead, we will continue to advance energy-saving initiatives and embed sustainability strategies into our daily operations, further strengthening our overall competitiveness in the global power management market.

President Michael Ho



About This Report

Report Overview

Cyber Power Systems, Inc. (hereafter referred to as CyberPower) publishes its Sustainability Report annually, aiming to continuously disclose not only its financial performance but also the achievements in environmental, social, and governance (ESG) operations, actively working toward its vision of sustainable business practices. This report was published in August 2025, with the next report expected in August 2026.

Reporting Scope

This report covers the period from January 1, 2024, to December 31, 2024, and will be issued annually. The scope of this report is primarily focused on the Taiwan headquarters (Taipei) and Tainan facility of CyberPower, excluding overseas subsidiaries and investment companies. Any information related to non-Taiwan regions will be noted in the report. The financial figures disclosed in this report are sourced from CyberPower's consolidated financial statements for 2024. For more detailed information regarding affiliated companies, please refer to CyberPower's Official Website for the "2024 CyberPower Annual Report." There have been no significant changes in the organization's size, structure, ownership, or supply chain during the reporting period.

Compilation Guidelines

This report is prepared in accordance with the Global Reporting Initiative (GRI) Sustainability Reporting Standards, with the General Standards adopting the 2021 version. Each Topic Standard applies the version corresponding to its year of publication, and the GRI Content Index is provided in the appendix.
The report also references the recommendations of the Financial Stability Board's (FSB) Task Force on Climate-related Financial Disclosures (TCFD), as well as the industry disclosure standards published by the Sustainability Accounting Standards Board (SASB).
In addition, the company complies with the requirements set forth in the Taiwan Stock Exchange (TWSE) "Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies", disclosing information in accordance with Appendix 1-14 "Sustainability Disclosure Indicators for the Other Electronics Industries" and Appendix 2 "Climate-related Information of Listed Companies."

Main Responsible Team and Quality Management Method

CyberPower has established the "Sustainable Development Best Practice Principles" in accordance with the "Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies" to regulate the internal procedures for preparing and verifying the company's Sustainability Report. The company plans to incorporate these procedures into its "Internal Control System" next year as part of the annual audit program. All related procedures are submitted to the Board of Directors for review and approval to ensure the adequacy of the system.

Procedures	Methods	Responsible Team
Compilation Planning	This report is coordinated and planned by the Sustainability Task Force. The relevant responsible departments provide the data, strategic objectives, and performance indicators disclosed in the report. The Sustainability Task Force is responsible for the final integration, compilation, and proofreading of the content.	Sustainability Task Force and Relevant Responsible Departments
Internal Review	The finalized report is reviewed by the relevant responsible departments to ensure the completeness and accuracy of its content, and is then approved by the highest executive of each respective department.	Relevant Responsible Departments and Their Highest Executive
External Review	The report is verified by an independent third-party assurance provider in accordance with the AA1000 Assurance Standard (v3), Type 1 moderate level of assurance, to ensure that its content complies with the GRI Sustainability Reporting Standards, the Sustainability Accounting Standards Board (SASB) disclosure standards, and the AA1000 AccountAbility Principles 2018.	AFNOR Asia
	The greenhouse gas (GHG) emissions have been verified by an independent third-party verification body in accordance with the ISO 14064-3:2019.	
	The financial data have been audited and certified by a certified public accounting firm in accordance with the International Financial Reporting Standards (IFRS).	Deloitte & Touche
Final Approval	The finalized report is submitted by the Financial Department to the Board of Directors and will be publicly released only after review and approval by the Board.	Financial Department and Board of Directors

Contact Information

If you have any suggestions or questions regarding this report or CyberPower's sustainability initiatives, you are welcome to contact us. Sustainability information is also available on the CyberPower Sustainability Website https:esg.cyberpower.com/en

Sustainability Task Force
Address: 11F., No.26, Jinzhuang Rd., Neihu Dist., Taipei City 114, Taiwan
Mail: esg@cyberpower.com
Phone: +886-2-8792-9510



01 Sustainability Governance

Honors and Recognition
Sustainability Roadmap
Sustainability Governance Framework
Material Topics and Stakeholders

Honors and Recognition



2022

- USA: CRN Channel Partner Alliance Program Recognition
- USA: CRN Products of the Year – 3-Phase Modular UPS Systems
- USA: CRN Tech Innovator Awards Finalist – PFC Sinewave Rackmount UPS Systems
- USA: Guiding Tech The Best UPS System for Computers
- Taiwan: Top 40 Best Taiwan Global Brands
- Taiwan: Taiwan Excellence Award - Smart App Online (High-Density) UPS

2023

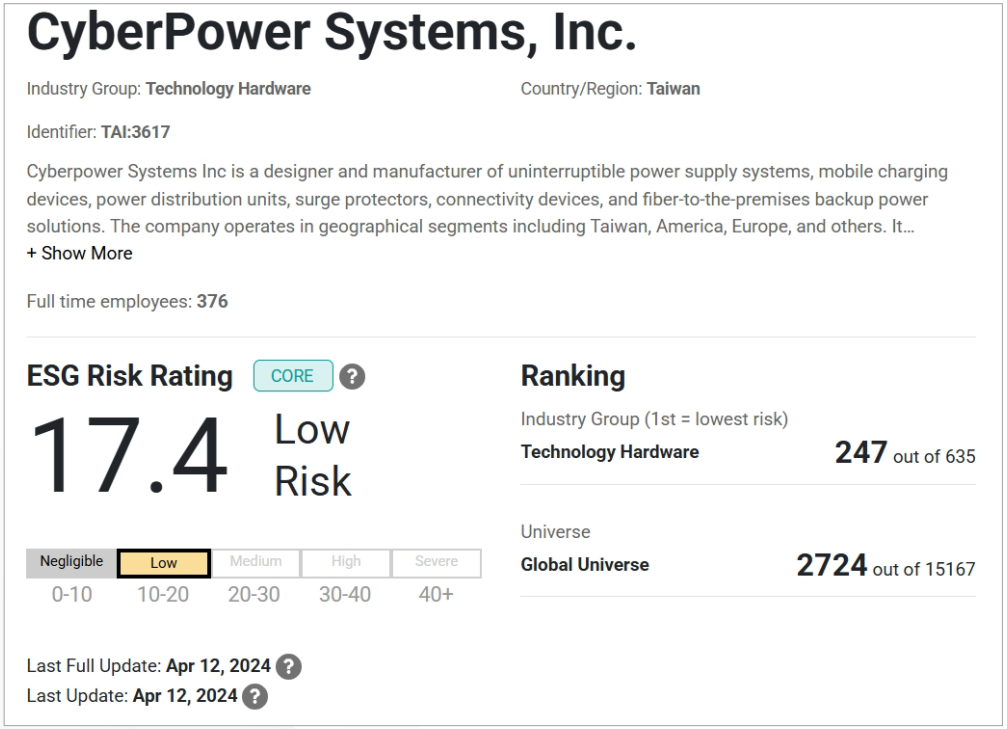
- USA: CRN Channel Partner Alliance Program Recognition
- USA: CRN Edge Computing 100 List
- USA: ChannelPro-SMB Readers' Choice Awards for Best UPS & Power Conditioning Vendor Silver Winner
- Japan: BCN Award Top 3 UPS Brand at Retail Channels
- Taiwan: Top 40 Best Taiwan Global Brands

2024

- Rated "Low Risk" in Sustainalytics' ESG Risk Ratings
- USA: CRN Channel Partner Alliance Program Recognition
- USA: CRN Edge Computing 100 List
- USA: CRN Products of the Year – PFC Sinewave 1U Rackmount UPS Systems
- USA: CRN Tech Innovator Awards Finalist –Smart App Sinewave Lithium UPS Series
- Japan: BCN Award Top 3 UPS Brand at Retail Channels
- Taiwan: Top 40 Best Taiwan Global Brands

Rated "Low Risk" in Sustainalytics' ESG Risk Ratings

Sustainalytics, a globally recognized agency specializing in environmental, social and governance (ESG) risk ratings, classified CyberPower as "Low Risk" in its latest evaluation released in April 2024. CyberPower received a score of 17.4, indicating its effective governance and risk control across ESG dimensions.



(Source: Sustainalytics)

CyberPower honored in CRN's 2024 Edge Computing 100 and PARTNER PROGRAM GUIDE

CRN®, a publication under The Channel Company in the United States, continues to deliver high-quality technology news and insights to solution providers, IT channel partners and value-added resellers.

CyberPower was recognized in CRN's 2024 Edge Computing 100 list for its continued innovation in power management solutions that meet the demands of edge computing. The company distinguished itself in the edge hardware category.

In addition, CyberPower continues to enhance resource allocation and support through its Channel Partner Alliance program, which has been established in the U.S. for eight years. The program has earned widespread market recognition for fostering long-term, trusted relationships with partners. As a result, it received a five-star rating in CRN's 2024 Partner Program Guide.

Honored with a spot among Taiwan's Top 40 International Brands in 2024

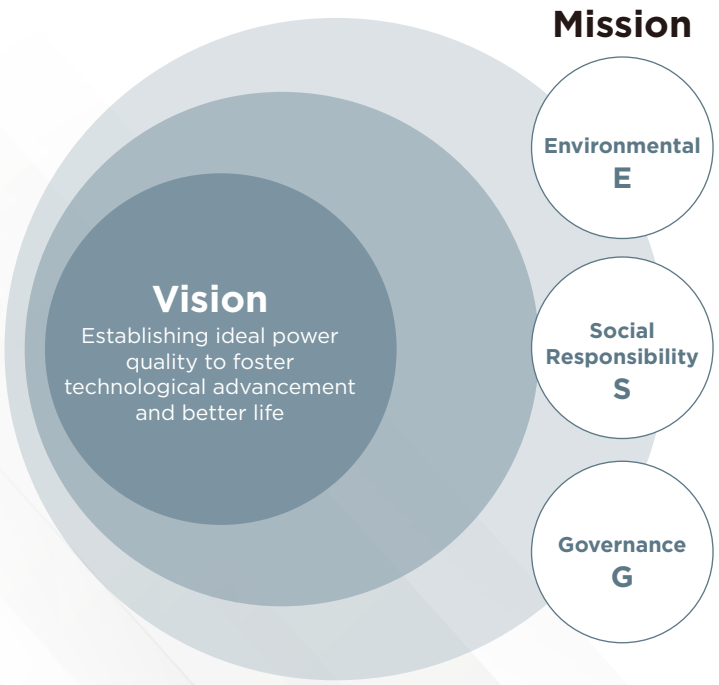
The Taiwan Top International Brands program is organized by the Taiwan Institute of Economic Research and conducted in partnership with Interbrand, a globally recognized authority in brand valuation. The annual evaluation adopts the same methodology as Interbrand's Global Top 100 rankings, combining financial performance metrics with qualitative analysis of brand management. CyberPower has received this honor for five consecutive years, reflecting the company's strong performance and recognition in brand development.

Sustainability Roadmap

Sustainability Vision and Mission

CyberPower was founded on the mission of "establishing ideal power quality to foster technological advancement and better life." Guided by its commitment to environmental responsibility— "making the greatest possible contribution to the environment", the company actively promotes sustainable business practices. With more than 25 years of experience in product development and manufacturing, CyberPower not only meets global market demands but also applies its technical expertise to social impact and environmental improvement, achieving sustainability with professional excellence.

In response to global sustainability trends and the challenges of climate change, CyberPower has established three core pillars for its sustainability blueprint: green economy, climate action, and ethical management. The company is dedicated to helping users reduce energy costs while supporting environmental protection and social welfare. By integrating its core strengths with global sustainability efforts, CyberPower continues to advance toward smart energy efficiency, low-carbon transformation, and shared value creation—contributing to a resilient society and a sustainable future.



Environmentally Friendly, Driving the Green Economy

CyberPower promotes low-carbon product development through technological innovation, such us its proprietary GreenPower UPS™ technology. The company has long participated in the ENERGY STAR® program, striving to improve energy efficiency and reduce the carbon footprint of its products. By helping users conserve energy and cut emissions, CyberPower delivers both performance and environmental benefits.

Aligning with Global Standards and Responding to Climate Action

CyberPower prioritizes occupational health and safety, enhances employee training and wellness programs, and actively engage in community service and environmental education. By formulating environmental policies and implementing energy management systems, we proactively respond to international climate initiatives. We also deepen communication with stakeholders to jointly create sustainable value.

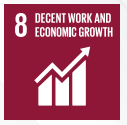
Upholding Ethical Management to Build a Sustainable Foundation

CyberPower upholds the principles of honesty and integrity, ensuring full compliance with regulations and sound internal governance. By establishing management systems and operational processes rooted in sustainability, we strengthen risk control and build a resilient foundation for long-term growth. Sustainable governance is integrated into our daily operations and embedded throughout the company's practices.

Commitment to the United Nations Sustainable Development Goals (SDGs)

In response to the SDG Impact Standards for Enterprises developed by the United Nations Development Programme (UNDP), CyberPower has established strategies and policies since 2023 aligned with the Sustainable Development Goals (SDGs). Led by the Sustainability Task Force, the company promotes cross-functional collaboration and focuses on five key areas to advance diverse sustainability initiatives. CyberPower is dedicated to creating a positive impact on both society and the environment through responsible business practices.

In 2024, CyberPower is committed to supporting 10 Sustainable Development Goals (SDGs) and implementing 35 related initiatives. These initiatives cover three key areas of sustainability: environmental, social and governance (ESG).

Sustainable Development Goals	SDGs Action Initiative
 SDG 3 GOOD HEALTH AND WELL-BEING	• Responded to the blood donation campaign hosted by Taipei Neihu Technology Park Development Association, rallying employees and neighbors to collect 225 bags of blood for the Taipei Blood Center (TBSF) • Subsidized employee health check-ups and continued follow-ups, with 331 participants and an investment of NT$ 2,640,800 • Organized 5 health seminars, with a total participation of 255 individuals
 SDG 4 QUALITY EDUCATION	• Organized one workplace experience activity for employees' children, helping 11 students discover and develop their suitable career paths • As of 2024, CyberPower has released 9 educational videos and 21 blog articles to help users better understand power fundamentals, making backup power planning and implementation more accessible • Employees have access to the HyRead e-library, which offers more than 110,000 e-books for borrowing • The company invested NT$148,085 in external training for all employees, totaling 380.5 hours
 SDG 5 GENDER EQUALITY	• The proportion of female executives has reached 31.25% of all managerial positions, achieving gender diversity at the senior leadership level
 SDG 7 AFFORDABLE AND CLEAN ENERGY	• Solar power generation reached 3,736.8 kWh in Taiwan and 1,860 kWh in China, reflecting continued expansion of clean energy use • Solar panel replacement at the Taipei headquarters was completed, with an installed capacity of 25.81 kWp, improving efficiency by 156.05% compared to the previous model • In support of Earth Hour, organized by the World Wide Fund for Nature (WWF), the company joined other businesses across Taiwan to save approximately 289,000 kWh of electricity—equivalent to the carbon reduction of planting about 13,005 20-year-old trees
 SDG 8 DECENT WORK AND ECONOMIC GROWTH	• Net sales totaled NT$12,492,000 thousand, marking a 6.49% increase from the previous year • Earnings per share (EPS) reached NT$24.75, up 49.28% year over year • Annual employee welfare expenditure reached NT$12,384,353, a growth of 5.09% compared to the previous year • No occupational accidents occurred, maintaining a safe and friendly work environment • Continued promotion of local sourcing, with the proportion of local procurement in China (Cyber Power (Shenzhen) Ltd) reaching 96.42%, a 13.93% increase from the previous year

Sustainable Development Goals	SDGs Action Initiative
 SDG 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE	• Recognized by CRN Magazine in the US as one of the Top 100 Edge Computing Companies of the Year • Secured five new patents, bringing the total number of patents to 304 • Invested NT$395,626 thousand in individual research and development
 SDG 12 RESPONSIBLE CONSUMPTION AND PRODUCTION	• The UPS System (CST135UC2) replaced polystyrene with 100% recyclable molded pulp. Based on 2024 shipment volumes, this change is expected to reduce polystyrene usage by 9,187.2 kilograms annually • The Universal Power Supply (CPUAC1U1300) adopted paper packaging in place of plastic, with an estimated annual reduction of 3,157.38 kilograms of plastic based on 2024 shipment volumes • The Intelligent Management Solution (Including network management cards and sensors) replaced blister packs and cushioning materials with 100% recyclable molded pulp, reducing plastic use by an estimated 522.92 kilograms, based on 2024 shipment volume • No violations of health and safety regulations or voluntary standards occurred, and there were no incidents of hazardous substance exceedance • No violations related to product and service information and labeling occurred • All hazardous industrial waste was handled by fully compliant contractors
 SDG 13 CLIMATE ACTION	• Completed ISO 14064-1 Greenhouse Gas Inventory and Verification for major production sites in China and the Philippines • Completed ISO 14067 Product Carbon Footprint and Verification for the Smart APP Online (High Density UPS) series • Adopted the Task Force on Climate-related Financial Disclosures (TCFD) framework to effectively manage climate risks and enhance corporate climate resilience • Implemented the Sustainability Accounting Standards Board (SASB) standards to improve disclosure transparency and industry relevance • Participated in the EcoVadis Sustainability Assessment to track performance across four key sustainability themes • Joined the Carbon Disclosure Project (CDP) to advance climate strategy and management • Among the company's ENERGY STAR-certified uninterruptible power systems, 99% of products exceeded the certification standards
 SDG 16 PEACE, JUSTICE AND STRONG INSTITUTIONS	• No employees were dismissed due to corruption, demonstrating the company's commitment to ethical business practices • No major cybersecurity incidents occurred, reflecting effective implementation of information security measures and risk management
 SDG 17 PARTNERSHIPS FOR THE GOALS	• Organized company tours to strengthen partnerships across Asia, Europe, the Middle East, and the Australia–New Zealand regions

Sustainability Governance Framework

To strengthen sustainability development management and establish a robust governance framework, CyberPower adopted its own "Sustainable Development Best Practice Principles" in early 2022, in accordance with the "Sustainable Development Best Practice Principles for TWSE/TPEx Listed Companies." The Global Brand Marketing Division was tasked with forming a Sustainability Task Force, composed of dedicated personnel, responsible for planning, evaluating, and executing sustainability initiatives. The company's efforts focus on five key areas: Corporate Governance, Employee Care, Environmental Sustainability, Responsible Supply Chain, and Social Contribution.

The Sustainability Task Force, in accordance with the "Sustainable Development Roadmap for TWSE/TPEx Listed Companies," formulates short-term, mid-term, and long-term goals, completes sustainability planning within the statutory timeline, and reports at least once a year to the Board of Directors on the establishment and operation of the sustainability plan. The progress of greenhouse gas (GHG) inventory and verification is reported quarterly to the Board, while the results of the Sustainability Report preparation are presented annually.

The Board of Directors regularly monitors the implementation and results of sustainability projects. When necessary, it urges the Sustainability Task Force to make adjustments to ensure that sustainability strategies and measures are fully integrated into daily operations, thereby achieving corporate governance and sustainable development goals.

In 2024, CyberPower published its second Sustainability Report, further enhance information transparency. To strengthen climate action management, the company has progressively expanded the boundaries of its GHG inventory. In addition to operations in Taiwan, certain subsidiaries in China and the Philippines obtained ISO 14064-1 certification, and selected product lines completed ISO 14067 certification, demonstrating CyberPower's commitment to sustainable development through concrete actions.
CyberPower regards sustainability as one of its core strategies and works closely with stakeholders to build a sustainable future. The company regularly discloses its progress and shares outcomes through its Sustainability Website, highlighting proactive efforts across five key areas.

Key Sustainability Matters Reported by CyberPower to the Board of Directors

Corporate Governance
- Completed the 2023 GHG inventory for CyberPower's standalone entity and obtained third-party verification statements.
- Established preparatory procedures and timelines for the 2024 GHG inventory in China and the Philippines.
- Participated in the Carbon Disclosure Project (CDP) by completing the Climate Change and Water Security questionnaires.

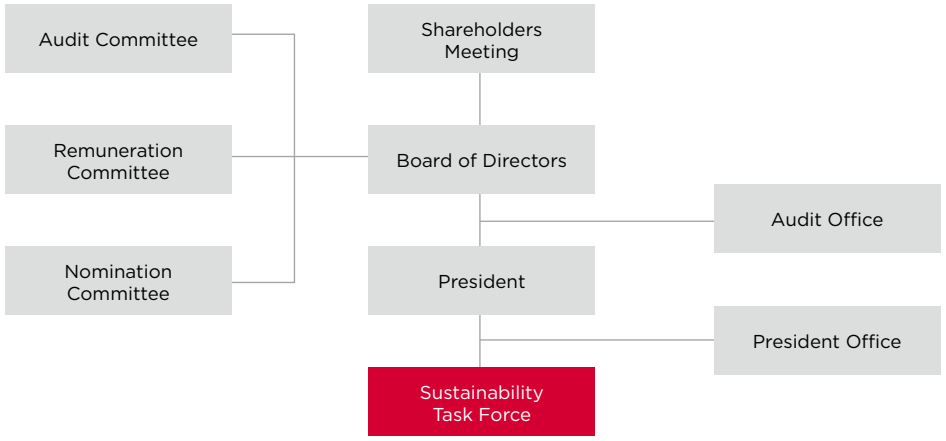
Employee Care
- Organized workplace experience activity for employees' children, leveraging company resources to support career exploration.
- Hosted a Michelin Star Dining Experience to encourage employees and their families to enjoy fine dining experiences together.

Environmental Sustainability
- Responded to the World Wide Fund for Nature (WWF) Earth Hour lights-off campaign.
- Independently developed a Building Management System (BMS) to automate control of air conditioning systems.

Sustainable Supply Chain
- Completed the EcoVadis Sustainability Assessment, covering four key themes.
- Held company tours to strengthen brand and product knowledge among partners in Asia, Europe, the Middle East, and Oceania, deepening mutual partnerships.

Social Contribution
- Supported post-earthquake economic recovery by purchasing local gift boxes from Hualien for employee enjoyment.
- Organized two blood donation activities, joining forces with employees and local communities to contribute to social welfare.

Sustainability Governance Structure



Material Topics and Stakeholders

Materiality Assessment Process

CyberPower follows the GRI Sustainability Reporting Standards 2021 and adopts GRI 3: Material Topics 2021 as the core framework for identifying and managing material topics. Additionally, the company references the AA1000 AccountAbility Principles 2018, applying the four key principles of Inclusivity, Materiality, Responsiveness, and Impact to guide the identification and communication of material issues.
In line with these standards, CyberPower discloses the impacts, management approaches, and practices related to each material topic. These results serve as a foundation for aligning the company's sustainability goals and strategies, while enhancing transparency and the effectiveness of communication with stakeholders.

1	2	3	4	5	6
Collection of Sustainability Issues	Stakeholder Engagement	Evaluation of Operational Impacts	Identification of Material Topics	Assessment of Material Topics	Determination of Material Topics
In response to national policies and sustainability initiatives, the materiality analysis process begins with an evaluation of the company's operations, value chain, ESG rating requirements, and industry trends to identify potential economic, environmental, and social impacts. The process also considers the foundation of interaction between the stakeholders and the company, incorporating input from various departments into the identification of sustainability topics.	Following the five principles of the Stakeholder Engagement Standard 2015 (SES)—Dependency, Responsibility, Tension, Influence, and Diverse Perspectives—key stakeholder groups are identified and prioritized.	A materiality workshop was held to align stakeholder concerns and expectations, resulting in the identification of 22 sustainability topics.	A "Sustainability Impact Assessment Questionnaire" was conducted with senior management to evaluate the actual and potential positive and negative impacts of each sustainability topic, including the likelihood of occurrence, impact scale and scope, and risks of human rights violations. At the same time, a "Sustainability Concern Questionnaire" was distributed to key stakeholders to assess their level of concern for each topic.	Internal repeated reviews and validations were conducted to ensure the appropriateness of the identified material topics and threshold criteria, guaranteeing that no significant topics are omitted or insufficiently addressed. This process enhances the completeness, inclusiveness, and comprehensiveness of the material topics, while confirming strong alignment with the company's sustainability strategy.	A total of 9 material topics were identified for 2024. This report fully discloses the impacts of each material topic and presents corresponding policies, commitments, management approaches, performance indicators, and targets.

Stakeholder Engagement

Based on the five principles of the AA1000 Stakeholder Engagement Standard 2015 (SES), CyberPower conducted a comprehensive assessment of stakeholders based on Dependency, Responsibility, Tension, Influence, and Diverse Perspectives. Six key stakeholder groups were identified: (1) Employees, (2) Shareholders / Investors, (3) Government Agencies, (4) Customers, (5) Suppliers, and (6) Communities / Non-profit Organizations. To fully understand stakeholder priorities and the actual or potential impacts on them, the company maintains diverse and two-way communication channels to actively collect and respond to stakeholder concerns on sustainability topics.
During the topic identification process, besides adhering to national policies and the company's operational strategy, relevant frameworks and standards were integrated, including the Task Force on Climate-related Financial Disclosures (TCFD), Carbon Disclosure Project (CDP), United Nations Sustainable Development Goals (SDGs), United Nations Global Compact (UNGC), and the Responsible Business Alliance (RBA) Code of Conduct. Focusing on economic, environmental, and social dimensions, 22 sustainability topics closely related to company operations were consolidated. These topics were discussed and analyzed according to industry trends, value chain characteristics, and corporate development strategies, assessing their actual impacts on economy, environment, society, and human rights. This process supported the identification and prioritization of the company's annual material topics, helping stakeholders better understand and evaluate the company's sustainability performance.
To facilitate effective communication with a broad range of stakeholders through the Sustainability Report, the company has established a Stakeholder Section on its Official Website and provides a dedicated contact email at esg@cyberpower.com. Stakeholders are encouraged to submit inquiries, suggestions, or complaints regarding material topics or report content, ensuring open and smooth communication channels and positive interaction.

Stakeholder Engagement Overview

Stakeholders	The Significance of Stakeholders to CyberPower	Topics Concerned	Major Communication Channels and Frequency		
			Standing	Regular	Ad hoc
Employees	A core driver of business growth and sustainability culture	• Economic Performance • Innovation and Research • Ethical Management • Information Security • Talent Development • Human Rights Policy	• Internal Communication Platform • Employee Feedback Box: fairdeals@cyberpower.com	• Employee Welfare Committee Meeting (biweekly) • Labor-Management Meeting (quarterly) • Occupational Safety and Health Committee Meeting (quarterly) • Performance and Development Review (annual) • Employee Health Check-up and Medical Consultation (annual) • Sustainability Report (annual)	• Department Meeting • Employee Training • New Employee Training • New Employee Forum • Events and Seminars • Electronic Announcements • Sustainability Concern Questionnaire
Shareholders / Investors	A source of financial support focused on profitability and governance transparency	• Economic Performance • Innovation and Research • Ethical Management	• CyberPower Official Website (Investor) • Shareholder and Investor Feedback Box: investor@cyberpower.com	• Investor Newsletter (monthly) • Market Observation Post System (MOPS) (monthly) • Financial Statement (quarterly) • Annual Report (annual) • Sustainability Report (annual)	• Sustainability Concern Questionnaire
Government Agencies	Regulators and policymakers influencing corporate compliance and sustainability strategy	• Economic Performance • Product Quality • Supply Chain Management • Information Security • Climate Change Adaptation	• CyberPower Official Website • CyberPower Sustainability Website	• Market Observation Post System (MOPS) (monthly) • Financial Statement (quarterly) • Corporate Governance Evaluation System(annual) • Regulatory Supervision and Audit by Authorities (annual) • Annual Report (annual) • Sustainability Report (annual)	• Official Document • Sustainability Concern Questionnaire
Customers	Driver of product and service innovation; source of revenue and market trust	• Ethical Management • Economic Performance • Product Quality • Supply Chain Management • Information Security • Climate Change Adaptation	• CyberPower Official Website (CyberPower Worldwide) • CyberPower Sustainability Website • Online Service Platform • Customer Service Hotline • Customer Service Email	-	• Business Review Meetings and Client Visits • Customer Audits and Requirement Requests • Customer Satisfaction Survey • Project Meetings and Technical Workshops with Clients • Sustainability Concern Questionnaire
Suppliers	Influencer of product quality and delivery timelines; key to value chain stability	• Ethical Management • Product Quality • Economic Performance • Information Security	• CyberPower Official Website • CyberPower Sustainability Website • Supply Chain Management Platform	• Supplier Evaluation (annual) • Supplier Audit (annual) • Documented / On-site Audit (annual) • Conflict Mineral Investigation (annual)	• Partner Meetings • EHS and Corporate Social Responsibility (CSR) Management Briefing • Update of “Management Regulations of Hazardous Substances” • Signing of “Quality Statement” • Signing of Integrity Clause in the “Procurement Agreement” • Sustainability Concern Questionnaire Survey
Community / Non-profit Organizations	Enhancer of local engagement and public image; promoter of social impact	• Waste Management • Social Engagement	• CyberPower Official Website • CyberPower Sustainability Website	-	• Public Welfare and Charity Activities • Volunteer Services • Social Media • Sustainability Concern Questionnaire

Materiality Assessment Results

Following stakeholder engagement, CyberPower promptly conducted a systematic assessment of operational impacts, leading to the identification, review, and confirmation of material topics. The Company utilized the "Sustainability Impact Assessment Questionnaire" and the "Sustainability Concern Questionnaire" to implement a standardized and quantifiable evaluation process. Based on the scoring results, material sustainability topics to be disclosed in this report were prioritized and selected accordingly.

After a comprehensive evaluation and review, a total of nine material topics were confirmed for 2024, including one environmental topic, two social topics, and six economic topics. The Sustainability Task Force convened relevant departments to jointly review the assessment process and the appropriateness of the evaluation criteria. Upon ensuring there were no omissions, the results served as the basis for compiling the content of this Sustainability Report.

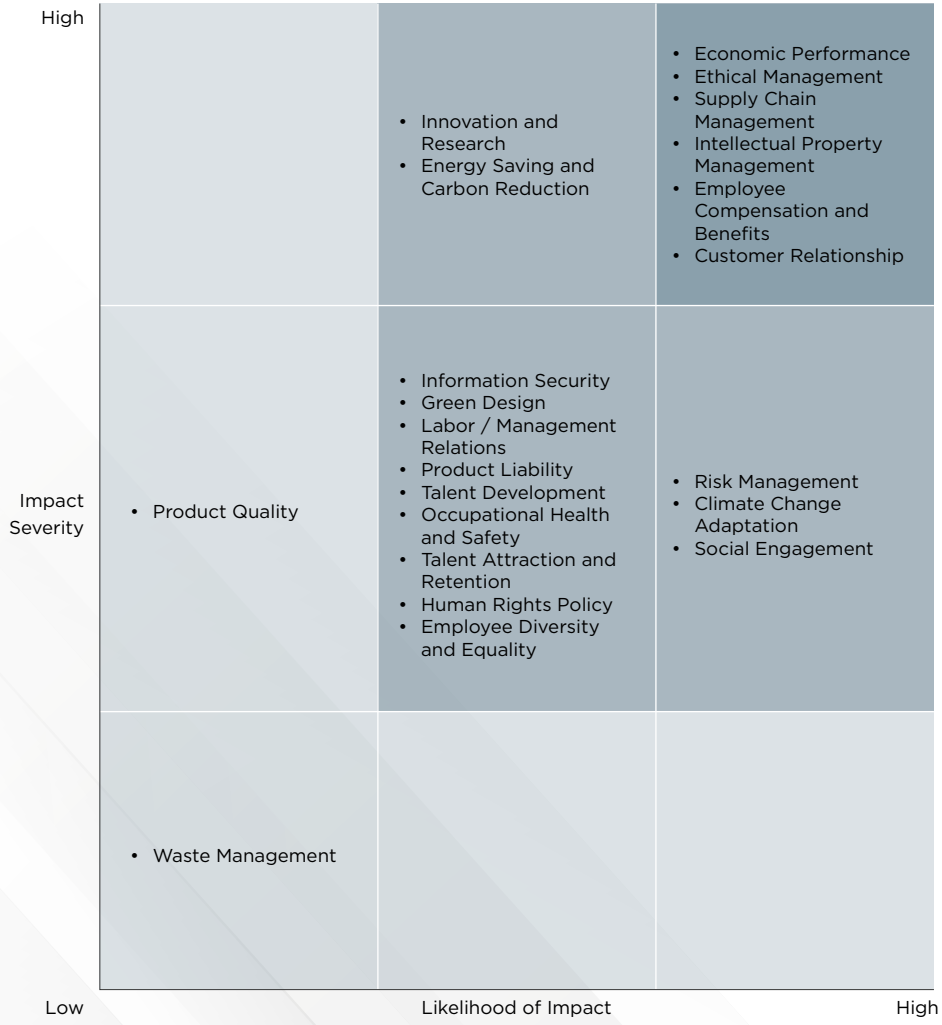
List of Material Topics

Material Topics	Positive Actual / Potential Impact	Negative Actual / Potential Impact	Risk Management	Value Chain Impact			Corresponding Section
				Upstream	CyberPower	Downstream	
Economic Performance	• Stable economic performance reflects market competitiveness, enhances corporate credibility, and supports overall operational growth • Consistently strong financial performance helps attract investors, retain key talent, and expand positive impacts on society and the environment	• Weak financial structure or poor performance may undermine the company's competitive advantage and market trust, thereby affecting its financing capabilities and supply chain stability • Prolonged financial pressure may lead to reduced resources for R&D and sustainability, negatively impacting commitments to stakeholders and social responsibility	Adopting prudent operational strategy, balance operational performance and employee well-being, and support long-term business stability. Maintaining a solid financial system in compliance with regulations, ensuring transparent financial reporting, strengthening governance, and delivering long-term value to shareholders	●	●	●	02 About Us
Innovation and Research	• Continuous investment in innovative R&D and patent strategies enhances product value and strengthens brand competitiveness • Creation of customer value through green design and smart feature innovations responds to the global emphasis on energy efficiency and carbon management	• Lack of stable R&D investment or failure to capture market trends may slow product innovation and reduce market acceptance, leading to a decline in competitiveness • Ineffective commercialization of R&D outcomes or insufficient patent protection may undermine R&D investment returns and increase the risk of counterfeiting	Advancing cross-border R&D projects and product development mechanisms with a focus on user experience and market orientation. Investing in green design and digital solutions, such as energy-saving and smart power management technologies, to help users reduce energy consumption and drive innovation and sustainable value creation	●	●	●	04 Product Innovation and Service
Product Quality	• Adherence to high quality standards supports brand reputation, increases customer satisfaction and repurchase intention, and strengthens long-term customer relationships • Comprehensive quality management reduces risks of returns, repairs, and claims, improves operational efficiency, and enhances supply chain stability and collaboration	• Inadequate quality control may result in product defects, customer complaints, or regulatory violations, leading to compensation claims and reputational damage • Long-term quality instability may weaken customer trust and market competitiveness, affecting revenue and expansion into international markets	Implementing strict quality management systems, supported by UL-certified safety labs and EMC testing facilities. Conducting safety and stability testing during product development. Ensuring end-to-end quality control based on international standards and local regulations to meet global compliance and customer requirements, while maintaining consistently high product quality	●	●	●	04 Product Innovation and Service
Ethical Management	• Establishment of a high-standard integrity and governance culture enhances organizational transparency, reduces compliance risks, and increases willingness to collaborate among investors and customers • Implementation and communication of anti-corruption policies and internal control systems help prevent fraudulent behavior, protect employee rights, and safeguard corporate reputation	• Insufficient integrity management systems and communication mechanisms may lead to misconduct such as fraud or bribery, resulting in legal actions, fines, and reputational damage • Lack of stakeholder trust may undermine the company's sustainable competitiveness in the supply chain and capital markets	Adhering to principles of integrity and corporate governance by establishing business ethics guidelines and anti-corruption internal controls, fully implementing a zero-tolerance policy on corruption. Strengthening internal audits and stakeholder conduct training, enforcing supplier management through quality and business ethics declarations, preventing misconduct, and safeguarding corporate reputation and trust		●		03 Corporate Governance

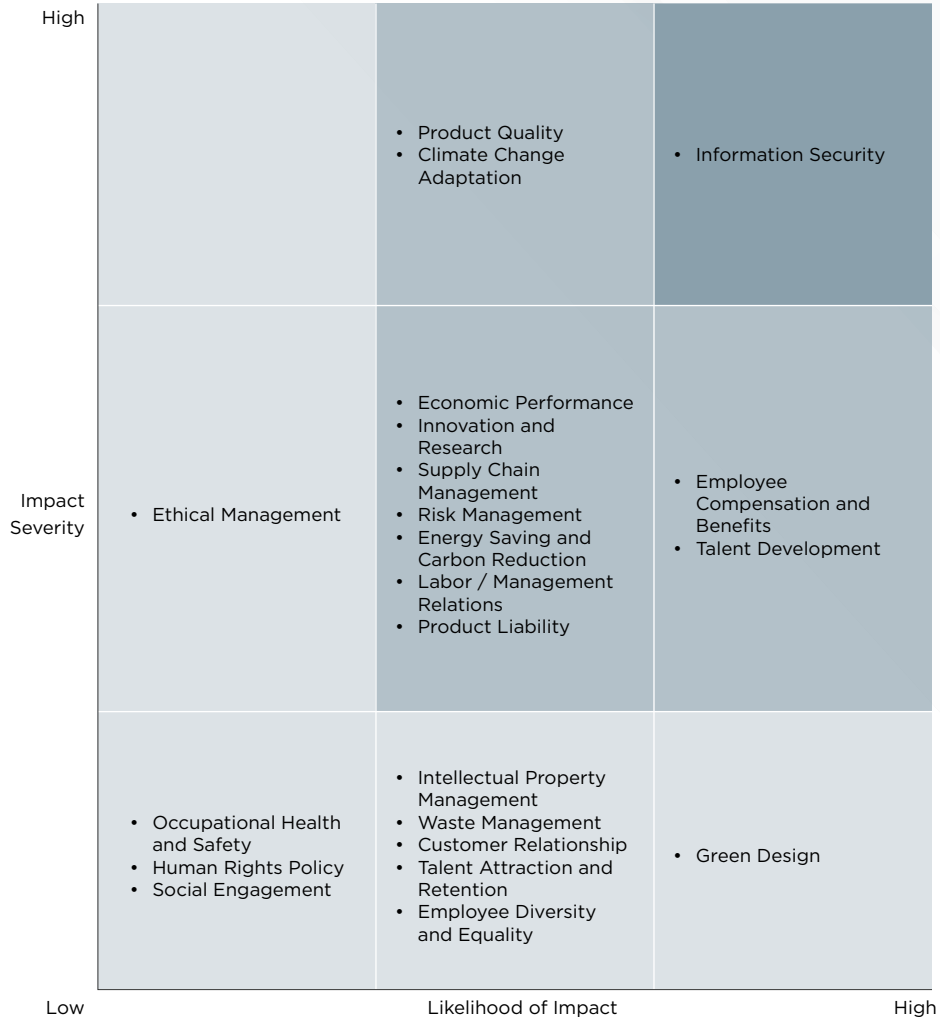
Material Topics	Positive Actual / Potential Impact	Negative Actual / Potential Impact	Risk Management	Value Chain Impact			Corresponding Section
				Upstream	CyberPower	Downstream	
Supply Chain Management	• Implementation of supplier management and audit systems supports raw material quality and delivery stability while reducing operational risks • Practice of responsible supply chain management strengthens corporate social image, addresses sustainability requirements from global brands and customers, and enhances competitive advantage	• Failure to properly manage supplier conduct and compliance risks may result in regulatory violations, environmental pollution, or issues related to conflict minerals, leading to reputational damage, customer contract termination, or legal penalties • Supply chain disruptions or shortages of critical materials may directly impact production stability and delivery performance, resulting in operational losses	Implementing responsible supply chain principles by establishing supplier management policies, conducting annual evaluations and ad-hoc audits, focusing on compliance and promoting supplier conflict minerals investigations. Enhancing overall supply chain sustainability awareness and management capabilities through on-site guidance, achieving a collaborative model of mutual growth across the value chain	●	●	●	05 Supply Chain Management
Information Security	• Establishment of a robust information security management system helps protect customer and corporate data, while reducing risks of operational disruption and regulatory non-compliance • Regular drills and system upgrades strengthen information security resilience, supporting digital transformation and innovative applications in smart manufacturing	• Insufficient identification and management of information security risks may result in customer data breaches, system outages, operational losses, significant reputational damage, and potential fines or legal liabilities • Lack of proper incident reporting and response mechanisms may further erode stakeholder trust in the company	Establishing information security management systems covering confidential data control, personal data protection, and information security incident response. Conducting regular security drills and system recovery tests to ensure data integrity and business continuity. Continuously enhancing the level of protection to safeguard customer privacy and operational security	●	●	●	03 Corporate Governance
Climate Change Adaptation	• Enhancing energy efficiency, reducing greenhouse gas (GHG) emissions, and managing climate risks help lower carbon footprint, meet regulations, and boost resilience and competitiveness • Proactive climate action improves brand image, attracts sustainability-focused investors and customers, and drives long-term value	• Failure to effectively identify and manage climate risks may lead to tangible impacts such as increased energy costs, carbon taxes or regulatory penalties, and supply chain disruptions • Inability to meet stakeholder expectations on climate governance may reduce market trust and ratings agency evaluations, thereby affecting capital costs and business expansion	Conducting ISO 14064-1 Greenhouse Gas Inventory and ISO 14067 Product Carbon Footprint to assess energy use and emissions. Implementing TCFD framework to evaluate climate transition risks and physical risks. Integrating energy-saving and carbon reduction strategies to boost climate resilience, risk response, and operational stability	●	●	●	06 Environmental Protection
Talent Development	• Systematic talent development strengthens employee skills, fosters innovation and learning, and boosts operational efficiency and competitiveness • Improved employee engagement and growth opportunities help stabilize workforce structure and reinforce corporate culture and sustainability	• Lack of long-term talent development strategies and learning resources may cause key skill gaps, talent loss, and organizational decline • Insufficient growth opportunities and unfair treatment can lower morale, damage branding, and affect overall operational stability	Committed to building a diverse, equitable, and inclusive workplace with merit-based employment, free from discrimination based on race, nationality, gender, age, political views, or religion. Emphasizing talent development and fair compensation to support employee growth and create shared value with the company		●		07 Social Inclusion
Human Rights Policy	• Establishing a human right-respectful work environment enhances employee well-being and trust, strengthening organizational cohesion, productivity, and corporate image • Integrating human rights protection into corporate governance boosts customer and investor trust, supporting sustainable development	• Failure to implement human rights protections may lead to discrimination, workplace bullying, forced labor incidents, resulting in legal liabilities, labor disputes, and reputational damage • Improper management of supply chain human rights risks may trigger media scrutiny, brand boycotts, and loss of customers	Supporting the “Universal Declaration of Human Rights,” “United Nations Global Compact,” and “International Labour Organization Conventions.” Committed to upholding freedom of association, protecting against child labor, eliminating forced labor and employment discrimination. Continuously monitoring human rights risks and promoting related education and preventive measures	●	●	●	07 Social Inclusion

CyberPower conducts an internal impact analysis on various sustainability topics, where department-level managers quantitatively score each topic based on the likelihood of occurrence and degree of impact. The average scores are used as the basis for analysis to assess the potential positive opportunities and negative risks each topic may pose to operations. To focus on potentially material topics, each impact was rated on a scale of 1 to 5 for both positive and negative impacts, with inclusion thresholds established: an average score of 3.7 or higher for positive impacts, and 2.0 or higher for negative impacts. After statistical aggregation, positive and negative impact matrices are created to visually present the possible effects of each topic on business operations, serving as a key reference for subsequent materiality determination.

Positive Impact Assessment



Negative Impact Assessment



After completing the internal impact analysis, CyberPower further incorporated feedback from external stakeholders to develop a materiality assessment framework that integrates both internal and external perspectives. For the internal part, based on the impact evaluation results, the top four issues with the highest scores were selected separately from both the positive and negative matrices as the preliminary selection. For the external part, the top two issues with the highest stakeholder concern rankings from the survey were selected as supplements. In cases where issue scores were tied, senior management carefully reviewed and decided whether to include the issue, enhancing the professionalism and fairness of the decision-making process.
Combining the internal and external analysis results, nine key sustainability issues were finalized for 2024. A materiality matrix was also created to illustrate each issue's substantive impact on the company's operations and the intensity of external stakeholder concern. This matrix serves as the basis for preparing the report content and focusing sustainability strategies.

Matrix of Material Topics



Changes in Material Topic

Materiality Increased in 2024

- Information Security (Medium → High):
  Rising global information security threats and customer demands highlight the need to strengthen management and response systems
- Ethical Management (Medium-High → High):
  Sustainability trends and international standards increase the focus on governance and supply chain integrity
- Talent Development (Low → Medium-High):
  Internal talent upgrading and regional expansion drive higher demand for employee training and development
- Supply Chain Management (Low → Medium-High):
  Heightened international supply chain risks call for stronger supplier audits and sustainability requirements
- Climate Change Adaption (Low → Medium-High):
  The TCFD framework and expanded carbon accounting raise the importance of climate risk management and disclosure

Materiality Decreased in 2024

- Product Liability (High → Low):
  Quality and safety systems are now routinely managed, resulting in relatively stable risks
- Labor / Management Relations (Medium-High → Low):
  Well-established labor communication mechanisms and no major disputes in recent years
- Occupational Health and Safety (Medium-High → Low):
  Production environment risks are controllable with comprehensive health and safety measures in place
- Risk Management (Medium-High → Low):
  Risk management processes have become more institutionalized, leading to decreased attention to this issue
- Energy Saving and Carbon Reduction (Medium-High → Low):
  Ongoing energy-saving efforts continue, while external focus shifts to climate resilience and carbon disclosure
- Talent Attraction and Retention (Medium-High → Low):
  Low and stable employee turnover makes this a lower priority for stakeholders in the short term
- Customer Relationship (Medium → Low):
  Stable channel and after-sales operations foster mutual trust and cooperation



02 About Us

About CyberPower
Business Operations
Economic Performance
External Engagement

About CyberPower

Founded in 1997, CyberPower has followed a path to success through engineering excellence and quality standards in power protection and computer accessories. We build a comprehensive line of power protection products, including Uninterruptible Power Supplies (UPS), Power Protection and Management Equipment, Power Adapter and Computer Peripherals, and Data Center Power Management Solutions.
CyberPower has cultivated its brand over the years, providing safe and energy-efficient products globally. Our precise global branding strategy has garnered numerous awards. Our advanced manufacturing facilities and precision equipment enable us to offer a comprehensive range of power solutions. From corporate data centers to small businesses and home users, we provide high-quality power supplies to safeguard critical equipment.

CyberPower Company Overview

Company Name	Cyber Power Systems, Inc.
Date of Establishment	1997/06/27
Address	11F., No.26, Jinzhuang Rd., Neihu Dist., Taipei City 114, Taiwan
Worldwide Employees	Approx. 3,000
Paid-in Capital[Note]	NT$941,660 Thousand
Main Business	Uninterruptible Power Supplies (UPS), Data Center Power Management Solutions, Power Protection and Management Equipment, and Power Adapter and Computer Peripherals
Net Sales	Consolidated: NT$12,492,000 Thousand Individual: NT$7,562,873 Thousand

Note: The paid-in capital is as of January 31, 2024.

Global Locations

The Company is primarily engaged in export of its own brand CyberPower at the percentage of over 90% (including OEM services for retailers and Telecom operators) to mainly the Americas and Europe. Other markets served by the remaining subsidiaries are listed on the right:



Major Product and Service Sales by Region in the Past 3 Years

(Unit: NT$ Thousand)

Sales Regions		2022		2023		2024	
		Amount	Percentage	Amount	Percentage	Amount	Percentage
Domestic Sales		182,430	1.63	126,950	1.08	152,439	1.22
Export Sales	Americas	8,501,131	75.78	8,591,508	73.24	9,461,612	75.74
	Europe and Africa	1,499,947	13.37	2,034,398	17.34	1,491,172	11.94
	Asia and Oceania	1,015,076	9.05	932,935	7.95	1,217,002	9.74
	Others	19,135	0.17	45,377	0.39	169,775	1.36
Total		11,217,719	100.00	11,731,168	100.00	12,492,000	100.00

Headquarters and Subsidiaries

Headquarters	Address
Cyber Power Systems, Inc.	11F., No.26, Jinzhuang Rd., Neihu Dist., Taipei City 114, Taiwan
Global Locations	**Address**
Cyber Power (Shenzhen) Ltd	Block 2, Yangyonghe Riverside Development Zone, Tangxiayong, Songgang Sub-district, Bao'an District, Shenzhen, Guangdong, China
Cyber Energy (Shenzhen), Inc.	Room 1601, Jiayu Building, Hongxing Community, Songgang Street, Baoan District, Shenzhen City, Guangdong, China
Best Top (Shenzhen), Inc.	Block 1, Yangyonghe Riverside Development Zone, Tangxiayong, Songgang Sub-district, Bao'an District, Shenzhen, Guangdong, China
Ning Yuan Xian CyberPower, Inc.	In Shilipu Industrial Park, Ningyuan County, Hunan, China
Cyber Power Technology (ShenZhen), Inc.	Room 1601, Jiayu Building, Hongxing Community, Songgang Street, Baoan District, Shenzhen City, Guangdong, China
CliqueFie Co., Ltd.	2F.-2, No. 26, Jinzhuang Rd., Neihu Dist., Taipei City
Cyber Energy Co., Ltd.	2F.-1, No. 26, Jinzhuang Rd., Neihu Dist., Taipei City
Dongguan Cyber Energy Co., Ltd.	Block A.B, Donixing Industrial Park, Hangmei Village, Dongkeng County, Dongguan, Guangdong, China
Cyper Power Systems (USA), Inc.	4241 12th Avenue East Suite 400 Shakopee, MN 55379
Cyber Power Systems K.K.	3F, S3 Chiyoda-Iidabashi, 3-1-5, Iidabashi, Chiyoda-ku, Tokyo 102-0072
Cyber Power Systems B.V.	Flight Forum 3545 5657DW Eindhoven The Netherlands
Nitram SAS	Zone Industrielle Saint Séverin 28220 Cloyes Sur Le Loir France
CyberPower Systems GmbH	Edisonstr. 16, 85716 Unterschleissheim, Germany
Cyber Power Systems S.A. DE C.V.	Avenida Insurgentes Sur número 1457, colonia Insurgentes Mixcoac, delegación Benito Juárez, C.P. 03920, en la Ciudad de México
Cyber Power Systems (India) Private Limited	No. 702, Kushwah Chambers, Makwana Road, Marol, Andheri East, India 400059
Cyber Power Systems Manufacturing, Inc.	Units A & B, Block 1, Lot 6 Phase 2 Golden Gate Business Park Buenavista I General Trias Cavite, Region IV-A, Philippines, 4107
Phisonic Technology Corporation	Units A1, Block 1, Lot 6 Phase 2 Golden Gate Business Park Buenavista II General Trias Cavite, Region IV-A, Philippines, 4107

Note 1: Global locations include subsidiaries and sub-subsidiaries.
Note 2: For more information, please refer to the "2024 CyberPower Annual Report", P.85

Business Operations


Innovation & Research


Safety Testing


Manufacturing


Quality Management


Brand Marketing


Customer Service

CyberPower has a dedicated R&D engineering team of more than 350 employees worldwide, along with 7 production bases, including an injection molding factory located in Taiwan, China, and the Philippines. Since its establishment, the company has developed power management software alongside hardware products, ranging from early personal software to enterprise, cloud, and data center management solutions. This integrated approach delivers significant value to our customers, extending beyond the capabilities of hardware alone.

Through innovative technologies, we design and manufacture a comprehensive range of products to meet various market demands, including Uninterruptible Power Supplies (UPS), Data Center Power Management Solutions, Power Protection and Management Equipment, and Power Adapter and Computer Peripherals. All our products are engineered with our proprietary advanced technology, and through our relentless pursuit of excellence, we consistently deliver high-quality solutions. Additionally, our in-house safety test lab is audited by 3rd-party certificate laboratories, including UL from the US and TUV Rheinland from Germany. With sufficient resources and equipment, we conduct pre-production testing to ensure that products sold in international markets comply with local regulations.

To meet the expectations of all stakeholders, CyberPower continues to drive innovation while upholding the principles of integrity and pragmatism in brand management. Over the years, our efforts have earned widespread international recognition. Through strategic brand marketing, we enhance both corporate image and product value, and actively expand into global markets to meet the diverse needs of customers worldwide.

At the same time, we are committed to strengthening localized customer service systems, providing users with professional support to ensure a stable and reliable service experience.

CyberPower strives to become a world-leading provider of power management solutions, creating maximum value for users and partners. We will connect the supply chain and work closely with customers, focusing on the development of energy-saving technologies to meet all power management and customer service needs. Our goal is to bring intelligence, energy efficiency, and sustainability to people's lives.

CyberPower Main Products and Functions

Product Category	Functions
Uninterruptible Power Supplies (UPS)	Provides connected devices clean power and automatically switches to battery power during a blackout to prevent equipment such as computers, communications devices, consumer electronics, medical devices, and transportation systems from failing.
Data Center Power Management Solutions	Provides reliable and secure power distribution and management for data centers, offering early warning to prevent unexpected shutdowns and significantly enhancing the reliability and availability of data center power supply. Intelligent models feature high-precision metering for precise energy consumption monitoring, serving as a key indicator for optimizing data center energy efficiency and meeting the diverse power distribution needs of data centers.
Power Protection and Management Equipment, and Portable Power Adapter	A compact, lightweight, and portable power converter designed to transform readily available power sources into usable power for mobile electronic devices such as laptops, smartphones, PDAs, and digital cameras. This converter acts as a high-frequency noise filter under normal conditions and incorporates voltage clamping components to absorb excessive voltage energy during power surges, protecting downstream electronic equipment.
Solar Inverter and Energy Storage Equipment	Converts direct current power generated by solar panels into alternating current power for grid integration. If equipped with energy storage, excess electricity can be stored for later use to power loads.
Others	Customized electronics, such as USB hubs, cables, etc.

Business Ratios at Present

The main products marketed by CyberPower are divided into 4 categories. Based on the annual turnover of 2024, the business ratio of Uninterruptible Power Supplies (UPS) is about 56.44%, that of Data Center Power Management Solutions about 30.38%, that of Power Protection and Management Equipment about 11.33%, and that of Power Adapter and Computer Peripherals about 1.85%.

Production and Sales Performance of Main Products in the Past 3 Years

(Unit: NT$ Thousand / %)

Product Category	2022		2023		2024	
	Sales Revenue	Proportion	Sales Revenue	Proportion	Sales Revenue	Proportion
Uninterruptible Power Supplies (UPS)	6,189,088	55.17%	6,467,362	55.13%	7,050,276	56.44%
Data Center Power Management Solutions	2,951,062	26.31%	3,418,635	29.14%	3,794,939	30.38%
Power Protection and Management Equipment	1,538,004	13.71%	1,608,135	13.71%	1,415,717	11.33%
Power Adapter and Computer Peripherals	539,565	4.81%	237,036	2.02%	231,068	1.85%

Core Competence

CyberPower is committed to becoming a global leader in power management solutions. Through the strength of its own brand, technological innovation, in-house manufacturing, agile responsiveness, and a strategic global presence, the company continues to reinforce its leading position in the market. Its core competitive advantages are outlined as follows:

Comprehensive Solutions: User-Centric Approach with Agile Market Response

With robust capabilities in R&D, manufacturing, software development, operations management, and marketing, the company is well-positioned to respond swiftly to market demands and deliver power management solutions tailored to real-world scenarios. Beyond offering products, CyberPower integrates both hardware and software to address a wide range of power-related challenges, demonstrating high value-added services and advanced system integration capabilities.

Brand Marketing Strength: Building a Global Presence through Its Own Brand

Since its establishment, CyberPower has remained focused on developing its own brand to expand its footprint in international markets. Through multi-channel marketing strategies, the company has built a trustworthy and highly recognizable global brand image. CyberPower continues to enhance its after-sales service capabilities across global markets and foster strong brand loyalty. Its performance has been recognized with numerous international awards, clearly setting the company apart from competitors in both Taiwan and the global UPS industry.

Market Insight: Participating in Standard-Setting to Stay Ahead of Technological Trends

Renowned for its expertise and industry reputation, CyberPower is frequently invited by major international corporations to participate in the development of product specifications for future offerings. This involvement provides early access to emerging technologies and market trends, enabling the company to make proactive investments in R&D and production planning. As a result, CyberPower demonstrates strong market foresight and agile responsiveness, further reinforcing its competitive advantage.

Innovative R&D: Deep Technical Capabilities Driving Product Value

CyberPower has established R&D teams across seven major product lines, supported by an in-house safety laboratory and a professional anechoic chamber that enable rapid product verification and technical optimization. The company also develops its own power management software and SNMP / HTTP modules, effectively enhancing the intelligence and added value of its products. This integrated approach ensures seamless alignment between hardware and software within the R&D framework, further strengthening CyberPower's innovation capabilities.

In-House Manufacturing: Cost Control, Quality, and Supply Stability

CyberPower operates its own manufacturing facilities, allowing for effective control over product costs, quality, and lead times through integrated in-house production systems. Backed by a robust supply chain management framework, the company can flexibly manage inventory and provide customized manufacturing to meet the demands of fluctuating global markets. Even during major global disruptions, CyberPower has consistently ensured stable product delivery, demonstrating strong manufacturing resilience and dependable fulfillment capabilities

Economic Performance

2024 Material Topic: Management of "Economic Performance"

Material Topics	Economic Performance
GRI Standards	GRI 201-1 Direct economic value generated and distributed GRI 207-1 Approach to tax GRI 207-2 Tax governance, control, and risk management GRI 207-3 Stakeholder engagement and management of concerns related to tax
SDGs	
Policy or Commitment	The company adopts prudent operational strategy, optimizing resource allocation to ensure the well-being of employees. We comply with the requirements of the government and competent authorities. We develop robust and comprehensive financial systems, uphold the principles of financial openness and transparency, strengthen our corporate governance, and strive to achieve sustainable operations, with a strong focus on maximizing shareholders' interests.
Indicators and Goals	Short-term (1-2 years) • Achieve the goals set out in the annual budget • Invest approximately 5% of annual turnover in product research and development Mid- and Long-term (over 2 years) • Stable growth and profitability enhancement • Continuous communication with the capital market to optimize financial structure and operational capabilities
Effectiveness Tracking Mechanism	• Set annual budgets and hold regular management meetings to track, review, and determine countermeasures. The company held a total of 9 management meetings in 2024 • Established an Audit Committee and a Remuneration Committee to strictly supervise the company's accounting, financial processes, and internal audits • Invited to attend 3 investor conferences
Annual Actions and Measures	• Actively explored new domestic and overseas customers, and strengthened relationships with existing customers in order to achieve business performance • Regularly review costs and expenses to achieve cost control and stable growth • Revenue growth of 6.49% compared to the previous year • Net profit budget achievement rate 125.68%

Direct Economic Value Generated and Distributed by Organization

(Unit: NT$ Thousand)

Category		2022	2023	2024
Direct Economic Value Generated	Operating Revenue	11,217,719	11,731,168	12,492,000
	Non-operating Income	73,275	173,301	232,024
The Total of Direct Economic Value Generated		11,290,994	11,904,469	12,724,024
Economic Value Distributed	Operating Costs	8,230,899	7,993,433	7,993,433
	Employee Compensation and Welfare	1,793,355	1,887,958	2,029,862
	Payments Made to Investors	459,254	728,070	1,412,491
	Payments Made to Governments	259,871	522,045	622,408
	Community Investments	0	0	0
The Total of Economic Value Distributed		10,743,379	11,131,506	12,058,194
Economic Value Retained		547,615	772,963	665,830

Note: Economic Value Retained = Direct Economic Value Generated – Economic Value Distributed.

CyberPower takes prudent operational strategy and continues to adjust the strategy and develop new markets. In 2024, the consolidated revenue was NT$12,492,000 thousand, net income after tax was NT$2,308,378 thousand, and earnings per share was NT$24.75. Compared to 2023, revenue in 2024 increased by 6.49% from the previous year, and the net profit budget achievement rate was 125.68%.

Condensed Comprehensive Income Statement in the Past 3 Years[Note 1]

(Unit: NT$ Thousand)

Category	Unit	2022	2023	2024
Operating Revenue	NT$ Thousand	11,217,719	11,731,168	12,492,000
Operating Costs	NT$ Thousand	6,486,741	6,138,321	6,127,250
Operating Margin	NT$ Thousand	4,730,978	5,592,847	6,364,750
Operating Expenses	NT$ Thousand	3,570,642	3,778,650	3,937,466
Net Operating Profit	NT$ Thousand	1,160,336	1,814,197	2,427,284
Net Non-Operating Income and Expenses	NT$ Thousand	339,474	122,807	521,495
Pre-tax Profit	NT$ Thousand	1,499,810	1,937,004	2,948,779
Income Tax	NT$ Thousand	(342,208)	(462,219)	(640,401)
Net Income	NT$ Thousand	1,157,602	1,474,785	2,308,378
Other Comprehensive Income (Net Value after Tax)	NT$ Thousand	120,497	7,621	136,387
Total Comprehensive Income	NT$ Thousand	1,278,099	1,482,406	2,444,765
Net Income Attributable to Shareholders of the Parent Company	NT$ Thousand	1,142,846	1,468,530	2,283,855
Total Comprehensive Income Attributable to Owners of The Parent Company	NT$ Thousand	1,262,801	1,476,889	2,418,949
Earnings Per Share	NT$	13.41	16.58	24.75
Cash Dividend[Note 2]	NT$	5.0	8.0	15

Note 1: Entities included in the consolidated financial statements include: all subsidiaries and sub-subsidiaries. For more information, please refer to the "2021.Q4-2024.Q4 Consolidated Financial Statements", P.9-10.
Note 2: Based on surplus year.

Approach to Tax

The company adheres to tax regulations and fulfills our corporate social responsibility goals. Aiming to create corporate value and improve tax risk management, we have developed tax governance, transfer pricing policies, and comprehensive tax management system and approach, along with real-time and prompt handling procedures. The following taxation governance policies have been established to enhance corporate value, fulfill corporate social responsibility and civic duty, and implement sustainable development.

The Role and Responsibility of Tax Governance

The role and responsibility of tax governance are as follows:

Chief Finance Officer

The Head of Finance & Accounting Division is responsible for verifying and approving the overall tax governance policy according to the operating strategy and environment, to ensure the effective operation of the tax management mechanism.

Tax Management Unit

The tax management unit is the Finance Department, which is responsible for regularly reporting tax-related management status to the Head of Finance & Accounting Division.

Effective Tax Rate in the Past 3 Years

(Unit: NT$ Thousand; %)

Category	2022	2023	2024
Pre-tax Profit	1,499,810	1,937,004	2,948,779
Income Tax	342,208	462,219	640,401
Income Tax Paid	226,742	486,465	570,019
Effective Tax Rate on the Books	23%	24%	22%
Effective Cash Tax Rate	15%	25%	19%

Tax Governance, Control, and Risk Management

CyberPower's tax governance policy is founded on transparency, openness, and regulatory compliance. We adhere to local tax regulations and legislative principles at every operational location, ensuring accurate tax declaration and payment, and we have not engaged in any unethical or illegal behavior or concerns. Regarding the declaration and payment of taxes, we appointed qualified accountants or tax agents in each region when there is a need to communicate with the tax authorities. Transactions between related parties must adhere to arm's length principles and comply with the relevant tax regulations in each region, particularly the jurisdiction's transfer pricing rules, ensuring that the pricing and terms of these transactions meet local regulatory standards for fairness, legality, and adherence to applicable laws.

Policy for Communication with Stakeholders of Tax-related Issues

One of the main stakeholders of CyberPower is the tax authority of the government. The tax declaration and payment of the company have been handled according to the provisions of the relevant laws and regulations of each country. In case of any ambiguity regarding applicable laws and regulations in daily operation process, we contact the relevant authority directly or through Deloitte Taiwan to inquire about appropriate handling methods. If tax audit work is conducted, relevant data shall be immediately prepared after the relevant notice is received, and we will coordinate with the tax authority to verify the data.

To demonstrate the transparency in our tax governance policy, the tax information related to other stakeholders like shareholders and investors, will be provided in the Stakeholder Section on the CyberPower Official Website, the Annual Report, and during shareholders' meetings.

External Engagement

External Initiatives

Supported International Initiatives

- The United Nations' 17 Sustainable Development Goals (SDGs), advocating for integrated sustainability indicators across social, economic, and environmental dimensions, along with global collaborative efforts toward sustainability
- The "United Nations Global Compact," promoting sustainable governance by addressing issues related to human rights, labor, environment, and anti-corruption within organizations

Environmental	• The Task Force on Climate-related Financial Disclosures (TCFD), assisting investors and decision-makers in understanding an organization's climate-related risks, opportunities, and financial impacts, helping them navigate transformational challenges • Participate in the Carbon Disclosure Project (CDP), measuring and improving companies' carbon management systems effectively
Social	• International Labour Organization (ILO), continuously improving the working and living conditions of employees while safeguarding their rightful rights • Social Accountability 8000 (SA8000), ensuring the human rights, environmental practices, and ethics of supply chain partners comply with international standards of conduct • Responsible Business Alliance (RBA), ensuring that supply chain partners provide a safe working environment and that workers are treated with respect • Responsible Minerals Initiative (RMI), rejecting to use conflict minerals
Governance	• The United Nations Convention against Corruption (UNCAC), establishing a robust governance system for prevention and anti-corruption efforts

Eligibility in Trade Unions / Associations

Public Associations and Advocacy Organizations with Significant Involvement

Organization Name	Strategic Significance	Membership
Solar PV Generation System Association of R.O.C (PVGSA)	Promote the adoption of green energy, acquire the latest industry information, and establish a network with engaged peers	Sponsorship Member
Taiwan External Trade Development Council (TAITRA)	Expand overseas distribution channels, stay abreast of global trade and industry trends, participate in international exhibitions and marketing activities, enhance the brand's international visibility, and boost export order opportunities	Member
Taipei Neihu Technology Park Development Association	Promote business networking and resource sharing among enterprises, monitor local industry policies and development trends, participate in public affairs and advocacy activities, and strengthen collaborative relationships with the government and local businesses	Member



03 Corporate Governance

Governance Structure
Functional Committees
Ethical Management
Legal Compliance
Risk Management
Information Security

Governance Structure

Policy and Commitment

CyberPower adheres to the core principles of integrity in management and responsible governance. The company is committed to establishing a transparent and robust corporate governance framework to strengthen the effectiveness of the Board of Directors, ensure legal and regulatory compliance, and protect the rights and interests of shareholders and stakeholders. In accordance with the "Company Act," "Securities and Exchange Act," and other relevant regulations, CyberPower has adopted the "Corporate Governance Best Practice Principles," which clearly define the responsibilities and operational guidelines of the Board of Directors and its functional committees.

To uphold ethical business conduct and integrity, the company has established the "Ethical Corporate Management Principles" and the "Code of Ethical Conduct." These documents address key areas including anti-corruption, conflict of interest prevention, prohibition of insider trading, information confidentiality, and accurate and honest disclosure. In addition, CyberPower has implemented a conflict-of-interest declaration system and an internal whistleblower mechanism. The Audit Department is responsible for receiving and investigating reported violations and ensuring that whistleblowers are protected throughout the process. Both principles have been approved by the Board of Directors and reported to the shareholders' meeting for the record. They are publicly disclosed, enforced by the Finance & Accounting Division, and are applicable to all employees.

To implement the core values of ESG, CyberPower places strong emphasis on economic governance, human rights protection, and environmental conservation. The company has established the "Sustainable Development Best Practice Principles" as a core guideline for promoting sustainable operations. CyberPower is publicly committed to ensuring that all business activities comply with responsible business conduct and align with the following key domestic and international initiatives and standards:

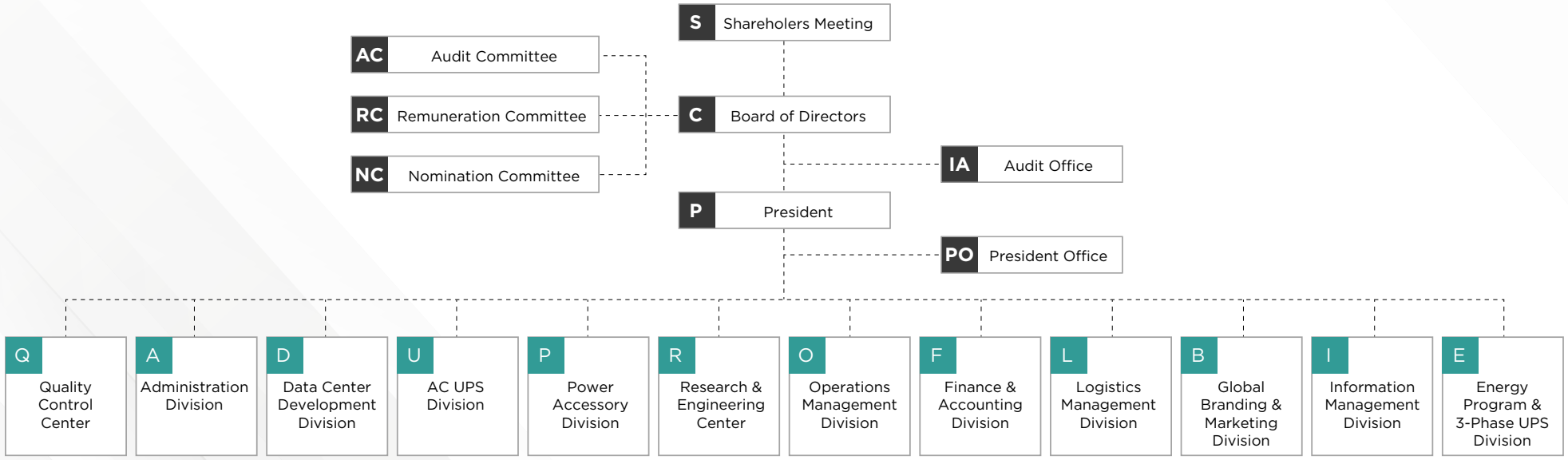
- "United Nations Guiding Principles on Business and Human Rights (UNGPs)"
- "Ethical Corporate Management Best Practice Principles for TWSE/TPEx Listed Companies"
- "Guidelines for the Adoption of Codes of Ethical Conduct for TWSE/GTSM Listed Companies"
- "Sustainable Development Best Practice Principles for TWSE/TPEx Listed Companies"
- "Corporate Governance Best Practice Principles for TWSE/TPEx Listed Companies"

All sustainability-related principles have been reviewed and approved by the Board of Directors. CyberPower communicates these principles effectively with both internal and external stakeholders through its Official Website, meetings, contractual provisions, and internal platforms. English versions are also provided to strengthen international alignment and enhance transparency.

CyberPower's framework also includes commitments to relevant due diligence and early warning mechanisms, particularly with regard to human rights. The company adheres to the principles of "Universal Declaration of Human Rights," the "United Nations Global Compact," and the "International Labour Organization Conventions," striving to uphold the fundamental rights and dignity of all stakeholders.

To strengthen integrity and governance throughout the industry value chain, CyberPower also requires supply chain partners to sign the Integrity Clause in the "Procurement Agreement," thereby jointly promoting the shared goals of ethical business practices and sustainable development.

Organizational Structure



Note: For more information on the corporate governance structure and the responsibilities of each department, please refer to the "2024 CyberPower Annual Report."

Board of Directors

The highest governing body of CyberPower is the Board of Directors, which is responsible for decision-making, oversight, and managing the company's economic, environmental, human rights, and social impacts. The current board consists of 7 members, including 3 independent directors, who represent 42.86% of the seats. The Board was re-elected in June 2023, with the term running from June 2023 to June 2026.
CyberPower values the diverse industry experiences, professional backgrounds, and capabilities of its board members while continuing to incorporate perspectives from different genders, ages, and disadvantaged groups. In accordance with Article 20 of the company's "Corporate Governance Best Practice Principles," the current board includes 2 female directors, and directors who also serve as company executives occupy less than one-third of the Board seats. The company is committed to promoting the board's independence and gender diversity to enhance the diversity of perspectives in decision-making and reduce overall operational risks.

Board Member and Individual Director Diversity Implementation

Title	Name	Nationality	Gender	Age	Board Meeting Attendance Frequency	Holding Other Directorship Positions	Representative of Stakeholders	Items of Diversity							
								Ability to Make Judgments about Operations	Accounting & Financial Analysis	Business Management	Risk Management	Knowledge of the Industry	An International Market Perspective	Leadership	Decision-making Ability
Chair	Chih Yuan Investment Co., Ltd. Representative: Kuo, Chin	R.O.C.	Female	61-65	8	Yes	Shareholder	●	●	●	●		●	●	●
Director	Ning Yuan Investment Co., Ltd. Representative: Ho, Lien-Hsun	R.O.C.	Male	51-60	8	Yes	Shareholder and Employee (President)	●		●	●	●	●	●	●
Director	Hsien Yueh Investment Co., Ltd. Representative: Lee, Chien-Chin	R.O.C.	Male	51-60	8	Yes	Shareholder	●		●	●	●	●		●
Director	Lu, Lee-Da	R.O.C.	Male	71-75	7	Yes	None	●		●	●	●	●	●	●
Independent Director	Wang, Chin-Yen	R.O.C.	Female	61-65	4	Yes	None	●	●	●	●		●		●
Independent Director	Ou Yang, Mang	R.O.C.	Male	51-60	4	No	None			●	●	●	●	●	●
Independent Director	Ko, Po-Cheng	R.O.C.	Male	51-60	6	No	None	●	●	●	●		●		●

Note: For more information, please refer to the "2024 CyberPower Annual Report" P.4, P.8, and P.16.

Board Nomination and Selection

On March 23, 2023, CyberPower elected 7 directors (including 3 independent directors) at the General Shareholders' Meeting. With the unanimous consent of all directors present, Wang, Chin-Yen, Ou Yang, Mang, and Ko, Po-Cheng were nominated as candidates for independent directors.
Following a review by the Nomination Committee, the 7 director candidates, including 3 independent directors, were evaluated based on their diversity, independence, as well as academic background, professional experience, industry expertise, and professional skills relevant to the impact to the organization. All candidates were confirmed to meet the requirements outlined in Articles 2, 3, and 4 of the "Regulations Governing Appointment of Independent Directors and Compliance Matters" for Public Companies and Article 192-1 of the "Company Act" As a result, the list of 7 director candidates was approved, with Wang, Chin-Yen, Ou Yang, Mang, and Ko, Po-Cheng included as nominees for independent directors on the company's 2023 candidate list.
Kuo, Chin has served as the Chair of CyberPower for many years, bringing expertise in operational judgment, business management, leadership, decision-making, and crisis management. She has consistently provided professional and comprehensive guidance on the company's operations and strategic decisions. As a result, she has been unanimously re-elected by the newly appointed board members to continue as Chair of CyberPower, greatly benefiting the company's future.

Conflict of Interest Avoidance

The highest governance authority of CyberPower is led by Chair Kuo, Chin, who does not hold any other executive management positions. All board members are appointed through a nomination process. The Board of Directors has established the "Regulations Governing Procedure for Board of Directors Meetings" in accordance with the "Regulations Governing Procedure for Board of Directors Meetings of Public Companies," which includes clear guidelines on the principle of conflict-of-interest avoidance for directors.
Currently, CyberPower faces potential conflicts of interest arising from directors holding positions on other boards. To prevent and mitigate such conflicts, the company has implemented a comprehensive conflict of interest avoidance policy. Directors are required to uphold the highest ethical standards, exercise prudence, and fulfill their fiduciary duties with integrity. The policy mandates that board members disclose the key details of any conflict of interest related to meeting agenda items where they, or the legal entities they represent, may have vested interests. If such conflicts could harm the company's interests, the directors must refrain from participating in discussions and voting on the matter, and are prohibited from proxy voting on behalf of other directors.

Director Recusal Due to Conflict of Interest

Meeting	Proposal	Director Name	Reason for Recusal	Voting Participation
10th Board, 9th Meeting 2024/08/08	Proposal for Managerial Compensation	Ho, Lien-Hsun	Ho Lien-Hsun, representative of Ning Yuan Investment Co., Ltd., also serves as the President of the company and thus has a personal interest.	Due to a conflict of interest, the director voluntarily recused himself from the discussion and voting. The chair consulted with the other attending directors, and the proposal was approved as presented.
10th Board, 11th Meeting 2024/12/19	Proposal for Compensation of Chair, Managers, and Chief Auditor	Kuo, Chin Ho, Lien-Hsun	Kuo, Chin as the Chair had a personal interest. Ho Lien-Hsun, representative of Ning Yuan Investment Co., Ltd., also serves as the President of the company and thus has a personal interest.	Due to a conflict of interest, both directors voluntarily recused themselves from the discussion and voting. The acting chair consulted with the other attending directors, and the proposal was approved as presented.

Note: For more information, please refer to the "2024 CyberPower Annual Report" P.16.

Board of Directors Education and Training

The members of the CyberPower Board of Directors are committed to continuously enhancing their industry expertise and governance experience to foster sustainable development, staying aligned with global business management trends, and strengthening corporate governance and risk management capabilities. We arrange courses for the Board of Directors that fully cover economic, environmental, and social-oriented topics to enrich the governance knowledge and trend insights required. Furthermore, we ensure that independent directors are kept informed by regularly providing relevant law information, as well as messages from competent authorities. Based on the needs and feedback from the Board of Directors, the company is committed to strengthening the dissemination of information and further education programs, ensuring fulfillment of the leadership and supervisory functions. In 2024, the Board of Directors had a total of 42 hours of education and training, with an average of 6 hours per person. The courses covered sustainability-related regulations and the impact of net-zero carbon emissions on financial reporting, helping directors stay informed on economic, environmental, and social issues.

Directors' Education and Training

Title	Name	Organizer	Date	Course	Hours
Representative Director	Kuo, Chin	Taiwan Corporate Governance Association (TCGA)	2024/05/10	The ESG Legal Issues Faced by Board of Directors	3
		Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3
Representative Director	Ho, Lien-Hsun	Taiwan Corporate Governance Association (TCGA)	2024/05/10	The ESG Legal Issues Faced by Board of Directors	3
		Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3
Representative Director	Lee, Chien-Chin	Taiwan Corporate Governance Association (TCGA)	2024/05/10	The ESG Legal Issues Faced by Board of Directors	3
		Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3
Director	Lu, Lee-Da	Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3
		Securities and Futures Institute (SFI)	2024/10/18	2024 Insider Trading Prevention Awareness Seminar	3
Independent Director	Ou Yang, Mang	Taiwan Corporate Governance Association (TCGA)	2024/05/10	The ESG Legal Issues Faced by Board of Directors	3
		Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3
Independent Director	Wang, Chin-Yen	Taiwan Corporate Governance Association (TCGA)	2024/05/10	The ESG Legal Issues Faced by Board of Directors	3
		Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3
Independent Director	Ko, Po-Cheng	Taiwan Corporate Governance Association (TCGA)	2024/05/10	The ESG Legal Issues Faced by Board of Directors	3
		Accounting Research and Development Foundation (ARDF)	2024/08/08	Practical Analysis of the Impact of Net-Zero Carbon Emissions on Financial Reporting	3

Note: For more information, please refer to the "2024 CyberPower Annual Report" P.9-10.

Board Performance Evaluation

To implement corporate governance, and enhance the functions of the Board of Directors, CyberPower has established the "Regulations of The Board Performance Evaluation", including an annual self-assessment of the Board of Directors and functional committees, and a self-assessment of the performance of individual board members. Measurement items for performance evaluation of the Board of Directors include five aspects: participation in the company's operation, improvement in the Board of Directors' decision quality, composition and structure of the Board of Directors, election and continuing education of directors, and internal control. The Remuneration Committee also reviews and recommends relevant salary payment standards and exact amounts based on the evaluation results. In 2024, the results from self-evaluations of the Board of Directors, functional committees, and individual directors achieved an attainment rate of over 90% for all measurement indicators, surpassing the standard. The performance evaluation results were submitted to the Board of Directors in December 2024.

In addition to internal self-assessments, CyberPower also hires external evaluation agencies every 3 years to access the performance of its Board of Directors. The most recent external evaluation was carried out by the Taiwan Institute of Ethical Business (TIEB) in 2022. The evaluation report included recommendations on increasing the proportion of female directors and preparing a Sustainability Report. The company has already addressed these suggestions at the shareholders' meeting on June 13, 2023. After a full re-election of directors, by the end of 2023, the proportion of female directors was 2 out of 7, reflecting tangible progress in gender diversity. Concurrently, the company also engaged external consultants for the first time to assist in planning and preparing the Sustainability Report, thereby enhancing communication and information transparency with stakeholders.

Remuneration Policy for Directors and Executives

The Remuneration Committee, composed of independent directors who provide external diverse perspectives and opinions, establishes and reviews the remuneration policies, systems, standards, and structures for directors and executives. The committee meets at least twice a year to review the remuneration package, ensuring its competitiveness and appropriateness.

The annual remuneration package of the Board of Directors consists of remuneration, directors' compensation, and business execution expenses. Directors who also serve as employees are additionally compensated with salary and bonuses, and the remuneration of senior executives includes salary, bonuses, and retirement benefits. There are no other significant special benefits, and the retirement benefits system is the same as that of other employees, which is implemented in accordance with legal regulations. The above remuneration is regularly disclosed in the company's Annual Report. For details in 2024, please refer to the "2024 CyberPower Annual Report," P.11-14.

In accordance with CyberPower's "Articles of Incorporation," the company shall allocate a minimum 2% of the profits as employee remuneration, and the Board of Directors may also allocate up to 2% of the profits as remuneration for directors.

The directors' remuneration is determined by the "Regulations of The Board Performance Evaluation." In addition to the company's overall business performance and future business risks, reasonable remuneration is provided to directors based on the extent of their participation in business, the quality of decisions, the performance achievement rate, and relevant contribution. The executives' remuneration consists of salary and bonuses with the salary based on industry standards, job level, professional competence, and responsibilities. The bonuses are based on a combination of financial indicators (e.g., revenues, profit margins, growth rate, and achievement of operational efficiency) and non-financial indicators (e.g., innovation and integration, risk management and information security, the significant deficiencies in their departments' compliance with laws and operational risk issues). The Remuneration Committee and the Board of Directors review the appropriateness of the remuneration of directors and executives, and the remuneration system is reviewed from time to time for actual business conditions and relevant laws and regulations to strike a balance between sustainable operations and risk control.

Unjust Enrichment Policy

To guide the directors, executives, and all employees to perform their duties and activities by ethical standards and codes of conduct, CyberPower has established the "Ethical Corporate Management Principles," the "Codes of Ethical Conduct of Board of Director and Management," and the "Codes of Ethical Conduct." Violations of the above rules and regulations will be subject to disciplinary action in accordance with company's "Work Rules" and "Employee Reward and Punishment Policy." If there is specific evidence of embezzlement, misappropriation of funds, or acceptance of bribes or kickbacks, employment may be terminated immediately without prior notice. We expect all employees, including executives, to fulfill their management and supervisory responsibilities and strictly adhere to the codes of ethical conduct, ensuring the company's sustainable growth and development.

Functional Committees

To manage operational risks and monitor the company's impact on the economy, the environment, people, and human rights, CyberPower has established several functional committees under the Board of Directors, including the Audit Committee, the Remuneration Committee, and the Nomination Committee. Each functional committee is responsible for developing, approving, and updating strategies related to relevant impacts, based on feedback from stakeholders regarding significant events or suggestions related to positive and negative risks arising from the company's operations. The feedback is collected from general business communication channels, internal meetings, questionnaires, surveys, and document signing, as well as due diligence via the established complaint system. The Board of Directors is responsible for overseeing the impact management procedures and outcomes of the functional committees. The results are regularly reported and reviewed for procedural effectiveness during annual meetings.

Audit Committee

CyberPower established the Audit Committee on June 12, 2020, to perform corporate risk control. The committee is composed of 3 independent directors elected at the shareholders' meetings, and holds cross-departmental risk management meeting at least once every quarter to discuss the issues related to significant risks. Its work priorities are to execute the fair presentation of financial statements of the company, effective implementation of election of CPAs and their independence and performance, internal control, compliance with laws and regulations, control of existing and latent risks of the company. The Audit Committee determines whether to present risk reports to the Board of Directors based on their materiality. In 2024, a total of 7 Audit Committee meetings were held, with an average attendance rate of 100%.

The Members of Audit Committee

Name	Title	Gender	Term
Wang, Chin-Yen	Independent Director (Convener)	Female	2023/06/13-2026/06/12
Ou Yang, Mang	Independent Director (Committee Member)	Male	2023/06/13-2026/06/12
Ko, Po-Cheng	Independent Director (Committee Member)	Male	2023/06/13-2026/06/12

Remuneration Committee

CyberPower has established a Remuneration Committee and the "Remuneration Committee Charter" to enhance corporate governance and strengthen the Board of Directors' remuneration management. The committee assists the Board in evaluating and determining the remuneration for directors and senior executives, ensuring that their compensation is competitive in the market and motivates senior executives to adopt a long-term business mindset. In 2024, a total of 3 Remuneration Committee meetings were held, with an average attendance rate of 100%.

The Responsibilities of the Remuneration Committee

- Regularly review the "Remuneration Committee Charter" and propose revisions
- Establish and periodically review the policies, systems, standards, and structures of the company's annual and long-term performance goals and remuneration for directors and executives
- Regularly evaluate the achievement of the company's performance goals for directors and executives and determine the plan and amount of their individual remuneration

The Members of Remuneration Committee

Name	Title	Gender	Term
Ko, Po-Cheng	Independent Director (Convener)	Male	2023/06/21-2026/06/12
Wang, Chin-Yen	Independent Director (Committee Member)	Female	2023/06/21-2026/06/12
Ou Yang, Mang	Independent Director (Committee Member)	Male	2023/06/21-2026/06/12

Nomination Committee

CyberPower established the Nomination Committee on November 12, 2018. The committee is composed of 3 independent directors elected by the Board of Directors, with more than half of them being Independent Directors. The responsibilities of the Nomination Committee are seeking, reviewing, and nominating director candidates, as well as building and developing the organizational structures and corporate governance of the Board of Directors and committees. The committee shall hold meetings at least twice a year and as needed. In 2024, a total of 2 Nomination Committee meetings were held, with an average attendance rate of 100%.

The Members of Nomination Committee

Name	Title	Gender	Term
Ou Yang, Mang	Independent Director (Convener)	Male	2023/06/21-2026/06/12
Ko, Po-Cheng	Independent Director (Committee Member)	Male	2023/06/21-2026/06/12
Wang, Chin-Yen	Independent Director (Committee Member)	Female	2023/06/21-2026/06/12

Ethical Management

2024 Material Topic: Management of "Ethical Management"

Material Topics	Ethical Management
GRI Standards	GRI 205-1 Operations assessed for risks related to corruption GRI 205-2 Communication and training about anti-corruption policies and procedures
SDGs	
Policy or Commitment	Adhere to the principle of corporate governance of ethical management and practicing a zero-tolerance policy on corruption. All employees are strictly required to hold themselves and their suppliers and partners to the highest standards of business conduct to protect the interests of all stakeholders and meet their expectations.
Indicators and Goals	Mid- and Long-term Goals (2-5 Years) • Maintain a corruption-free environment; no substantiated incidents of corruption • Continuous education and training on ethical management and anti-corruption • Continuously strengthen the integrity culture of employees and partners through education, training, and communication
Effectiveness Tracking Mechanism	• All new employees are required to receive ethical management and anti-corruption education and training upon joining the company. • Employees, suppliers, and other partners may report corrupt activities via business ethics mailbox. Upon receiving a report, the company will handle through the established process. If the case is substantiated, the involved individuals will be penalized, and internal awareness will be strengthened, along with improvements to the management process. • Internal audit and whistleblower system • Self-declaration of employee conflict of interest avoidance
Annual Actions and Measures	• To effectively enhance all employees' awareness of anti-corruption, we organized education and training programs aimed at reducing the likelihood of such incidents. • No corruption incidents or related reports occurred • The result of the risk assessment was low and within the tolerable range. There were no instances of corruption, no employees were disciplined or terminated, and no business partners had their contracts terminated or not renewed due to corruption violations. • There were no major violations of laws or regulations resulted in fines or penalties

Ethical Management Implementation

With reference to the "Ethical Corporate Management Best Practice Principles for TWSE/TPEx Listed Companies," CyberPower establishes its "Ethical Corporate Management Principles," which is implemented and published on the Official Website after being approved by the Board of Directors. Both the Board of Directors and senior executives are committed to actively implementing the management policies.

To prevent unethical behavior, the company has established an analysis mechanism to assess business activities with a higher risk of unethical conduct and has developed preventive measures accordingly. To avoid trading with parties involved in unethical activities, CyberPower considers the legitimacy of its distributors, suppliers, customers, and trading partners and evaluates whether they engage in unethical conduct before entering into business or contractual relationships.

The relevant inspection items are as follows:

1. The company's operating location and organizational structure
2. The risk of corruption in the company's operating country
3. The bribery risk of the company in its related industries
4. The company's long-term operating condition, goodwill, and reputation
5. The company's records of unethical behavior such as bribery or illegal political contribution

In addition, the company has established the "Codes of Ethical Conduct of Board of Director and Management" which specifies that they must not use their position to seek undue benefits or harm the interests of the company, and must not obtain undue benefits through false statements or other unfair trading methods based on information obtained through their job. To prevent unethical behavior, The CyberPower "Work Rules" clearly regulates that if any employee involves in acts of embezzlement, unauthorized utilization of company funds, acceptance of bribes or commissions, substantiated by concrete evidence" in a severe way, the employment relationship can be terminated without prior notice. Furthermore, the company has formulated the "Codes of Ethical Conduct" based on the Ethical Corporate Management Principles to guide employees in carrying out their duties and activities with ethical standards and behavior norms.

In accordance with the "Ethical Corporate Management Principles" and "Codes of Ethical Conduct," CyberPower has implemented an annual self-declaration of employee interest avoidance on the Human Resource Management system. In Taiwan, a total of 371 questionnaires were distributed in 2024, with 14 employees reporting conflicts of interest. The reported conflict situations were categorized as either insignificant, exempt from competition prohibition, or involving direct supervision over the relevant business.

Anti-corruption and Anti-bribery Policies

CyberPower advocates for integrity in business operations and adheres to high ethical standards in all business activities. We take a zero-tolerance approach toward corruption and bribery and have established relevant policies for ethical management. Clear guidelines against corruption and bribery have been established, and we provide communication and training to employees and business partners to help prevent bribery and corrupt practices, including the prohibition of gifts from suppliers and customers, especially during holidays.

Communication on Anti-corruption Policies and Procedures

Category	Communication Channels / Methods	Number of People (Companies) Reached	Percentage
Governance Units[Note 1]	Email Announcement	All (7 People)	100%
Employee	Email Announcement	All (385 People)	100%
Business Partners[Note 2]	Notice of the Integrity Clause in the "Procurement Agreement"	All (441 Companies)	100%

Note 1: The governance unit includes members of the Board of Directors; the employee category includes all CyberPower employees (including the Tainan factory).

Note 2: Business partners include the new suppliers to whom Cyber Power Systems, Inc. (284 companies) and its main production base, Cyber Power (Shenzhen) Ltd (193 companies), have sent "Procurement Agreements."

CyberPower conducted a 100% risk assessment of unethical behavior (including corrupt practices) across all divisions in 2024, evaluating the business activities within the scope of business that have a higher risk of unethical behavior. Based on this assessment, preventive measures were formulated to prevent unethical behavior. The result of the risk assessment for 2024 is low and within the tolerable range. There were no actual cases of corruption, no employees were disciplined or terminated, and no business partners had their contracts terminated or not renewed due to corruption.

Legal Compliance

Complying with legal regulations and operating legally and ethically are the most fundamental responsibilities of a company and are crucial to its long-term sustainability. CyberPower ensures that its operations comply with local regulations by closely monitoring any regulatory changes or updates that may impact the company. The company also conducts regular compliance assessments based on the "Legal Compliance Regulations" to ensure that each unit's operations align with relevant requirements and standards.

CyberPower regularly self-evaluates the implementation effectiveness and efficiency of the internal control system. Each unit completes the self-assessment and provides relevant information at the beginning of every year. After being reviewed by the Audit Office, the Board of Directors and the president evaluate the effectiveness of the overall internal control system and issue a statement. The statement is available on the Market Observation Post System (MOPS).

In the event of significant occurrences that substantially impact our operations — defined as a single event where fines exceed NT$1 million or an event that could cause considerable damage to operational performance and reputation — such events must be disclosed in the Sustainability Report. This ensures adherence to our principles of transparency and compliance with the GRI standards' requirements for balanced reporting. In 2024, we did not incur any fines or penalties due to major violations of laws or regulations.

Legal Compliance Training

To provide immediate assistance and consultation services related to legal and regulatory matters to all departments, we maintain an internal announcement platform managed by a dedicated team, where employees can access relevant information and educational materials. Meanwhile, we have long-term partnerships with professional and reputable legal firms and consultants to ensure compliance with laws and regulations through legal advisors. The responsible departments regularly conduct educational training sessions on various regulations, create FAQs, and disseminate information through announcements. These efforts ensure that our employees are well-informed and up –to date on the latest regulations, helping them review and update their practices to avoid unintentional violations. This also strengthens their awareness of legal compliance and ethics, reinforcing the fundamental social responsibility of our company

Legal Compliance Training Overview

Training Course	Objective and Benefits	Training Participants	Duration	Participation Rate
Preliminary Assessment of Patent Infringement	To enhance the ability of R&D and related staff to make preliminary assessments of potential patent infringement risks, helping to identify potential disputes early, avoid legal and financial losses, and strengthen patent awareness during product development.	178 employees from R&D-related departments	1 hour	92.7%

Complaint and Suggestion Channels

Integrity and responsible business practices are the foundation of a company's sustainable operation. CyberPower has established various complaint and suggestion channels to encourage stakeholders to report, file complaints, or provide suggestions regarding dishonest, unethical behavior or any business activities that may cause environmental, economic, social, and human rights impacts. When an employee engages in unethical behavior, the company will warn or discipline the employee based on the severity and impact of the incident in accordance with the "Employee Reward and Punishment Policy." The company does not tolerate corruption or any form of fraudulent behavior. If anyone discovers a violation of laws, regulations, or ethical codes, they can provide sufficient information to report to the following units: 1. department supervisor; 2. The head of Audit Office, Human Resource Department, or Legal Department; 3. corporate internal reporting system. The company will assign the Audit Office to investigate the case based on the circumstances. The investigation process and related information of the relevant parties are kept confidential at all times, and the progress of the case will be reported to the Chair.

The reporting channels are listed on the Official Website. Internal concerns from employees can be appealed via the Audit Office, the employee appeal mailbox, or the sexual harassment hotline managed by the Human Resource Department. Complaints can also be reported to the Audit Office or through the employee reporting mailbox at fairdeals@cyberpower.com (which also serves as the supplier's Integrity reporting mailbox). External channels include the investor relations mailbox at investor@cyberpower.com on the Official Website. Reports involving senior executives or directors can be made through an independent reporting mailbox at tellus@cyberpower.com. Every reported case will be investigated promptly, with progress reported to the Chair.

Employee appeals and report information will be investigated according to internal control procedures, and the Audit Office will be instructed to investigate related matters in a confidential manner. The investigation and whistleblowers' personal and reporting information will remain confidential to protect whistleblowers, unless the law requires the disclosure of such information. CyberPower will take appropriate legal measures to ensure the whistleblowers and information are protected. Should any illegal (including corruption) and immoral behavior be revealed with reasonable proof, CyberPower considers it a serious violation of company policies and local regulations, and will handle the case in accordance with company policies and local laws. In 2024, we did not receive any reports.

Risk Management

Risk Management System

CyberPower continues to identify and respond to various risk scenarios that may impact business operations through cross-departmental collaboration. Each responsible department regularly reviews and assesses potential risks within its area of responsibility and implements suitable measures. Risk identification has been embedded into daily departmental operations and is integrated with internal control and audit mechanisms to enhance consistency and effectiveness in response measures.

The Finance & Accounting Division consolidates the company's risk management practices and performance annually, in accordance with corporate governance regulations, and reports the findings to the Board of Directors. This ensures that the governance level remains informed of the overall risk landscape and emerging trends. The 2024 report covered key issues including information security, intellectual property rights, sustainability management, and ethical management. Through Board oversight, the company continues to enhance its risk management maturity and strengthen its overall risk response capabilities.

Risk Management Process

External Regulatory Requirements	Internal Policy Development	Execution by Responsible Departments	Governance Reporting	Continuous Improvement
• Based on the corporate governance code and regulations set by the competent authorities.	• Internal management policies are established to address various risks.	• Responsible departments implement the internal policies accordingly.	• The Finance & Accounting Division consolidates execution results and operational status and reports to the Board of Directors.	• Each responsible department adjusts practices and countermeasures according to actual implementation. • Integrating internal controls, audits, and self-assessments into daily management systems.

Risk Management Strategy

Risk Impact, Response Strategies, and Actions

Risk Type	Causes of Risks	Response Strategies and Actions	Responsible Unit
Strategic and Operational Risks	• Decrease in supply and increase in price of raw materials due to climate change • Regulatory and reputational risks arising from government regulations and international initiatives regarding carbon emissions	• Continuously invest in R&D and innovation to develop new products and improve existing products to compete for the company's sustainable development • Regularly visit key customers and maintain strong communication to stay updated on market trends, while providing advanced technology to meet evolving demands	President Office Operations Management Division Logistics Management Division
Market Risks	• Supply chain management risks caused by the rising awareness of human rights and environmental protection • Risks associated with supply chain violations of government regulations	• Identify functions that competitors have overlooked and accelerate the development of new products • Due to energy supply tensions and logistics instability resulting from the Russia-Ukraine war, the Procurement and Product Departments have collaboratively developed a one-year procurement strategy in advance to ensure price stability and continuous supply. • Diversification of manufacturing bases to minimize risks due to global power competition, related policy restrictions, tariffs, and other control measures	Finance & Accounting Division Operations Management Division Logistics Management Division

Risk Type	Causes of Risks	Response Strategies and Actions	Responsible Unit
Financial Risks	• Interest rate risk arising from credit loans • Risk of delayed or non-payment by customers due to economic conditions • Cash liquidity risk • Exchange rate risks arising from being a multinational company or frequent transactions with foreign companies	• Analyze interest rate risk and simulate multiple improvement options, such as refinancing or other financing methods, to calculate the impacts of specific interest rate changes on profit and loss • Conduct credit risk management analysis on customers, evaluating their credit quality, and taking out appropriate insurance to transfer the related risks • Monitor cash flow requirements to anticipate and ensure that the company has sufficient funds for operations. • Due to the uncontrollable factors of exchange rates, adopt the real-time online exchange rate system and strengthen the connection with financial institutions to study the trend of exchange rate, serving as a reference for foreign exchange trading and settlement, and reducing exchange rate risks	Finance & Accounting Division
Regulatory Risks	• Risks associated with government regulations on related industries, such as wastewater, waste discharge, or restrictions on raw materials	• Pay attention to the latest amendments to laws and regulations that may affect the company, and continuously improve internal processes to ensure compliance	Relevant Responsible Departments
Climate Change Risks	• Decrease in supply and increase in price of raw materials due to climate change • Regulatory and reputational risks arising from government regulations and international initiatives regarding carbon emissions	• Reduce costs by importing raw materials from multiple regions • Obtain ISO 14001 Environmental Management System and introduce greenhouse gas (GHG) inventory, use energy-saving equipment, and improve carbon reduction measures	Procurement Department Administration Department
Supply Chain Management Risks	• Supply chain management risks caused by the rising awareness of human rights and environmental protection • Risks associated with supply chain violations of government regulations	• Conduct an annual assessment of primary suppliers as the basis for risk management and perform both documented and on-site audits • In addition to the quality, price, and delivery of the suppliers' products, focus on their capabilities, environmental and safety certificates, to avoid production interruption risk due to major ecological or safety accidents • If a supplier violates the relevant laws or initiatives, provide counseling and set a deadline for improvements to determine whether to continue the cooperation	Procurement Department
Occupational Safety Risks	• Accidents caused by insufficient disaster prevention awareness • Safety risks caused by hardware equipment in the company's buildings or facilities	• Conduct regular annual inspections of the work environment, as well as safety training and fire drills • Regularly inspect the company's hardware equipment (e.g., buildings, electrical equipment, etc.) to ensure they are in good condition, and purchase public liability insurance with a maximum coverage of US$10 million for the office to further protect the workplace	Administration Department
Information Security and Personal Data Risks	• Damage, leakage, or loss of confidential information (including physical data) • Risk of hackers attacking external websites or internal systems to steal confidential information	• Servers, firewalls, virus updates, and other operations in the server room should be inspected by information security professionals and reviewed by the IT supervisor to ensure that all inspection items are properly executed • Regularly back up all programs and data files, and automatically execute scheduled snapshot backups of storage devices every day • Engage external information security consultants to provide improvement suggestions and to assist in the implementation of information security solutions • External information security consultants conduct security awareness training for all employees through both in-person and online sessions, and carry out annual social engineering drills to strengthen overall awareness of security risks	Information Management Division

Information Security

2024 Material Topic: Management of "Information Security"

Material Topics	Information Security
GRI Standards	GRI 418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data
SDGs	
Policy or Commitment	Build a corporate culture centered on customer trust and information security, ensuring full protection of customer privacy and swift, effective response to any data breaches, thereby minimizing damage and restoring customer confidence to the greatest extent possible
Indicators and Goals	Short-term Goals (1-2 years) • Develop and update policies, including "Information Security Management Measures" and "Control Measures for Information Security Inspections" • Conduct annual information security training for employees and hold social engineering drills for all employees twice a year • Establish a complaint handling mechanism with a dedicated team for investigation and resolution Mid-term Goals (2-5 years) • Deploy information security technologies, including data encryption and the enhancement of data security • Implement a monitoring system for real-time tracking of data access to detect risks promptly • Review and improve response strategies based on experiences from drills and simulated incidents Long-term Goals (5+ years) • Establish a collaboration mechanism by joining the Taiwan Computer Emergency Response Team (TWCERT/CC) to share and cooperate in addressing information security challenges • Regularly review and update privacy policies and security regulations to maintain robust protections
Effectiveness Tracking Mechanism	• Regular Evaluation: Evaluate progress toward goal achievement every quarter or every 6 months • Monitoring Metrics: Set performance indicators, such as tracking employee training participation rates and response times for security incidents • Problem Resolution Mechanism: Create a system to track and resolve issues promptly during strategy implementation • Continuous Improvement: Establish a feedback mechanism to summarize experiences from complaints, employee feedback, and monitoring data, and continuously improve execution strategies
Annual Actions and Measures	• Establish emergency response plan and team • Conduct regular drills • Implement risk-monitoring mechanism • Enhance communication and transparency • Continuous monitoring and improvement • Completed 2 information security maintenance measures • Conducted 2 social engineering drills to boost employee awareness • Provided a information security training for all employees • Held a security awareness campaign with a total of 319 participants in both in-person and online 1-hour session

Information Security Policy

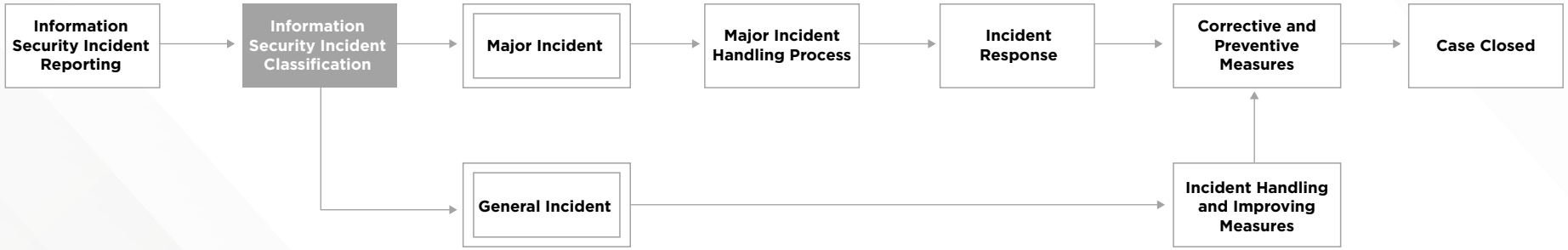
To strengthen the protection of information assets and enhance operational resilience, CyberPower has designated the System Architecture Department to oversee information security management. This department is responsible for establishing information security governance policies, supervising the implementation of security measures, promoting employee training and awareness, and regularly assessing security risks. Overall performance is reported directly to the President. The scope of information security primarily covers IT services managed by the Information Management Division, as well as other relevant departments across the company. CyberPower continuously conducts vulnerability scanning, security system audits, penetration testing, abnormal behavior analysis, and data backup procedures, thereby establishing a multi-layered defense framework through institutionalized mechanisms.

In accordance with the "Information Security Management Measures" and the company's internal information security management policies, CyberPower has proactively implemented a compliant Managed Detection and Response (MDR) system for endpoint detection and response. The company's information security policies are reviewed regularly to ensure alignment with regulatory requirements and evolving technology trends. Additionally, with guidance from external information security consultants, the company conducts penetration testing, social engineering drills, graded incident reporting, and abnormal log management. These measures ensure that the company's information security management is equipped with early warning, prevention, response, and recovery capabilities.

Operating Procedure for Information Security

To effectively prevent and handle information security incidents, CyberPower has established an incident reporting procedure that clearly differentiates between major and general security incidents, with corresponding response protocols based on the type of incident. When an information security incident occurs, the Information Management Division follows standardized procedures for reporting, documentation, and initial response, and conducts further investigation and corrective actions depending on the nature of the incident. When necessary, a cross-departmental response team may be convened to coordinate the resolution, ensuring information risk control and uninterrupted operations. In 2024, the company reported no information security incidents, demonstrating the effectiveness of its overall security management mechanisms.

Information Security Incident Workflow



Information Security Management Program

In accordance with its information security policy, CyberPower implements protective measures for its information assets. Security controls are established separately for files and equipment, covering aspects such as information access, data backup, system updates, and facility management. These measures ensure the confidentiality, integrity, and availability of the information processing environment. All operations are conducted by the Information Management Division following established procedures and are regularly audited and inspected to ensure compliance with the policy.

Category	Content
Security Controls for Files	• Information security professionals regularly inspect the update status of servers, firewalls, and antivirus software. The results are reviewed by the IT supervisor. • Access to the server room is strictly controlled through authorization. Unauthorized personnel must obtain approval from IT staff and be accompanied during entry. All entries and exits are recorded in an access control log. • All information systems require account registration and approval before use. Users must set a password, and password confidentiality is strictly enforced. • Various types of storage media must be regularly backed up, including system programs and data files. Backup copies are stored monthly at a secure offsite location and clearly labeled. • A server-client antivirus architecture is adopted, with centralized updates and virus scans performed by the server. This helps prevent data tampering and system intrusions.
Security Controls for Devices	• Smoking, eating, and bringing in non-business-related items are strictly prohibited in the server room. The facility is equipped with fire protection, air conditioning, dehumidification, and access control systems to minimize physical risks. • All vendors, maintenance personnel, or visitors entering the server room must be accompanied by IT staff. Entry and exit times, purposes, and personnel information must be recorded. • The server room environment and operational safety are reviewed regularly to ensure stable and secure operation of information equipment.

Information Security Advisory

To enhance information security governance and operational maturity, CyberPower has engaged external information security consultants since 2020 for professional guidance. The company has continuously implemented various security maintenance measures, including systematic vulnerability assessments, incident response simulations, and abnormal behavior analysis. These initiatives aim to strengthen the company's capabilities in risk early warning, defense, and response, while ensuring that the current security management mechanisms comply with the latest regulations and industry standards. The achievements of these consulting engagements and implementations in 2024 are as follows:

Maintenance Measures	Implementations	Performance Results and Future Plans
Penetration Test	• Conducted 1 standard penetration test during the testing period • Performed a gray-box Dynamic Application Security Testing (DAST) • Conducted a comprehensive inspection following OWASP standards • Provided a compliant website commercial tool report with recommended vulnerability remediation	Annual penetration testing and vulnerability scanning are conducted regularly to strengthen the protection of hosts and systems, thereby reducing the risk of cyberattacks.
Information Security Consultant Interviews (Quarterly, Total 4 Times in the Reporting Year)	• Planning of authorization and access control processes • Monitoring and interpretation of network layer / host layer IDS • Server room risk assessment and internal controls • Learning, monitoring, and warning of abnormal behavior • Monitoring and optimization of network and host security • Planning of backup and disaster recovery strategies	Providing domestic and international information security trends and case studies as a basis for adjusting security strategies, thereby enhancing overall defense and response capabilities.
Social Engineering Email Drills	• Completed 2 social engineering drills to enhance employee awareness of information security • Conducted information security awareness courses following the drills • Ran situational phishing email drills • Performed in-depth analysis of information security awareness	Helps the company identify and address issues and vulnerabilities related to email security, thereby enhancing vigilance and strengthening defenses against social engineering attacks.
Log Management and Real-Time Abnormal Analysis Platform	• Server and network equipment log recording and analysis • Warning of enterprise data leakage in Layer 7 services • Domain Server Log Collection and Storage • Warning of significant harmful commands (Cmd) • Verified the effectiveness of enterprise information security equipment investments • Completed information security event log traceability	Establish a comprehensive information security incident trail to enhance real-time monitoring and traceability, with plans to implement automated response capabilities in the future.
Threat Event Response Evaluation	• Scope: CyberPower EDR / MDR systems • Evaluation of significant accidental threats • Evidence collection from compromised hosts during events • Rapid screening of affected hosts • Evaluation of the scope of threat events • Evaluation report of the threat event response results	The detection and response capabilities of security incidents are enhanced through behavioral analysis of anomalous trajectories, helping to reduce potential security risks and losses.

Information Security Education and Training

CyberPower, in compliance with the "Information Security Management Measures" and internal information security policies, continuously enhances employees' awareness and response capabilities through training and simulation exercises. In 2024, the company conducted 1 training session and 2 social engineering drills. The courses combined theoretical knowledge with practical case studies, covering topics such as hacker techniques analysis, social engineering alerts, and key information protection measures. These efforts aimed to improve employees' risk identification and response capabilities in daily operations. The training participation rate reached 85.01% in 2024, with an average test score of 93.15, demonstrating the ongoing effectiveness of information security awareness initiatives.

Information Security Training Status in the Past 3 Years

Year	Training Courses	Course Objectives and Benefits	Trainees	Training Hours	Participation Rate
2022	Information Security Awareness Training - I	Data fraud, theft, and cyberattacks are among the most critical risks that companies must address. It is essential for all employees to cultivate strong information security awareness to protect both company and personal data from compromise.	All employees (343 participants)	1 hour	93.29%
	Information Security Awareness Training - II	By analyzing real-world global cases, we examine the latest cyber attack methods and psychological tactics to help employees better understand that information security risks are present in everyday life. They should approach and handle these situations with heightened caution.	All Employees (342 participants)	1 hour	93.56%
2023	Information Security Awareness Training	By analyzing real-world global cases, we examine the latest cyber attack methods and psychological tactics to help employees better understand that information security risks are present in everyday life. They should approach and handle these situations with heightened caution.	All Employees (364 participants)	1 hour	87.63%
2024	Information Security Awareness Training	Enhance information security defense capabilities by incorporating real-world case studies and simulated attack scenarios to help employees understand hacking techniques, sources of cyber threats, and the critical responsibilities and actions required at both individual and organizational levels.	All Employees (367 participants)	1 hour	85.01%

Note: The participation rate is calculated based on the number of employees on duty for the month.

Ongoing Efforts in Information Security Awareness Campaigns to Reinforce Response Capabilities and Proactive Actions

To deepen employees' information security awareness, CyberPower continued to foster a security-conscious culture in 2024. The company organized a dedicated awareness session focused on the risks associated with generative AI tools and case studies of social engineering scams. The session was delivered in a hybrid format (both in-person and online) with a total of 312 participants. The one-hour course aimed to help employees develop the appropriate mindset and behavioral guidelines for responding to digital threats.

Social engineering drills were continuously updated to reflect current information security trends, simulating realistic phishing email attack scenarios. Through pre-exercise briefings and post-exercise feedback, the company enhanced employees' ability to recognize and report suspicious emails. These efforts also contributed to building a culture of mutual vigilance and shared responsibility for information security. The results were significant—most employees actively reported suspicious messages during the drills, and overall accuracy and awareness have improved year over year, effectively reducing the risk of potential social engineering attacks.

Information Security Awareness Test Results in the Past 3 years

Item	2022	2023	2024
Number of Participants	343	364	367
Average Score	91	93.7	93.15

Personal Information Management Policy

CyberPower places great importance on protecting the company's confidential information, trade secrets, as well as the personal data of employees and customers. In addition to consistently complying with the "Personal Data Protection Measures" and other relevant domestic and international regulations on information security and privacy, the company has implemented comprehensive measures to strengthen information operations management and protective capabilities, along with dedicated mechanisms for safeguarding confidential information. Specific actions include:

- Enhancing employees' awareness and compliance with confidential information and personal data protection regulations through regular internal communications and educational campaigns
- Including information security and confidential data management as part of mandatory training for new hires, and continuing in-service training to enhance awareness and risk prevention in data handling
- Promoting proper information usage practices, such as locking screens when away from seats and enabling password protection, to prevent unauthorized access to sensitive information
- Conducting regular inspections by the Information Management Division on personal data servers to detect any intrusions or abnormal access records, and reinforcing access control measures for the server room to prevent data leakage incidents

Product Information Security

In addition to power protection products, CyberPower has actively developed and provided the PowerPanel Cloud service in recent years to meet the growing global demand for cloud solutions. This service enables users to remotely manage devices via the cloud system. PowerPanel Cloud incorporates robust security controls and comprehensive data protection measures. The key information security measures include:

Data Availability and Integrity	Strengthen and Consolidate Data Transmission	CREST Certifications
• Data Storage: Implementing data backup and recovery procedures • Data Processing: Complying with international standards such as the ISO 27001 Information Security Management System and ISO 27018 Protection of Personally Identifiable Information (PII) in Public Clouds, while regularly tracking and auditing the cloud system configurations	• Encrypting data using a hash key verification algorithm to ensure data integrity and security • Adopting one-time passwords (OTP)	• Adhering to the highest information security standards set by International financial institutions (IFIs) • Conducting regular system penetration testing



04 Product Innovation and Service

Innovation and Research
Product Quality
Customer Service

Innovation and Research

2024 Material Topic: Management of "Innovative and Research"

Material Topics	Innovation and Research
GRI Standards	Custom Material Topic
SDGs	 
Policy or Commitment	Gain a deep understanding of users' needs to develop products that are aligned with market trends, while focusing on the user experience to meet customers' expectations and requirements. Establishing a rigorous quality control system ensures that products meet standards to maintain the company's image and customer trust.
Indicators and Goals	Continuing Goals: • Invest at least 5% of total revenue in research and development (R&D) each year • Develop new technologies and products to enable continuous market growth Mid- to Long-term Goals: • Implement "sustainability" in product design, for instance, the use of raw material, product efficiency, and eco-friendly packaging design • Become a leader in power solutions
Effectiveness Tracking Mechanism	• Supervisors of product teams hold monthly meetings to align product development direction • Product teams meet regularly to ensure development progress • Regularly review customer feedback and satisfaction levels • Periodically check and evaluate key metrics and variables in the production process
Annual Actions and Measures	• The R&D investment was NT$395,626,000 • 5 new patents were obtained, bringing the total number of valid patents to 304 • Smart App Sinewave Lithium Battery UPS was awarded CRN's Tech Innovators, PFC Sinewave 1U Rackmount UPS was on the shortlist for CRN's Products of the Year, and CyberPower was recognized on CRN's Edge Computing 100 list

Five Major Goals of Innovation and Research


Enhance Performance


Strengthen Durability


Improve Aesthetics


Increase Efficiency


Reduce Environmental Impact

CyberPower places great importance on brand value and is committed to the development of products and long-term investment in core technological capabilities, to launch products that meet consumers' needs. We continue to develop new products and improve existing ones to establish a technological foundation for sustainable development. In 2024, our R&D expenses reached NT$395,626,000, accounting for 5.23% of the company's revenue, and we obtained 5 new patents, bringing the total number of valid patents to 304.

R&D Investment in the Past 3 Years

(Unit: NT$ Thousand)

Year	2022	2023	2024
Amount of Investment	359,334	365,663	395,626
Proportion in Revenue	4.52%	5.29%	5.23%

Patent Acquisition in the Past 3 Years

Country		Taiwan	China	USA	Germany	UK	Total
New Patents	2022	2	5	5	1	0	13
	2023	5	6	1	0	0	12
	2024	1	0	4	0	0	5
Cumulative Valid Patents		66	60	98	2	1	227

The strength of the brand's growth comes from a solid R&D foundation and innovative products. From the beginning, CyberPower established an R&D department focusing on technology research and product development, and currently, there are 7 R&D departments dedicated to different product lines. In addition to R&D departments for each product line, we have also independently developed DCIM, a data center power management system, and the cloud platform for power management, effectively enhancing the value of our products and providing comprehensive power management solutions to the market.
Furthermore, to improve engineers' technical proficiency and accelerate development speed, we have set up a safety laboratory and a fully anechoic chamber measuring 7m x 4m x 3m, helping R&D specialists monitor the product development progress anytime.

Highlights of Products in the Past 3 Years



PFC Sinewave (E)
The short-depth rackmount UPS for equipment requiring active PFC power source

Energy Saving Technology	Active PFC Compatible	Automatic Voltage Regulation (AVR)	Surge and Spike Protection	Hot-swappable Batteries



Online (High-Density)
The high performance online double-conversion UPS supplies optimal power and functionality with compact design

ECO Mode	High Density Design	High Output Power Factor	Battery Management Technology	Quick Charging Technology



Online S (Premium)
The online double-conversion UPS with built-in Remote Cloud Card for easy remote monitoring and management

ECO Mode	High Output Power Factor	Adjustable Charging Current	Maintenance Bypass Switch	Built-in Remote Cloud Card by Ethernet



Online S (Advanced)
The online double-conversion UPS with tiltable color LCD panel and Extended Battery Module auto-detection for efficient power management

ECO Mode	High Output Power Factor	Adjustable Charging Current	Extended Battery Module Auto-detection	Color LCD Panel

Highlights of CyberPower's Products in the Past 3 Years



Online (3-Phase)

Trustworthy battery backup with color LCD touch screen while supporting parallel expansion

ECO Mode	Color LCD Panel	LCD Touch Panel	UPS Parallel Expansion	Remote Management Capability



Modular UPS (3-Phase)

The 3-Phase Modular UPS with N+X redundancy design and high-density power modules for mission-critical applications

ECO Mode	High Density Design	Vertical Scalability	Flexible Installation Design	Color LCD with Touch Panel



Remote Management Card

The SNMP card allows users to monitor and manage UPS to perform remote management

1Gbps High-speed Data Transmission	Plug-and-play Installation	Command Line Interface Supported	Remotely Schedule Shutdown / Start-up / Reboot of the UPS	Automatic Event Notifications

Highlights of CyberPower's Products in the Past 3 Years



Grid-tied Inverter (3-Phase)

Intelligent 3-phase grid-tied inverter to provide solar energy and make profits by selling power

Work with Solar Panels	High DC to AC Energy Efficiency	Maximum Power Point Tracking	LCD Status Display	IP66-rated Waterproof Enclosure



Hybrid PV Inverter

The integrated hybrid PV inverter provides a perfect total solution for PV and battery energy management

Optimized Self-consumption Design	High DC to AC Energy Efficiency	Dual Independent MPP Trackers	Emergency Power Supply (EPS)	Terra Online Power Monitoring Platform



All-in-one Off-grid Inverter

Green solution for energy storage and reduced grid dependence

Generator Compatible	Built-in MPPT Charge Controller	Work with Solar Panels	Automatic Voltage Regulation (AVR)	Color LCD Panel

Green Products and Services

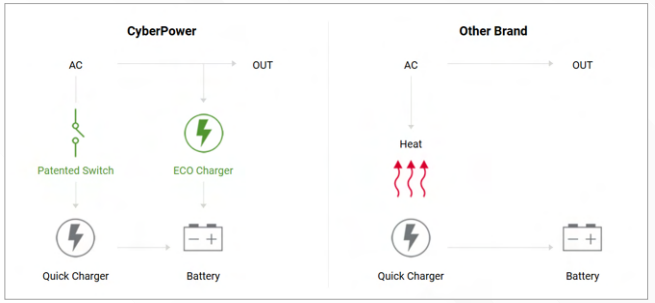
CyberPower specializes in the research and manufacturing of power protection and management systems, continuously striving for excellence in power quality and operational efficiency of products, as well as maintaining our commitment to the development of energy-saving technologies. After years of relentless effort, we have become an internationally recognized leader in the field of green UPS systems, possessing patented energy-saving technologies and offering energy-efficient products to users.

GreenPower UPS™ Technology

CyberPower's patented GreenPower UPS™ technology can reduce UPS energy consumption while improving its operating efficiency and reducing heat generation, resulting in significant energy cost savings compared to conventional UPS models. This patented technology includes two innovative designs:

- High-efficiency Design: It features advanced, compact, and energy-efficient inverters and chargers in place of conventional UPS designs, which can significantly enhance the UPS system's power efficiency and reduce its power consumption.
- Bypass Circuit Design: When the battery is fully charged, the bypass switch automatically disconnects the quick charger, preventing unnecessary power consumption of UPS.

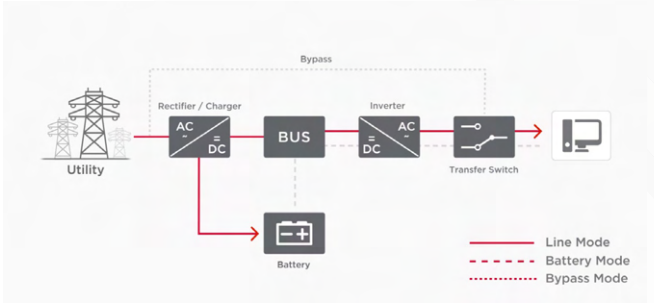
Under the same test environment and procedure inspected by SGS, the UT1050EG UPS from CyberPower's UT series reduces its energy consumption by up to 93% compared to other brands. This series significantly enhances energy efficiency and reduces carbon emissions while maintaining outstanding power protection and system stability.



ECO Mode

Some of CyberPower's advanced UPS systems feature ECO mode, which automatically adjusts the operation mode based on the quality of utility power, helping increase UPS efficiency. In the event of unstable utility power, the UPS system switches to line mode to ensure optimal power quality and protection. When the utility power is stable, the UPS system transfers to ECO mode, reducing UPS power consumption and energy costs greatly.

The OL12KRTHD UPS from CyberPower's Smart App Online (High-Density) series can increase UPS efficiency by up to 98.4% in ECO mode, reducing its energy consumption.ment.



ENERGY STAR Certification

ENERGY STAR is the US government-backed symbol for energy-efficient products, aiming to help businesses and individuals protect the environment and save on electricity bills by using energy-saving products. Receiving the ENERGY STAR certification means that the product meets the strict energy conservation standards of the U.S. Environmental Protection Agency. According to its official website data, ENERGY STAR-certified UPS systems can reduce energy losses by 30-55%, helping users conserve energy.

By 2024, 99% of CyberPower's ENERGY STAR-certified UPS systems exceeded the ENERGY STAR UPS standard. For instance, the OL2K2RTHDL UPS exceeds the ENERGY STAR efficiency requirement by 1.8%, saving energy costs and protecting the environment.

Eco-friendly Product Packaging

In addition to focusing on the development of energy-efficient products, CyberPower also actively implements green design and reduced-plastic packaging, aiming to minimize environmental impacts during product transportation. While ensuring transportation safety, we are gradually replacing traditional packaging materials with 100% recyclable alternatives, balancing product protection, logistics efficiency, and resource sustainability.

The Results of the Implementation of Eco-friendly Packaging

Product / Service	 UPS System (CST135UC2)	 Before New Universal Power Supply (CPUAC1U1300)	 Intelligent Management Solution (Including network management cards and sensors)
Implementation	• Replacing polystyrene with 100% recyclable molded pulp significantly reduces polystyrene usage and the product volume • Some of the package materials are sourced from the place of origin, reducing carbon emissions from transportation	• Replacing plastic packaging with paper drastically reduces plastic usage	• Replacing blister packs and cushioning materials with 100% recyclable molded pulp
Result	Based on the total shipment volume in 2024, an estimated reduction of 9,187.2 kg of polystyrene usage was achieved in one year.	Based on the total shipment volume in 2024, an estimated reduction of 3,157.38 kg of plastic usage was achieved in one year.	Based on the total shipment volume in 2024, an estimated reduction of 522.92 kg of plastic usage was achieved in one year.

Product Quality

2024 Material Topic: Management of "Product Quality"

Material Topics	Product Quality
GRI Standards	GRI 416-1 Assessment of the health and safety impacts of product and service categories GRI 417-1 Requirements for product and service information and labeling
SDGs	
Policy or Commitment	Adhering to the business philosophy of commitment to technology, customers, and employees, we strive to further enhance product quality and increase customer satisfaction with a pragmatic and excellence-driven approach. This will empower CyberPower to move forward with determination from a new starting point.
Indicators and Goals	Continuing Goals (Short-, Mid-, and Long-term): • Improve product quality through regular management system verification, prioritizing customer health and safety to ensure the delivery of safe and reliable products • Maintain a global customer satisfaction rate of over 90% in the short term, reduce the dissatisfaction rate to below 5% in the long term, and increase overall satisfaction rate to 95-97% • Continuously conduct quality issue analysis and testing, along with quality management, to reduce the product defect rate year by year
Effectiveness Tracking Mechanism	• Continuously maintain the quality management systems, including ISO 9001 and ISO 14001, and meet certification standards to ensure effective quality management • Evaluate future product improvements and R&D directions through customer satisfaction surveys • Apply for relevant certifications and labels to ensure that each product complies with local regulations and performance standards • Implement comprehensive quality management with rigorous IQC, IPQC, FQC, QE, OQC quality inspection standards and methods
Annual Actions and Measures	• Manufacturing sites have passed multiple third-party certifications, including ISO 9001, ISO 14001, QC 080000, TL9000, etc. • Main products have obtained various safety certifications, such as BSMI, UL, TUV Rheinland, ETL, Energy Star, etc. • All products comply with health and safety regulations and voluntary standards, with no incidents of hazardous substances exceeding permissible levels • There were no incidents of non-compliance concerning product and service information and labeling

Quality Management Policy

CyberPower values product quality and users' health and safety. Therefore, substantial resources have been invested in establishing quality management systems from product development, production, transportation, sales to product use. The company is certified by an independent third-party for the ISO 9001 Quality Management System, ensuring consistency and traceability in quality management processes.

According to the management system and departmental responsibilities established in the "Quality Manual," the Quality Control Center collaborates with R&D, Manufacturing, Procurement, and Warehousing units to jointly implement supplier management, incoming inspection, process monitoring, self-inspection, and final product inspection, maintaining comprehensive quality control from the source to final product delivery. In addition, internal audits, management reviews, and customer satisfaction surveys are conducted regularly to assess and continuously improve quality performance indicators, confirming the system's appropriateness and effectiveness.

To protect user health and environmental safety, CyberPower implements a strict hazardous substances control policy. All products comply with the EU Restriction of Hazardous Substances Directive (EU RoHS), the Registration, Evaluation, Authorization and Restriction of Chemicals (EU REACH SVHC), and the Waste Electrical and Electronic Equipment Directive (WEEE), meeting the requirements of the Packaging and Packaging Waste Directive (Directive 94/62/EC), dual certifications for ISO 14001:2015 Environmental Management System and IECQ QC 080000 Hazardous Substance Process Management System, confirming that both raw materials and recycled components are environmentally safe. In 2024, none of the company's main products were found to violate health and safety regulations or voluntary standards, demonstrating our commitment to product quality and sustainability.

Quality Management Process

CyberPower has established a comprehensive quality management process, from policy planning to oversight and improvement based on ISO 9001, TL9000, and IECQ QC 080000 management systems. The management team sets the quality policies and objectives, integrating risk management and internal audit mechanisms to lay the foundation for the quality system. During the development and supply stages, product design reviews, FMEA (Failure Mode and Effects Analysis), and supplier evaluations are conducted to ensure the quality of both products and incoming materials. The manufacturing process follows standardized operating procedures, supported by automated monitoring and equipment maintenance, to uphold process stability.

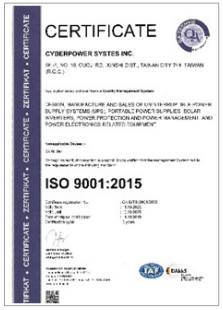
All products undergo four stages of inspection, including material buy-in, production, final processing and shipment, to reinforce consistency and reliability. Customer feedback and anomalies are addressed through 8D (Eight Disciplines) analysis and corrective and preventive actions, driving continuous improvement. Finally, system performance is continuously monitored through internal audits, management reviews, and external audit results. Findings are reported back into the quality policy and objectives, forming a PDCA (Plan-Do-Check-Act) cycle that strengthens the company's quality culture and sustainability management practices.

Quality Management Process Flow Chart



International Certifications of Quality Management

ISO 9001:2015 Quality Management System



Cyber Power
Tainan Factory



Cyber Power
(Shenzhen) Ltd



Dongguan
Cyber Energy Co., Ltd.



Cyber Power Systems
Manufacturing, Inc.

IECQ QC 080000:2017 Hazardous Substance Process Management



Cyber Power
(Shenzhen) Ltd

TL9000 Telecommunications Industry Quality Management Systems



Cyber Power
(Shenzhen) Ltd



Cyber Power Systems
Manufacturing, Inc.

Valid Safety Certifications of Main Products

Region	Certification		Type	Category
Taiwan	BSMI	Bureau of Standards, Metrology and Inspection	Safety / EMC / RoHS	Mandatory
European Union	CE	EU Mandatory Certification Mark	Safety / EMC / RoHS	
USA	DOE	DOE Certification	Efficiency	
Eurasian Economic Union	EAC	Eurasian Conformity Certification	Safety / EMC	
USA	FCC	Federal Communications Commission	EMI	
Canada	IC	Innovation, Science and Economic Development Canada	EMI	
Mexico	NOM	Mexican Official Standard Certification	Safety	
Australia / New Zealand	RCM	RCM Mark	Safety / EMC	
United Kingdom	UKCA	UK Conformity Assessment Mark	Safety / EMC / RoHS	Voluntary
USA	ENERGY STAR	ENERGY STAR	Efficiency	
Germany	GS Mark	German Safety Certification	Safety	
USA / Canada	Intertek ETL Listed	Nationally Notarized ETL Listed Mark	Safety	
Australia	SAA	Standards Australia	Safety	
USA / Canada	cTUVus	North American cTUVus Certification — Nationally Recognized Testing Laboratory	Safety	
European Union	TUV Rheinland	German TUV Rheinland	Safety	
USA / Canada	UL / C-UL	Underwriters Laboratories Co., Ltd.	Safety	
Japan	VCCI	Voluntary Control Council for Information Technology Equipment	EMI	

Product Labeling

To ensure product safety management, CyberPower has invested significant resources in product development, production, storage, and labeling. In addition to implementing appropriate safety measures for products of different specifications, we also ensure that all product labeling information is complete and compliant with relevant local regulations. In 2024, there were no incidents of non-compliance regarding the product and service information and labeling.

Product Carbon Footprint

CyberPower is actively responding to global warming and carbon tariffs. In 2023, we launched the first ISO 14067 Product Carbon Footprint for the Smart App Online (High-Density) UPS series. By engaging professional third-party verification, we ensure the accuracy and reliability of the carbon footprint data.

To deepen the understanding of carbon emissions generated throughout the product life cycle and to establish a foundation for future carbon reduction management, we continue to build internal knowledge and identify carbon hotspots. Based on these insights, we develop corresponding carbon reduction measures, including optimizing production processes, selecting more eco-friendly raw materials, improving transportation methods, and promoting the use of green products.

CyberPower firmly believes that these efforts not only help reduce our environmental impact but also demonstrate our commitment to the environment, society, and corporate governance. Through continuous review and improvement, the company aims to maintain a competitive edge under the pressure of future carbon market and environmental regulations, while also creating value for our shareholders and stakeholders.

Future Carbon Reduction Measures



Optimize Production Processes



Select More Eco-friendly Raw Materials



Improve Transportation Methods



Promote the Use of Green Products

ISO 14067:2018 Product Carbon Footprint



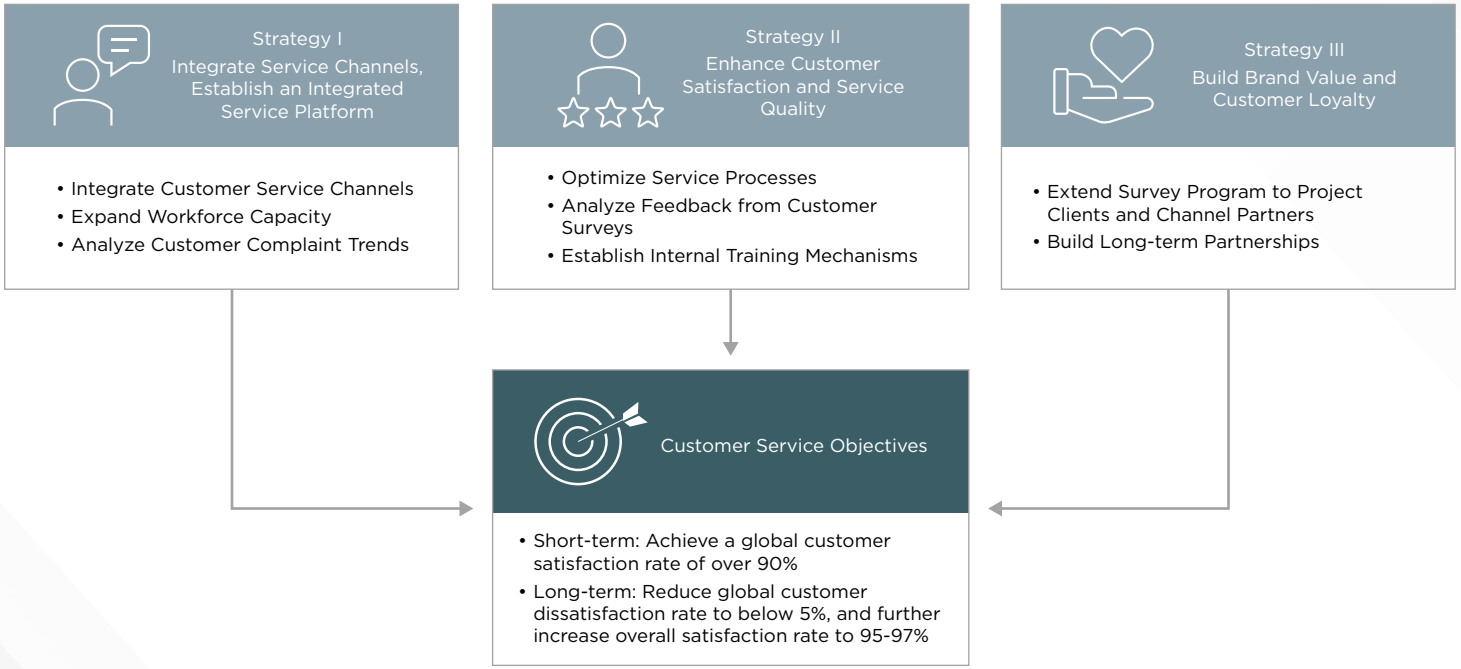
Smart App Online (High-Density)

Customer Service

Service Quality and Trust

CyberPower fully recognizes that effective customer relationship management is the foundation for sustainable business operations. The company is committed to delivering a customer-centric service experience by continuously enhancing customer trust, satisfaction, and brand loyalty through effective complaint handling procedures and feedback mechanisms. With a customer-focused approach, we have established a systematic management framework that encompasses product usage experience, after-sales service, and responsive communication to foster positive customer relationships.

Customer Service Strategic Objectives



Over the past three years, amid rapidly shifting global dynamics, some of CyberPower's customer service centers have undergone multiple relocations and workforce restructuring in response to operational adjustments. These changes have indirectly affected the customer experience and satisfaction. To effectively address these challenges, we have implemented the following adjustments:

- Optimize Workforce System: Adjust compensation and career development frameworks at customer service centers and evaluate diversified working models to enhance talent attraction and reduce turnover rates.
- Strengthen Training and SOPs: Focus on improving technical problem-solving skills and customer interaction quality. Define clear Standard Operating Procedures (SOPs) for special scenarios to enhance overall service consistency and efficiency.
- Improve Internal Management Mechanisms: Adjust departmental responsibilities and evaluation methods to clearly delineate roles and authorities, thereby strengthening team effectiveness and continuously improving service quality.

Customer Satisfaction Survey

CyberPower values every customer's feedback, regarding it as a vital foundation for enhancing service quality and deepening customer relationships. Since 2021, we have implemented an annual customer satisfaction survey system at our Global Customer Service Center. This is complemented by quarterly evaluation meetings, periodic customer interviews, and real-time online feedback mechanisms to continuously capture authentic customer opinions on products, services, and overall interaction experiences. These insights serve as critical references for service optimization and process improvement. To implement this system effectively and address varying regional systems and service models, we employ the following survey methods for the annual satisfaction assessments:

- Eurasia and Other Regions: After customers complete an online inquiry via the official website, a satisfaction rating prompt automatically appears, inviting customers to provide feedback on that service experience.
- North America: After customers complete service inquiries through the customer service system, a survey is emailed to them for rating, with responses automatically collected and aggregated by the system.

According to the 2024 survey statistics, customer satisfaction in Eurasia and other regions reached 91.33%, while North America's satisfaction rate was 84.60%. Despite facing numerous operational challenges, we continue to optimize our customer service systems, improve staff training, and integrate service experiences across regions to build a scalable and flexible global service network. In the short term, the goal is to maintain a global customer satisfaction rate above 90%. The long-term objective is to reduce global customer dissatisfaction rate to below 5% and increase overall satisfaction rate to between 95% and 97%. Moving forward, we will continue to enhance service efficiency and team responsiveness to further strengthen brand value and customer loyalty.

Communication Channels

Official Website / Customer Service Hotlines / Distributors & Resellers / E-commerce Platforms / Social Media

Customer Satisfaction Survey Results in 2024

Item	Eurasia / Other Regions	North America
Number of Surveys	568	26,419
Number of Responses	150	2,324
Customer Satisfaction Rate	91.33%	84.60%

Product and Service Optimization

CyberPower continuously optimizes its service systems and customer service processes, actively collecting product issues and market feedback for analysis and improvement measures to provide customers with more satisfying products and services.

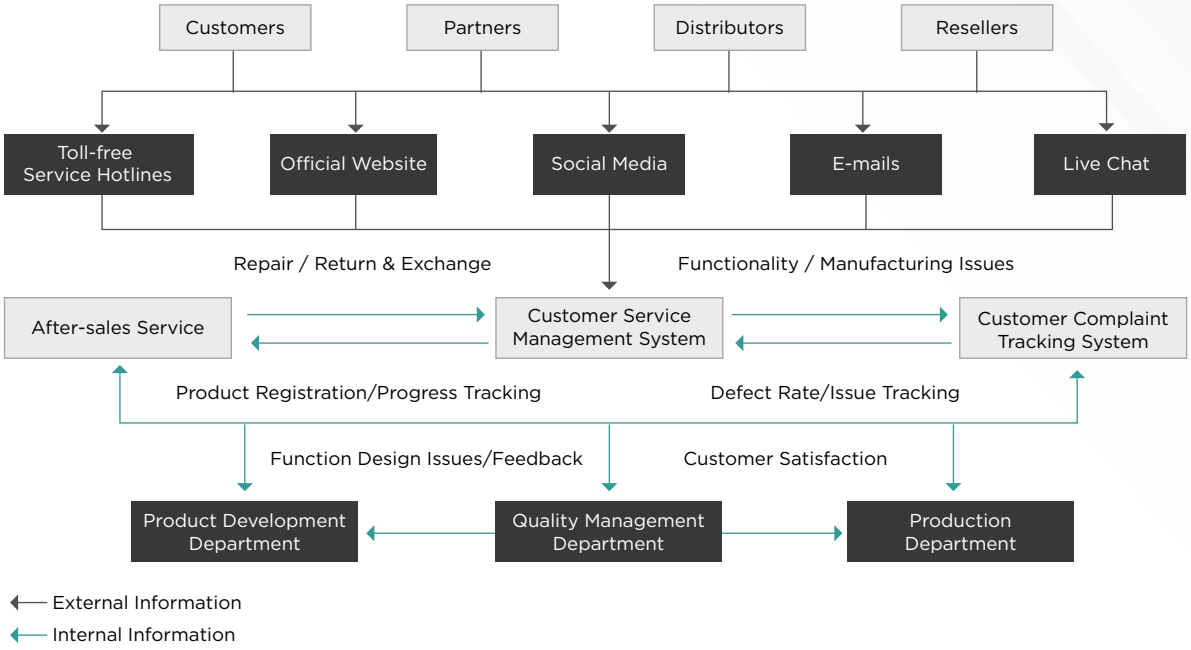
Continuous Optimization of Service Systems

To enhance after-sales service quality, CyberPower has established a Global Customer Service Center and an online service system. Through toll-free customer service hotlines, online customer service, web inquiry forms, and email, we provide real-time and high-quality customer service for English-speaking regions.

Enhancing Service Quality

CyberPower values customer feedback. In addition to listening to our customers attentively, we conduct thorough and careful analysis of their feedback to improve and develop products that meet their satisfactions, while continuously enhancing service quality.

The Management Process of Customer Service





05 Supply Chain Management

Sustainable Value Chain
Supplier Risk Assessment
Supplier Evaluation and Audit

Sustainable Value Chain

2024 Material Topic: Management of "Supply Chain Management"

Material Topics	Supply Chain Management
GRI Standards	GRI 204-1: Proportion of Spending on Local Suppliers GRI 308-1: New Supplier that were Screening Using Environmental Criteria GRI 414-1: New Supplier that were Screening Using Social Criteria GRI 414-2: Negative Social Impacts in the Supply Chain and Actions Taken
SDGs	
Policy or Commitment	CyberPower regards its suppliers as key partners. In addition to requiring quality, pricing, and delivery performance, the company also emphasizes suppliers' environmental, health, and safety management, sustainability capabilities, and supply stability. CyberPower has established guidelines to ensure that supply chain operations meet sustainability and compliance standards, and it upholds the principles of integrity, mutual benefit, and transparency to enhance overall supply chain resilience and responsible management.
Indicators and Goals	Continuing Goals (Short-, Mid-, and Long-term): • Continue increasing the proportion of Tier A suppliers and the overall evaluation achievement rate • Conduct annual risk assessments and audits for key suppliers, maintaining a 100% completion rate for documented audits • Ensure 100% signing rate of "Guarantee of Hazardous Substances" by suppliers • Encourage key suppliers to obtain international certifications such as ISO 9001, ISO 14001, and RBA
Effectiveness Tracking Mechanism	• Conducted annual evaluations of the top 30 suppliers by transaction volume, with tiered management based on assessment results • Issued improvement deadlines to Tier C suppliers; partnerships were not renewed for those failing to meet requirements • Performed regular documented and on-site audits, adjusting audit frequency and scope according to risk level • Implemented restricted "Guarantee of Hazardous Substances" and conflict minerals due diligence mechanisms for new suppliers
Annual Actions and Measures	• Promoted ethical business practices to 441 regular suppliers through the Integrity Clause in the "Procurement Agreement" • Completed documented audits for 87 suppliers and on-site audits for 46 suppliers • Terminated partnerships with 2 suppliers based on the risk control mechanism • Continued to promote local sourcing, with the local procurement percentage in China (Cyber Power (Shenzhen) Ltd) reaching 96.42%, a 13.93% increase compared to the previous year

CyberPower specializes in professional design, production, and sales of Uninterruptible Power Supplies (UPS) and power electronics products. Its supply chain spans upstream raw materials, midstream research and manufacturing, and downstream customer applications, forming a highly integrated and responsive sustainable value chain.

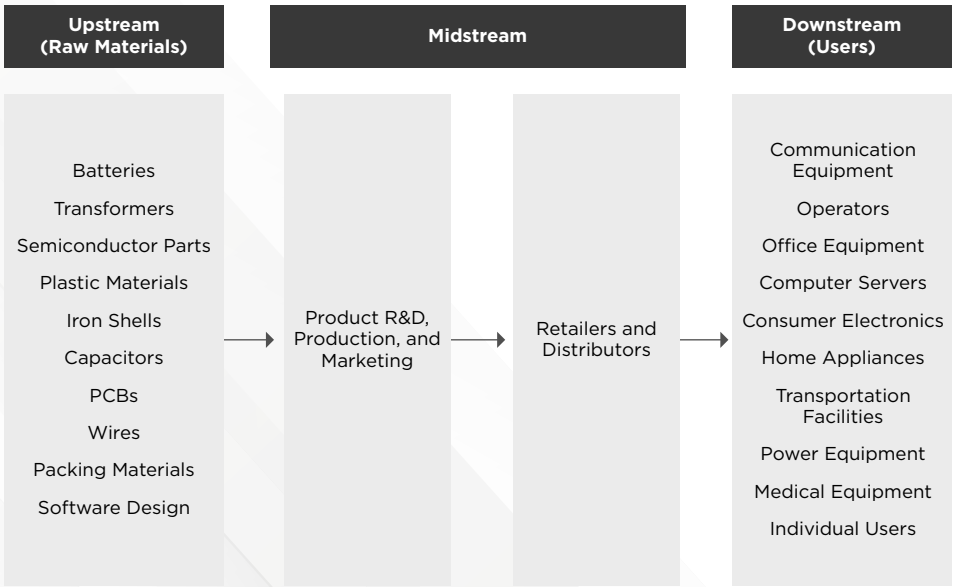
Upstream Supply Chain - Key raw materials include batteries, transformers, semiconductor components (e.g., micro-controllers, MOSFETs, Transistors, Diode), plastic and metal parts, capacitors, printed circuit boards, wiring, packaging materials, and application software design. The company sources from a diverse pool of suppliers, avoiding over-reliance on any single source. This approach ensures long-term partnerships and enhances supply chain resilience and adaptability.

Midstream Manufacturing - CyberPower maintains full control over product R&D, design, and assembly. Each product undergoes multiple stages of processing and rigorous testing, including functional verification, durability assessments, safety compliance checks, and final packaging, to ensure that product performance, quality, and safety comply with international standards. The R&D team adopts modular design, energy efficiency optimization, and smart management technologies to accelerate time-to-market and strengthen product competitiveness.

Downstream Applications - CyberPower-branded products are sold in over 100 countries worldwide, serving both commercial and consumer markets. Through its after-sales service system and customer feedback mechanisms, the company continuously monitors market trends and user needs, enhancing brand influence and customer satisfaction.

Commitment to Sustainability - CyberPower is dedicated to embedding sustainability across every link of its value chain. This includes implementing green design principles, developing energy-saving products, establishing low-carbon manufacturing processes, and promoting waste reduction initiatives. These efforts reflect the company's commitment to environmental protection and social responsibility, while building a globally competitive green supply chain.

Industry Value Chain of CyberPower



Supply Chain Management Policy

Quality Standard | Service and Innovation | Risk Assessment | Continuous Improvement | Sustainable Development

CyberPower has established comprehensive "Procurement Operations" and "Supplier Management Procedures" to regulate procurement processes, evaluation mechanisms, quality acceptance, and contract management. Sustainability principles are fully integrated into the core of CyberPower's supply chain management. Beyond basic requirements such as quality, delivery time, and pricing, the company places strong emphasis on suppliers' compliance practices, labor and human rights protection, environmental and occupational health & safety management capability to ensure overall supply chain resilience and integrity.

All partner suppliers are required to sign the "Quality Statement" and "Integrity Commitment Letter," and adhere to the "Management Regulations of Hazardous Substances" established by CyberPower. Suppliers must provide comprehensive documentation, including Material Declarations, product safety certifications, REACH / RoHS compliance statements, and third-party verification reports. These documents must be proactively updated prior to expiration to ensure that all delivered products comply with international regulations and CyberPower's internal green standards. This process helps prevent high-risk or prohibited substances from entering the supply chain, thereby reinforcing compliance and strengthening accountability.

In 2024, Cyber Power (Shenzhen) Ltd was awarded Platinum Rating from the Responsible Business Alliance (RBA) This prestigious recognition, granted following a rigorous third-party audit, covers five key dimensions: labor rights, health and safety, environmental responsibility, ethics, and management systems. The certification reflects the company's commitment to responsible business practices and demonstrates that its supply chain management has achieved the highest international standards.

Platinum Rating from the Responsible Business Alliance (RBA)



Cyber Power (Shenzhen) Ltd

Sustainable Procurement

CyberPower is dedicated to promoting the development of a sustainable supply chain by actively implementing local procurement policies. Through establishing strong partnerships with suppliers located in its operational regions, the company not only contributes to local economic growth but also helps shorten supply chain distances, improve responsiveness, and effectively reduce carbon emissions from long-distance transportation.

The company prioritizes working with local suppliers who possess recognized certifications and strong reputations. Within the operational boundaries defined in this report, all major operating sites adhere to the principle of local procurement preference when sourcing materials and services, thereby enhancing the flexibility and resilience of the supply chain.

Cyber Power (Shenzhen) Ltd, a key manufacturing site of the company, has implemented a long-term local sourcing strategy. In 2024, local procurement in China accounted for approximately 96.42% of total expenditures, demonstrating the company's steady progress in building a stable local supply network.

Percentage of Local Procurement at Cyber Power (Shenzhen), Ltd in the Past 3 Years

Item	2022	2023	2024
Percentage of Local Procurement	84.46%	84.63%	96.42%

Supplier Risk Assessment

To reduce the risk of operational disruptions and noncompliance, CyberPower conducts supplier risk identification and tiered management in accordance with its "Procurement Operations." All new suppliers must complete a preliminary qualification review and submit the following documents: a restricted "Guarantee of Hazardous Substances", an "Code of Integrity, Ethics, and Confidentiality Agreement", and a "Procurement Agreement." These documents affirm that the supplier's products, business conduct, human rights protections, and social responsibility efforts meet CyberPower's sustainability standards and comply with relevant regulations.

For suppliers identified with potentially high risk, the company initiates support and improvement measures based on actual conditions. These may include assistance in establishing environmental, health and safety management systems, strengthening internal control processes, and regularly tracking progress. If a supplier fails to meet standards after multiple improvement consultations, CyberPower will terminate the partnership in accordance with legal procedures, reinforcing its commitment to high standards in supply chain risk management.

Environmental Risk	• Require Suppliers to Sign the "Guarantee of Hazardous Substances" CyberPower requires all suppliers to sign a "Guarantee of Hazardous Substances" to affirm that the products or components they provide—including accessories, packaging materials and any items related to product delivery—comply with applicable regulations. If there is any violation of the applicable requirements, CyberPower reserves the right to terminate or rescind the contract to safeguard human health and environmental safety. • Implement Internal and External Controls Based on the "Management Regulations of Hazardous Substances" Internal: Control of product design, development, and procurement within the company External: Enforce supplier chemical substance management, establish the "Guarantee of Hazardous Substances" as a required document, and ensure suppliers complete it. For suppliers who refuse to comply, CyberPower requires a formal declaration to enforce strict chemical substance control.
Social Risk	• Require Suppliers to Sign the "Guarantee of Hazardous Substances" and Commit to Avoid the Use of Conflict Minerals According to investigations by the Responsible Minerals Initiative (RMI), armed groups in the Democratic Republic of the Congo and surrounding countries have illegally obtained minerals—including tantalum (Ta), tin (Sn), tungsten (W), gold (Au), cobalt (Co), and mica—through forced labor and child exploitation. As a responsible corporate citizen, CyberPower upholds humanitarian values and ethical social responsibility by requiring suppliers to avoid the use of conflict minerals sourced through unlawful practices. Since 2014, the company has adopted the Conflict Minerals Reporting Template (CMRT) developed by the RMI to assist suppliers in gradually sourcing minerals from certified smelters. Suppliers are required to disclose and regularly update information regarding the smelters and mines involved in their supply chains.
Governance Risk	• Require Primary Material Suppliers to Sign the Integrity Clause in the "Procurement Agreement" CyberPower requires all new suppliers to sign the Integrity Clause in the "Procurement Agreement." Only those who pass the evaluation and meet the required standards will be approved as qualified suppliers.

Supplier Evaluation and Audit

Supplier Evaluation

CyberPower regularly communicates with suppliers and contractors to assess their compliance with regulations and ensure adherence to the laws. The company also conducts regular evaluations of suppliers and contractors that have engaged in transactions with its Taiwan operations center during the current fiscal year.

The evaluation results are categorized into three levels: A, B, and C. For suppliers rated as Level C, the company will require corrective actions within a specified timeframe; failure to comply may result in termination of future cooperation.

To maintain supplier competitiveness, the company conducts annual evaluations of its suppliers. The weighting of assessment criteria is determined based on the significance of each supplier's impact on operations, and the results serve as a basis for supplier risk management. In 2024, the evaluation criteria and weightings include quality management, delivery reliability, service performance, cost control, and supplier management—all aimed at sustaining supplier competitiveness.

Supplier and Contractor Evaluation Results in the Past 3 Years

Vendor	Rating	2022	2023	2024
Supplier	A	61	41	57
	B	43	74	30
	C	5	0	2

Supplier Audit

CyberPower continues to strengthen supply chain resilience, placing high importance on the operational stability and sustainability of its partners. In accordance with risk management principles, the company adopts a differentiated audit strategy: conducting on-site inspections for critical material suppliers, newly onboarded vendors and underperforming partners, while evaluating general material suppliers or those without identified risks through documented audits.

In 2024, CyberPower conducted documented audits for 87 suppliers and contractors across Taiwan and China to assess baseline risks. Additionally, based on geographic location, transportation conditions and risk ratings, the company performed on-site audits for 46 suppliers. The audit scope included operational status, capacity utilization, future development plans and investment strategies—providing a comprehensive understanding of supplier performance and potential risks to inform procurement decisions and risk management.

For suppliers with operational instability or unsatisfactory performance, CyberPower initiates new vendor onboarding and material qualification processes to mitigate potential supply disruptions. Suppliers identified as high-risk but not immediately replaceable are placed on a watch list for regular monitoring and management. To ensure supply chain quality and governance effectiveness, CyberPower terminated partnerships with two suppliers that failed to meet required standards, demonstrating its commitment to supplier oversight and sustainable supply chain management.

Supplier and Contractor Audit Compliance in the Past 3 Years

Vendor Category		Supplier		
Audit Method		2022	2023	2024
On-site Audit	Planned Number of On-site Audits	--	32	46
	Actual Number of On-site Audits Completed	--	32	46
	Achievement Rate	--	100%	100%
Documented Audit	Planned Number of Documented Audits	109	115	87
	Actual Number of Documented Audits Completed	109	115	87
	Achievement Rate	100%	100%	100%

Note: In 2022, due to the COVID-19 pandemic, lockdowns and district management measures were implemented in China. In compliance with government policies, the company suspended business travel to affected areas, and therefore did not conduct any on-site supplier audits.



06 Environmental Protection

Climate Change Adaptation
Climate-related Risks and Opportunities
Greenhouse Gas and Energy Management
Water Resource Management
Waste Management
Energy Saving and Carbon Reduction

Climate Change Adaptation

2024 Material Topic: Management of "Climate Change Adaptation"

Material Topics	Climate Change Adaptation
GRI Standards	302-1 Energy consumption within the organization 302-3 Energy intensity 305-1 Direct (Scope 1) GHG emissions 305-2 Energy indirect (Scope 2) GHG emissions 305-3 Other indirect (Scope 3) GHG emissions 305-4 GHG emissions intensity 305-5 Reduction of GHG emissions
SDGs	
Policy or Commitment	CyberPower recognizes the material operational and financial impacts posed by climate change. In response, we have adopted the TCFD framework and integrated the ISO 14064-1 standard to identify carbon emission hotspots, plan energy-saving and carbon reduction pathways, and develop adaptation strategies and energy management mechanisms based on risk scenarios. Through this systematic approach, we aim to enhance corporate climate resilience while minimizing environmental impacts and transition risks.
Indicators and Goals	Short-term Goals (1-2 Years) • Continue implementing relevant initiatives, including equipment upgrades to improve energy efficiency and the adoption of renewable energy sources Mid-term Goals (2-5 Years) • Complete a consolidated group-wide greenhouse gas (GHG) inventory in accordance with ISO 14064-1 by 2026, and set emission reduction targets based on the results Long-term Goals (5+ Years) • Using 2024 as the base year, achieve a 7–10% reduction in Scope 1 and Scope 2 carbon intensity by 2030
Effectiveness Tracking Mechanism	• Annually identify climate-related risks and opportunities in accordance with TCFD, consolidating their impacts and potential financial implications • Implement inventory and third-party assurance mechanisms to monitor energy and carbon emission trends • Quantify the effectiveness of climate-related targets by comparing emissions data across scopes with annual revenue metrics
Annual Actions and Measures	• Continue expanding the scope of the GHG inventory and secure third-party assurance • Solar electricity generated in Taiwan reached 3,736.8 kWh, while in China it reached 1,860 kWh • Based on the four core areas of the TCFD, identify climate-related risks and opportunities, complete analysis of financial impacts, and implement adaptation actions • Carry out preparatory work for renewable energy certificates, and drive updates to high-efficiency energy-saving equipment while managing office energy conservation

Climate-related Risks and Opportunities

With the increasing frequency of extreme weather events posing widespread impacts on both society and economic systems, global attention to climate issues continues to intensify. The World Meteorological Organization (WMO) has warned that climate change is exacerbating disaster risks and posing serious threats to human livelihoods and the natural environment. The implementation of the "Paris Agreement," with its goal to limit global warming to well below 2 °C above pre-industrial levels—and preferably to 1.5 °C—has spurred countries to accelerate their decarbonization efforts. As a result, corporate operations are now navigating the dual challenge of climate risks and transition pressures.

In response, CyberPower has given heightened priority to the operational impacts of climate change. Since 2023, we have adopted the Task Force on Climate-related Financial Disclosures (TCFD) framework to strengthen our governance and response capabilities. This framework—comprising the pillars of Governance, Strategy, Risk Management, and Metrics and Targets—enables us to systematically identify and assess both risks and opportunities related to climate change.

Beyond Taiwan, we have extended our risk-assessment boundaries to include China and the Philippines, conducting robust analyses across these regions—focusing on policy shifts, extreme climate events, and energy transitions. By integrating climate risk into our operational planning and sustainability strategy, we are steadily enhancing climate resilience across all regions and laying a foundation for a low-carbon economy.

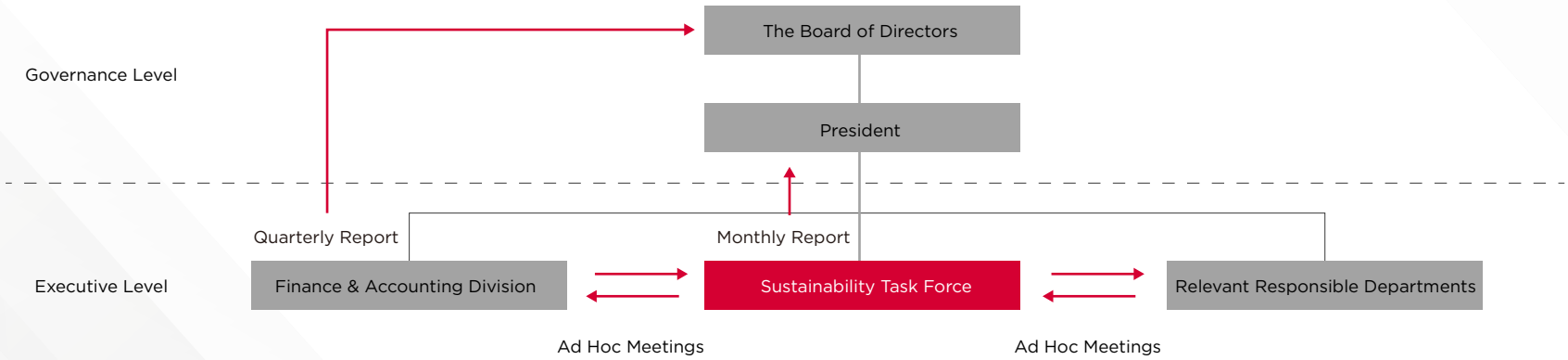
Climate Sustainability Governance

CyberPower's Finance & Accounting Division is responsible for consolidating potential impacts of various issues on both internal and external organizational aspects. The Sustainability Task Force, together with relevant responsible departments, collaboratively identifies and assesses climate risks and responses to climate impacts, discusses countermeasures, and formulates adaptation plans.

Climate management results are reported monthly by the Sustainability Task Force leader to the management team. The Finance & Accounting Division presents overall progress quarterly to the Board of Directors, assisting the Board in overseeing and guiding the company's climate actions, direction, and strategy.

The execution teams hold periodic meetings to discuss related measures and are gradually establishing a group-level governance framework covering Taiwan, China, and the Philippines to enhance risk transparency and decision-making foundations.

Climate Sustainability Governance Structure



Climate Risk Management

CyberPower systematically assesses the potential impacts of physical and transition risks on its operational sites, supply chain, and overall business performance based on climate risk categories. In this assessment, 2 physical risks, 4 transition risks, and 4 climate-related opportunities were identified. To enhance resilience, the company continues to promote energy-saving and carbon reduction initiatives, strengthen carbon management and energy efficiency at its sites, and develop adaptation measures based on assessment results. These efforts ensure stable operations under climate impacts while capturing climate-related opportunities.

Climate Risk and Opportunity Management Process

Identification and Assessment → Mitigation and Adaptation → Governance and Oversight

Climate Risk and Opportunity Assessment

CyberPower evaluates climate risks and opportunities using a two-dimensional matrix based on impact severity and likelihood of occurrence. The impact severity is categorized into three levels: low, medium, and high; while likelihood is classified as unlikely, possible, and very likely. This dual-axis assessment helps identify medium to high-risk climate issues for prioritized management.

Climate-related Risk and Opportunity Matrix

Impact Severity	High		1	3 4 5 6
	Medium		2 3	2 1 4
	Low			
Likelihood of Occurrence		Unlikely	Possible	Very Likely

Climate-related Risks and Opportunities List

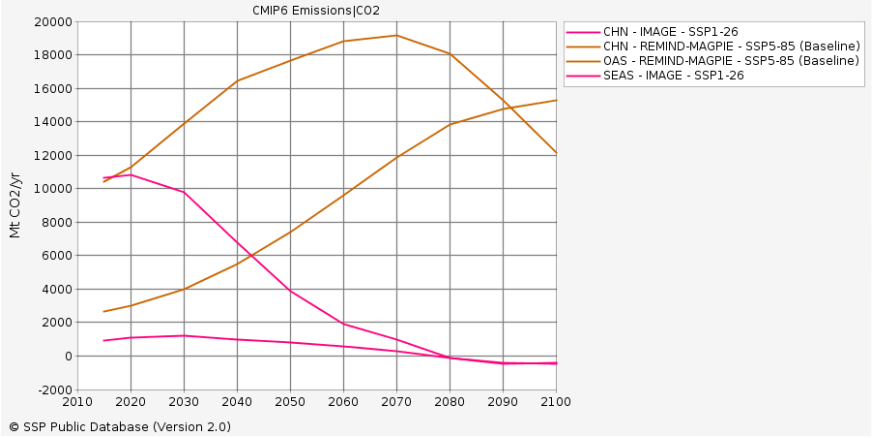
Climate Risks	1 Physical Risk (Typhoons, Floods, and Other Extreme Weather Events) 2 Physical Risk (Rising Annual Average Temperature) 3 Transition Risk (Policy and Regulatory Risk) 4 Transition Risk (Technology Risk) 5 Transition Risk (Market Risk) 6 Transition Risk (Reputational Risk)
Climate Opportunities	1 Resource Efficiency 2 Products and Services 3 Resilience 4 Energy Source

Physical Risks

To effectively understand the potential impacts of extreme weather events and long-term climate trends caused by climate change, CyberPower references the Intergovernmental Panel on Climate Change (IPCC) Sixth Assessment Report (AR6) and its Shared Socioeconomic Pathways (SSP) scenarios. The company selects the low emission scenario (SSP1-2.6) and high emission scenario (SSP5-8.5) for scenario simulation and analysis to predict potential climate risks to its operational sites.

This analysis is based on simulation results from the Coupled Model Intercomparison Project Phase 6 (CMIP6) and supplemented by multiple internationally recognized climate data platforms to estimate extreme climate change trends in Taiwan, China, and the Philippines.

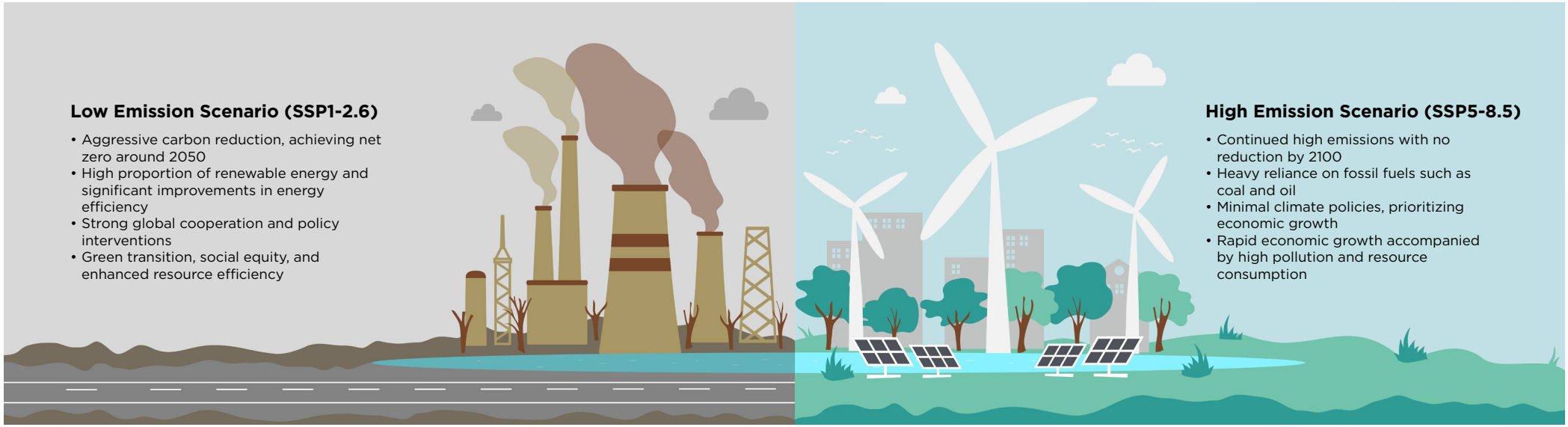
Shared Socioeconomic Pathways (SSP) scenarios



(Source: International Institute for Applied Systems Analysis (IIASA))

Under the low emission scenario (SSP1-2.6), carbon emissions in China and the Southeast Asia region (SEAS, including Taiwan and the Philippines) have shown a steady decline since 2020, with a significant reduction expected in the latter half of this century. Emissions are projected to approach net zero by 2100, demonstrating the effectiveness of climate policies and technological advancements in curbing emissions.

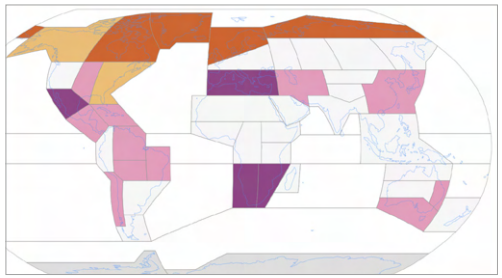
Under the high emission scenario (SSP5-8.5), carbon emissions in China and other Asian regions (OAS, including Taiwan and the Philippines) continue to rise, peaking around 2080 before experiencing only a slight decrease. This scenario reflects a lack of coordinated global mitigation efforts, resulting in uncontrolled regional greenhouse gas (GHG) emissions and heightened risks of extreme weather events and chronic climate impacts.



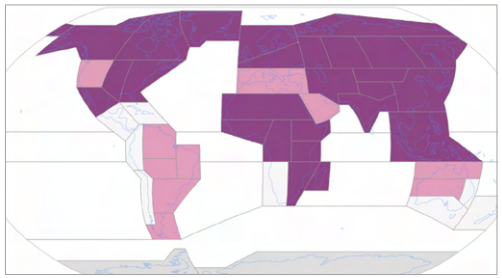
Immediate Physical Risk – Typhoons, Floods, and Other Extreme Weather Events

Regions	Low Emission Scenario (SSP1-2.6)	High Emission Scenario (SSP5-8.5)	Time Horizon
Taiwan	Increased frequency of afternoon thunderstorms and heavy rainfall has raised the burden on urban drainage systems	Intensified extreme rainfall and typhoon strength are increasing risks in coastal areas	Short-term
China	Slight increase in intense rainfall and rising drainage pressure, with short-duration downpours and mudslide risks emerging in some areas	Increasing frequency and intensity of heavy rainfall and typhoons are leading to greater risks of urban flooding and water accumulation	
Philippines	Slight increase in typhoon season intensity and heavy rain events, with elevated localized risks	Rising frequency and intensity of typhoons are affecting both coastal and inland areas, significantly increasing long-term flood risk	

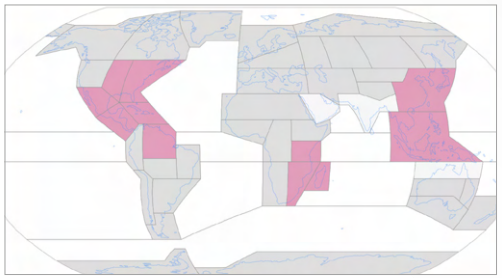
Extreme Climate Change Projections (Projected changes by 2100 compared to the 1995–2014 baseline)



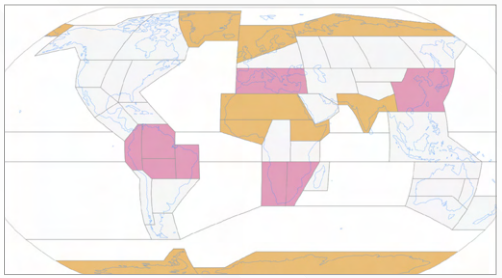
Drought



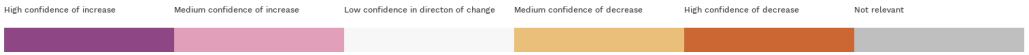
Flooding



Tropical Cyclones



Solar Radiation

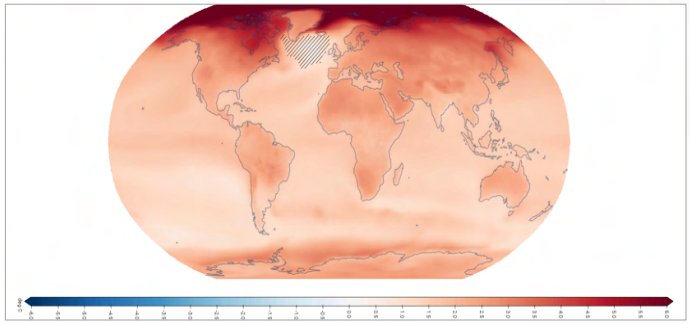


(Source: IPCC WGI Interactive Atlas)

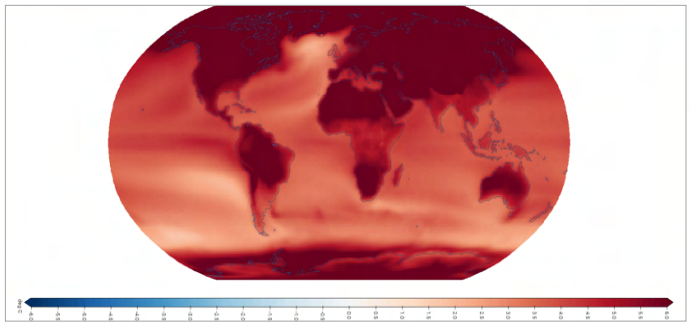
Chronic Physical Risk – Rising Annual Average Temperature

Regions	Projected Temperature Rise by 2100 (°C) – Scenario		Risk Details	Time Horizon
	Low Emission Scenario (SSP1-2.6)	High Emission Scenario (SSP5-8.5)		
Taiwan	1.6-2.0	1.6-5.2	Changes in temperature and precipitation will increase the alternating risks of flooding and drought, leading to greater climate instability	Long-term
China	1.6-2.0	1.6-5.2	Increased number of hot days and frequency of heatwaves will affect equipment cooling and labor productivity	
Philippines	1.2-1.5	1.3-3.9	Rising frequency of tropical cyclones and heavy rainfall will elevate risks of flooding and wind damage to facilities	

Projected Annual Temperature Increase under SSP1-2.6



Projected Annual Temperature Increase under SSP5-8.5



(Source: IPCC WGI Interactive Atlas)

Transition Risks

The company conducts climate-related transition risk assessments based on the TCFD framework, focusing on policy and regulations, technology, market, and reputational aspects. The analysis integrates CyberPower's business model, industry characteristics, and key market environments to identify operational risks and potential financial impacts that each regional site may face under carbon pricing mechanisms, increasing energy efficiency requirements, strengthened international procurement standards, and sustainability disclosure trends.

Risk Types	Regions	Risk Details	Time Horizon
Policy and Regulatory Risk	Global	Stricter carbon pricing, emissions trading schemes, and climate regulations are driving the need for compliance with both local laws and international decarbonization standards, such as the EU Carbon Border Adjustment Mechanism (CBAM), Taiwan's "Climate Change Response Act," and the US ENERGY STAR Program	Mid- and Long-term
Technology Risk		To meet energy efficiency requirements and net-zero targets, production processes and equipment must be upgraded or replaced. However, in some regions, technical support and resources remain insufficient	
Market Risk		International brands and buyers are tightening sustainability requirements, incorporating carbon footprint and ESG performance into supplier evaluations	
Reputational Risk		If sustainability disclosures are inadequate or corporate social responsibility efforts lack substance, the company may face scrutiny from customers, investors, or the media, potentially affecting brand trust	

Climate Opportunities

Opportunity Types	Regions	Opportunity Details	Time Horizon
Resource Efficiency	Global	In response to the trend of energy saving and carbon reduction, improving equipment efficiency and implementing smart monitoring systems effectively enhance operational and environmental performance	Mid- and Long-term
Energy Source		Aligned with the global energy transition, adopting renewable energy and green electricity helps reduce risks related to energy price volatility and carbon costs	
Products and Services		Facing the rise of green markets and increasing customer sustainability demands, promoting low-carbon design and the use of eco-friendly materials creates differentiation and expands sustainable product opportunities	
Resilience		To strengthen operational resilience, the company enhances its capacity to respond to climate impacts through climate risk assessments and cross-departmental adaptation actions	

Climate Change Strategy

CyberPower identifies risks and uncovers opportunities to estimate potential financial impacts under various climate scenarios, and accordingly adjusts its operational layout and resource allocation.

Physical Risk Strategy

Risk Types	Climate-related Issues	Potential Financial Impacts	Adaptation and Response
Acute Risk	Typhoons, Floods, and Other Extreme Weather Events	Workforce attendance instability and delivery delays lead to increased equipment maintenance costs	• Assess the modularization of product design to reduce material variety • Evaluate planned production to shorten lead time • Enhance backup power and personnel scheduling flexibility at plants; strengthen emergency management • Reinforce drainage and flood prevention facilities; establish early warning systems and post-disaster recovery procedures • Optimize warehouse layout and diversify logistics backup; adjust production scheduling flexibility • Strengthen disaster response mechanisms at coastal sites; review insurance coverage scope
Chronic Risk	Rising Annual Average Temperature	Elevated risks of supply chain and logistics disruptions may result in contract breaches and compensation expenses	• Implement Building Management System (BMS) that automatically adjust indoor temperatures based on real-time conditions • Establish employee health monitoring systems; introduce heat-resistant components and energy-efficient equipment • Optimize water resource management; adjust site selection criteria for warehouses and manufacturing bases • Establish backup suppliers; monitor water resource risk hotspots • Develop site-specific environmental policies; improve factory drainage systems and insurance arrangements
		Increased demand for cooling equipment and heightened employee health risks contribute to higher operational costs	
		Equipment damage, rising insurance premiums, and amplified post-disaster repair expenses adversely affect long-term operations	

Transition Risk Strategy

Risk Types	Potential Financial Impacts	Adaptation and Response
Policy and Regulatory Risk	Implementing carbon inventory, paying carbon fees, and complying with regulations and product standards may increase compliance and operational costs	• Monitor regulations related to carbon fees and carbon trading schemes in real time • Adjust manufacturing processes and internal systems in response to new regulations • Adopt ISO 14001 Environmental Management System, ISO 14064-1 Greenhouse Gas Inventory, ISO 14067 Product Carbon Footprint, and other relevant environmental standards to establish a comprehensive management framework
Technology Risk	High investment required for equipment upgrades and technological transitions may constrain R&D and production resource allocation	• Introduce energy-efficient equipment and optimize production systems to improve energy use efficiency • Establish a timeline and targets for adopting low-carbon technologies • Assess the use of renewable energy based on operational conditions
Market Risk	Poor sustainability performance may result in lost orders or missed opportunities with new clients, negatively impacting revenue	• Disclose product carbon footprint information in alignment with international customer requirements • Obtain third-party verification to maintain market competitiveness • Review carbon-related regulations in export markets and assess corresponding product response strategies
Reputational Risk	Damage to brand reputation may lead to shareholder pressure, investor divestment, and potentially lower scores in public tender evaluations	• Regularly review corporate sustainability performance and communication strategies • Implement sustainability ratings, voluntary disclosures, and stakeholder engagement mechanisms • Enhance internal training to strengthen employees' ability to address sustainability issues

Climate Opportunity Strategy

Opportunity Types	Potential Financial Impacts	Adaptation and Response
Resource Efficiency	Reduce energy costs and operational expenses, improving resource use efficiency	• Implement online approval system to replace traditional paper-based processes • Replace outdated machinery with high-efficiency equipment • Promote internal policies for energy usage • Introduce a smart monitoring platform
Energy Source	Lower long-term external energy procurement costs by increasing the share of clean energy	• Replace with high-capacity solar panels to increase the proportion of self-generated power • Continuously expand testing of solar inverters, uninterruptible power supplies (UPS), and other related products
Products and Services	Enhance product value-added features to create differentiation and expand green market opportunities	• Gradually standardize the product carbon footprint process • Use recycled materials and eco-friendly consumables • Continuously invest in R&D for more energy-efficient products and expand sales scale
Resilience	Strengthen corporate resilience to minimize climate change impacts while reducing customer losses	• Expand the scope of climate-related risk analysis • Enhance the comprehensiveness of scenario analysis

Climate Metrics and Targets

CyberPower is proactively addressing the impacts and pressures brought by climate change while seeking transformation opportunities to advance toward a low-carbon and sustainable future.

Emission Reduction Targets: CyberPower's base year for greenhouse gas (GHG) inventory was originally 2023. Due to the expanded GHG inventory boundary in 2024, which now includes certain subsidiaries in China and the Philippines, the base year has been adjusted to 2024. The reduction target is set to achieve a 7–10% decrease in carbon intensity by 2030. To track progress, based on Scope 1, Scope 2, and relevant Scope 3 (Categories 4.1 and 4.3) GHG emissions data from the Taiwan headquarters, carbon intensity decreased approximately 6.7% in 2024 compared to 2023.

Greenhouse Gas and Energy Management

Greenhouse Gas (GHG) Emissions

Since 2022, CyberPower has conducted an annual greenhouse gas (GHG) inventory in accordance with the international standard ISO 14064 1:2018. We engage qualified third party verification bodies to examine our GHG inventory. The scope of verification covers Scope 1 (Direct GHG Emissions), Scope 2 (Indirect GHG Emissions from Purchased Energy), and two categories under Scope 3 (Other Indirect Emissions): Category 4.1 (Upstream Emissions from Purchased Goods) and Category 4.3 (Waste Disposal). We continuously obtain GHG verification to ensure the accuracy and transparency of our carbon inventory, thereby strengthening stakeholder trust in our disclosures.

To meet stakeholder expectations for enhanced climate risk disclosure and carbon reduction commitments, in 2024 we expanded our GHG inventory boundary to include certain subsidiaries in China and the Philippines. We also updated our base year to 2024 to facilitate the formulation of subsequent carbon reduction targets and enable trend comparisons.

In 2024, CyberPower's total GHG emissions amounted to 8,619.323 tCO_2e, comprised of:

- Scope 1 (Direct GHG Emissions): 472.5543 tCO_2e
- Scope 2 (Indirect GHG Emissions): 5,349.5150 tCO_2e
- Scope 3[Note] (Other Indirect Emissions): 2,797.2532 tCO_2e

Note: Includes only Category 4.1 (Upstream Emissions from Purchased Goods) and Category 4.3 (Waste Disposal).

Greenhouse Gas Emissions and Emission Intensities in the Past 2 Years

Emission Categories		Parent Company[Note 1]		Other Subsidiaries[Note 2]
		2023	2024	2024
		Emissions (tCO_2e)		
Scope 1	Stationary Combustion	0.1642	0.1925	2.6908
	Mobile Combustion	16.8783	19.8991	107.9652
	Process Emissions	0	0	0.014
	Fugitive Emissions	111.8252	123.0282	218.7645
	Total	128.8677	143.1198	329.4345
Scope 2	Purchased Electricity Consumption	678.1014	653.8960	4,695.6190
	Total	678.1014	653.8960	4,695.6190
Scope 3	Upstream Fuel and Energy Emissions	139.0819	136.6418	2,460.6414
	Waste Disposal	8.1424	40.2395	159.7305
	Total	147.2243	176.8813	2,620.3719
Total GHG Emissions		954.193	973.897	7,645.425
Revenue (in NT$ million)[Note 6]		6,910.87	7,562.87	3,072.849
GHG Emission Intensity (Scope 1 + 2)[Note 7]		0.1168	0.1054	1.6353
GHG Intensity (Scope 3)[Note 7]		0.0213	0.0234	0.8527
Total GHG Emission Intensity		0.1381	0.1288	2.4881

Note 1: The parent company includes CyberPower Systems, Inc. and CyberPower Systems, Inc. Tainan Plant.
Note 2: Other subsidiaries include Dongguan Cyber Energy Co., Ltd., Cyber Energy (Shenzhen), Inc., Cyber Power Technology (ShenZhen), Inc., Cyber Power (Shenzhen) Ltd, Best Top (Shenzhen), Inc., Ning Yuan Xian CyberPower, Inc., Cyber Power Systems Manufacturing, Inc., and Phisonic Technology Corporation.
Note 3: Energy conversion and emission factors are established according to official announcements in each region.
- Taiwan: Based on the "GHG Emission Factor Management Table" Version 6.0.4 issued by the Ministry of Environment, Republic of China.
- China: Based on the "2022 Provincial Average Electricity CO_2 Emission Factor" announced by the Ministry of Ecology and Environment, the People's Republic of China.
- Philippines: Based on the "Philippine Grid Emission Factors (2018–2020)" published by the Department of Energy, Republic of the Philippines.
- Note 4: The GHG inventory is prepared using the Operational Control Approach.
- Note 5: Global Warming Potential (GWP) factors are based on the IPCC Sixth Assessment Report (AR6).
- Note 6: GHG emission intensity is calculated based on revenue in NT$ million. Revenue sources:
- Parent company: CyberPower Systems, Inc. Parent Company Only Financial Statements
- Other subsidiaries: Cyber Power Systems, Inc. Information on Affiliated Companies

Note 7: GHG emission intensity = GHG emissions (tCO_2e) ÷ Revenue (NT$ million).

Energy Management

CyberPower's energy consumption primarily comprises purchased electricity and a small amount of fossil fuels. The electricity is mainly sourced from Taiwan Power Company, State Grid Corporation of China, China Southern Power Grid, and the Luzon-Visayas power grid in the Philippines.

Purchased electricity accounts for 62.06% of the company's total greenhouse gas (GHG) emissions, making it the primary source of emissions.

Fossil fuels—including diesel, gasoline, and liquefied petroleum gas—are primarily used for company vehicles, generators, and gas stoves, and contribute only 0.03% of total GHG emissions, reflecting a minimal carbon footprint from these sources.

In 2024, the total energy consumption reached 40,902,591.0270 megajoules. CyberPower remains committed to enhancing its energy data management practices. By leveraging data analysis to identify opportunities for energy-saving improvements, the company aims to continuously increase energy efficiency and transition toward a high-efficiency, low-carbon operational model.

Energy Consumption within the Organization in the Past 2 Years (Scope 1 + Scope 2)

(Unit: Megajoules, MJ; NT$ million)

Energy from		Parent Company[Note 1]		Other Subsidiaries[Note 2]
		2023	2024	2024
Non-renewable Sources	Purchased Electricity	4,941,629.4874	4,966,298.9999	34,154,940.3097
	Diesel	2,207.9596	2,637.6840	1,296,958.5426
	Automotive Gasoline	233,786.0067	282,415.8324	159,291.8971
	Liquefied Petroleum Gas	0	0	35,330.1893
	Total	5,177,623.4537	5,251,352.5163	35,646,520.9387
Renewable Sources	Purchased Renewable Energy	0	0	0
	Solar Energy	17,032.5720	13,452.4800	6,696.0000
	Biofuels	0	0	0
	Total	17,032.5720	13,452.4800	6,696.0000
Total Energy Consumed		5,194,656.0257	5,264,804.9963	35,653,216.9387
Revenue[Note 4]		6,910.87	7,562.87	3,072.849
Energy Intensity[Note 5]		751.6646	696.1385	11,602.6583

Note 1: The parent company includes CyberPower Systems, Inc. and CyberPower Systems, Inc. Tainan Plant.
Note 2: Other subsidiaries include Dongguan Cyber Energy Co., Ltd., Cyber Energy (Shenzhen), Inc., Cyber Power Technology (ShenZhen), Inc., Cyber Power (Shenzhen) Ltd, Best Top (Shenzhen), Inc., Ning Yuan Xian CyberPower, Inc., Cyber Power Systems Manufacturing, Inc., and Phisonic Technology Corporation.
Note 3: Energy consumption figures are calculated based on calorific values published by the Energy Administration.
Note 4: Energy intensity is calculated based on revenue in NT$ million. Revenue sources:
- Parent company: CyberPower Systems, Inc. Parent Company Only Financial Statements
- Other subsidiaries: Cyber Power Systems, Inc. Information on Affiliated Companies

Note 5: Energy Intensity = Energy Consumption (megajoules, MJ) ÷ Revenue (NT$ million).

Water Resource Management

All CyberPower locations source their water from local municipal water systems and do not have private groundwater wells. The overall water supply is stable, with most sites located in areas with low to medium water risk. In Taiwan, water is supplied by the Taipei Water Department and Taiwan Water Corporation; in China, each factory receives urban and industrial water from local water authorities; the Philippines site also uses the local public water supply system.

The total water consumption in 2024 was 7.882 million liters. CyberPower actively implements water-saving measures by continuously replacing old equipment, installing water-saving facilities, and promoting water efficiency internally to reduce reliance on local water resources and mitigate potential risks associated with operations.

Water Consumption over the Past 2 Years

(Unit: million liters, ML; NT$ million)

Water Usage	Parent Company[Note 1]		Other Subsidiaries[Note 2]
	2023	2024	2024
Water Withdrawal	8.849	7.882	88.696
Water Discharge	8.849	7.882	88.696
Water Consumption	0	0	0
Revenue[Note 3]	6,910.87	7,562.87	3,072.849
Water Intensity	0.0012804	0.0010422	0.0288643

Note 1: The parent company includes CyberPower Systems, Inc. and CyberPower Systems, Inc. Tainan Plant.
Note 2: Other subsidiaries include Dongguan Cyber Energy Co., Ltd., Cyber Energy (Shenzhen), Inc., Cyber Power Technology (ShenZhen), Inc., Cyber Power (Shenzhen) Ltd, Best Top (Shenzhen), Inc., Ning Yuan Xian CyberPower, Inc., Cyber Power Systems Manufacturing, Inc., and Phisonic Technology Corporation.
Note 3: The company has no significant process water use or high water consumption demands. There is no substantial evaporation, adsorption, or other water loss during water usage. Therefore, water withdrawal and water discharge are estimated to be approximately equal, and water consumption can be considered zero.
Note 4: Water intensity is calculated based on revenue in NT$ million. Revenue sources:
• Parent company: CyberPower Systems, Inc. Parent Company Only Financial Statements
• Other subsidiaries: Cyber Power Systems, Inc. Information on Affiliated Companies
Note 5: Water Intensity = Water Usage (million liters, ML) ÷ Revenue (NT$ million).

Waste Management

The business waste generated by CyberPower mainly includes domestic waste, plastic waste, and paper waste. To reduce the environmental and operational impacts of waste, the company follows a life cycle approach by implementing circular economy measures focused on source reduction, enhancing resource reuse, and adopting recycled materials.

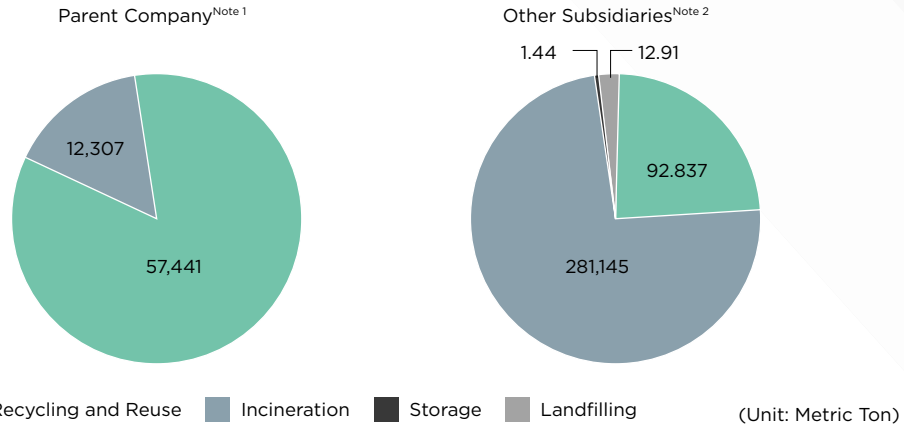
All waste is legally entrusted to qualified contractors for collection and disposal. The waste management processes are regularly audited to ensure compliance with local regulations. Through employee education and operational management, CyberPower continuously strengthens waste sorting and recycling mechanisms to achieve waste reduction and resource circulation goals throughout its operations.

Waste Disposal Amounts in the Past 2 Years

(Unit: Metric Tons)

Type of Waste	Parent Company[Note 1]		Other Subsidiaries[Note 2]
	2023	2024	2024
Outsourced General Industrial Waste	69.1435	69.7480	293.5550
Outsourced Hazardous Industrial Waste	0	0	94.8135
Total	69.1435	69.7480	388.3685

Waste Disposal Methods

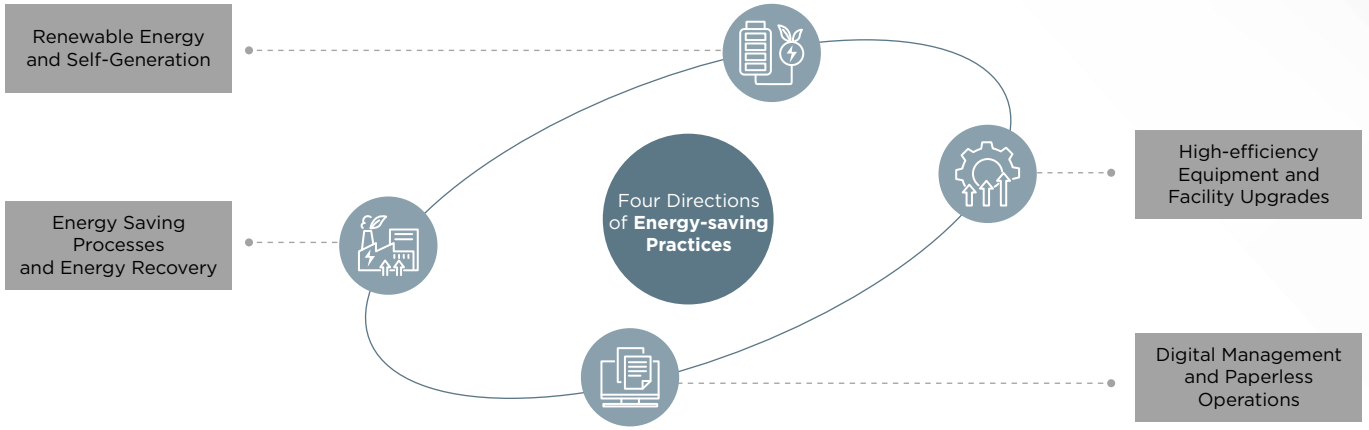


Note 1: The parent company includes CyberPower Systems, Inc. and CyberPower Systems, Inc. Tainan Plant.
Note 2: Other subsidiaries include Dongguan Cyber Energy Co., Ltd., Cyber Energy (Shenzhen), Inc., Cyber Power Technology (ShenZhen), Inc., Cyber Power (Shenzhen) Ltd, Best Top (Shenzhen), Inc., Ning Yuan Xian CyberPower, Inc., Cyber Power Systems Manufacturing, Inc., and Phisonic Technology Corporation.

Energy Saving and Carbon Reduction

Energy-saving Practices

CyberPower continuously optimizes its operational processes and facility management by implementing a variety of energy-saving measures to reduce energy consumption and enhance energy efficiency. These include the adoption of renewable energy systems, integration of energy recovery mechanisms during testing phase, deployment of intelligent air conditioning control systems, and promotion of paperless practices. By effectively consolidating energy-saving resources across both production and administrative functions, CyberPower is actively advancing toward a high-efficiency, low-carbon sustainable business model.



Featured Action | Renewable Energy Adoption and Performance

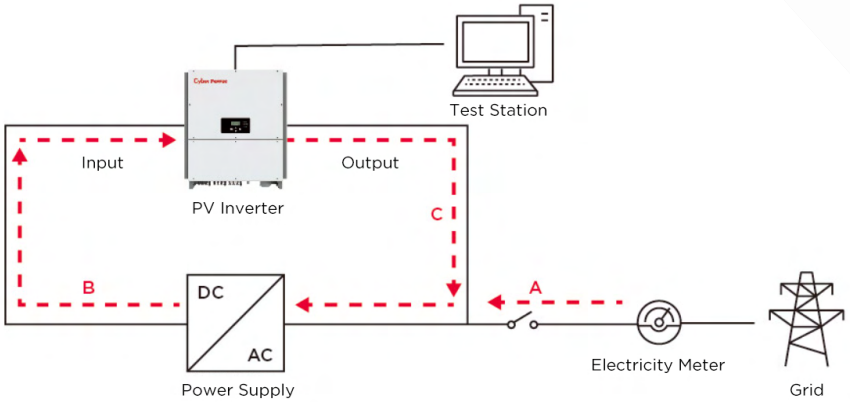
CyberPower is actively implementing solar power systems across its operations to increase the share of renewable energy and reduce operational carbon emissions. Solar installations are deployed at various sites based on local conditions and are integrated with energy management software to improve energy efficiency and enhance data transparency.

- Taipei Headquarters: In 2024, the total solar power generation reached 3,736 kWh. During the same year, the solar panels at the Taipei headquarters building were upgraded, achieving an installed capacity of 25.81 kWp. The new panels demonstrated a 156.05% improvement in efficiency compared to the previous models.
- Cyber Power (Shenzhen) Ltd: In 2024, the site generated a total of 1,860 kWh, providing a stable supply of electricity for factory operations.



Featured Action | Energy Efficiency in Manufacturing Processes and Energy Recovery

In addition to continuously developing high-efficiency products, CyberPower actively implements energy efficiency optimization throughout its manufacturing processes. During the testing phase, the electricity generated from solar inverters and UPS systems is fed back into the grid, offsetting a portion of the power consumed during production. This energy recovery approach helps reduce overall electricity demand and carbon emissions. Guided by a low-carbon manufacturing strategy, the company continuously enhances energy performance through practical actions to fulfill its carbon reduction commitments.



Featured Action ▌High-efficiency Equipment Implementation for Energy Optimization

CyberPower continuously improves the efficiency of its production facilities by gradually replacing high-consumption equipment to achieve its conservation and carbon reduction goals.

- Ning Yuan Xian CyberPower, Inc.: In 2024, a new variable frequency air compressor was installed to replace the traditional fixed frequency model. The variable model adjusts its operating frequency according to actual air pressure demands, effectively reducing energy waste. Operational observations indicate that the new equipment can save approximately 15% of electricity consumption compared to the older model. This not only lowers production electricity intensity but also improves system stability and lifespan, demonstrating CyberPower's tangible progress in promoting high-efficiency manufacturing.

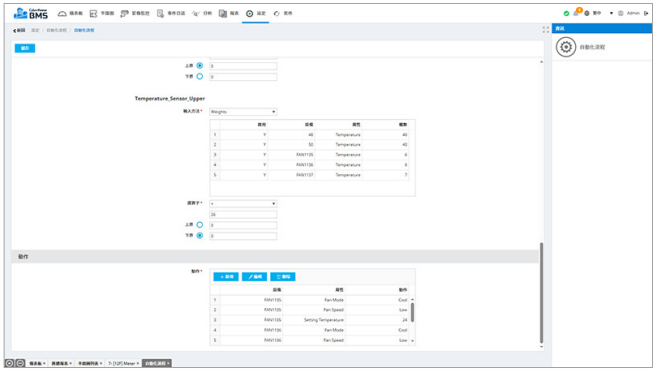
Featured Action ▌Paperless Operations and Resource Efficiency

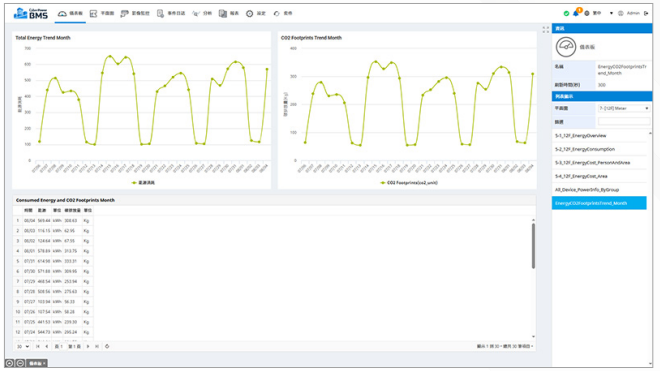
CyberPower continues to strengthen operational efficiency through digital transformation, promoting paperless office practices to reduce paper consumption and carbon emissions.

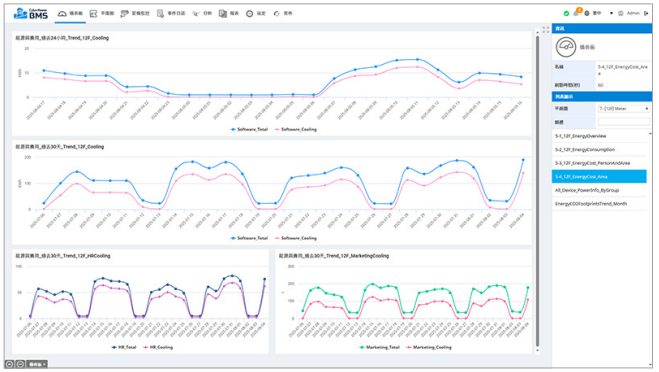
- Taipei Headquarters: Since 2011, CyberPower has been planning and implementing online approval system. In order to streamline our approval processes, the System Development Department established a state-of-the-art business process management system that provides seamless approval modules to all units.
  In 2024, a total of 162,391 approval processes were completed, estimated to have saved approximately 298,000 sheets of A4 paper, equivalent to a carbon reduction of about 1.86 metric tons CO_2e. This system has now replaced most paper-based approvals, and relevant units continue to expand its functionalities and integrate various workflows for cloud-based management.
- Cyber Power (Shenzhen) Ltd: Since July 2024, a paperless process has been implemented in gatehouse management, fully digitizing visitor registration and security checks. This has improved data integration efficiency and reduced the burden of paper-based tasks.
- Ning Yuan Xian CyberPower, Inc.: A paperless maintenance record system was introduced for elevator maintenance operations, replacing traditional paper records with online logging and storage. This effectively simplifies maintenance processes while enhancing transparency and environmental benefits.

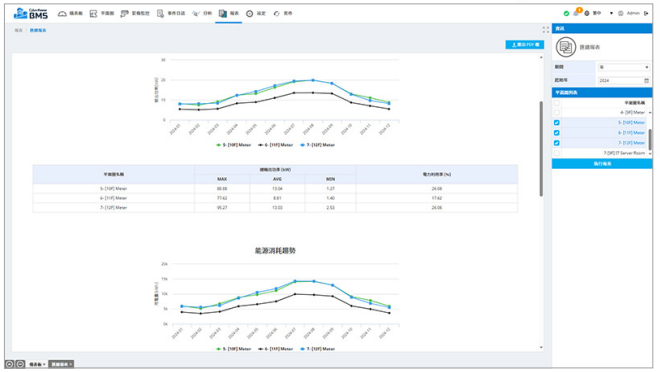
Featured Action ▌Adoption of Smart Building Management System to Enhance Energy Efficiency

Since 2021, CyberPower's Taipei headquarters has implemented a Building Management System (BMS) that connects to on-site temperature sensors, transmitting real-time environmental data to the system backend. Based on preset temperature ranges, the system automatically adjusts the operation mode of air conditioning. When the ambient temperature drops too low, the system switches the air conditioning to ventilation mode and reactivates cooling once the temperature rises. This approach effectively reduces energy consumption caused by prolonged compressor operation while enhancing indoor comfort. This intelligent control mechanism helps improve energy use efficiency and supports the company's corporate energy-saving and carbon reduction goals.









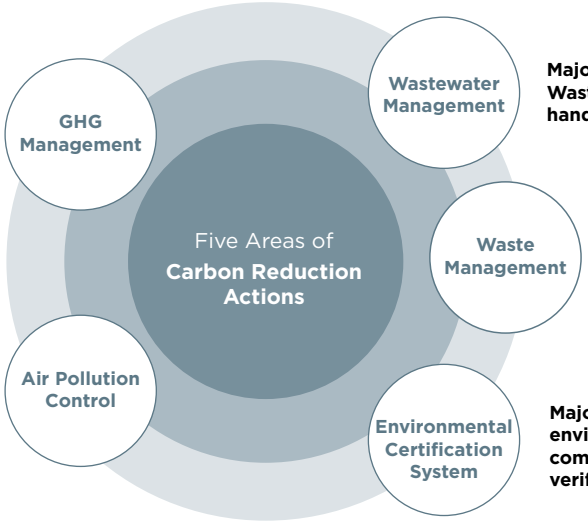
Carbon Reduction Initiatives

In response to climate change trends and to realize its sustainable business vision, CyberPower continuously strengthens its greenhouse gas (GHG) management mechanisms. Through institutionalized processes, risk identification, and site monitoring, the company implements effective carbon emission control and pollution reduction measures, demonstrating its corporate responsibility in carbon reduction. CyberPower conducts GHG inventories following ISO 14064-1 and gradually expands its organizational boundaries. The company's manufacturing sites also adopt the ISO 14001 Environmental Management System to identify significant environmental aspects from the source, plan control measures, operational standards, and contingency protocols. This creates a preventive and continuous management framework that undergoes regular third-party verification to ensure transparency of environmental data in compliance with regulations and international standards.

At the operational management level, CyberPower's major plants focus on reducing pollution sources and optimizing resource usage. Clear emission standards and control mechanisms are established for high-risk items including greenhouse gases, exhaust gases, wastewater, and waste, minimizing the environmental impact of operational activities. Looking ahead, the company will continue to enhance the completeness of environmental management data, deepen data utilization, and strengthen cross-departmental collaboration, laying a solid foundation for its net-zero transition and improved corporate climate resilience.

9 of our global sites implement ISO 14064, gradually expanding inventory boundaries to consolidate carbon emission data for reduction management.

Major sites activated carbon filtration systems are installed for specialized processes to control non-methane hydrocarbons (NMHC) emissions. Regular concentration testing and equipment maintenance are conducted in compliance with local environmental regulations.



Major sites have separate discharge pipelines for production and living areas. Wastewater is treated via neutralization tanks and sedimentation ponds, then handled by certified units. Testing is done before discharge, with records kept.

Major sites establish dedicated storage areas and disposal logs per the Solid Waste Control Procedure. Hazardous and electronic wastes are regularly handled by certified contractors, with transportation documents retained for inspection.

Major sites are ISO 14001 certified, regularly identifying significant environmental issues. Improvement actions focus on electricity use, compressed air systems, and chemical management, with implementation verified through internal and external audits.

Environmental and Safety Certifications

ISO 14001:2015 Environmental Management System



CyberPower Tainan Plant



Cyber Power (Shenzhen) Ltd

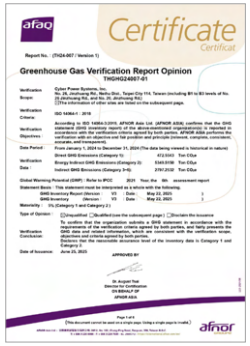


Dongguan Cyber Energy Co., Ltd.



Cyber Power Systems Manufacturing, Inc.

ISO 14064-1:2018 Greenhouse Gas Inventory



Cyber Power Systems, Inc.

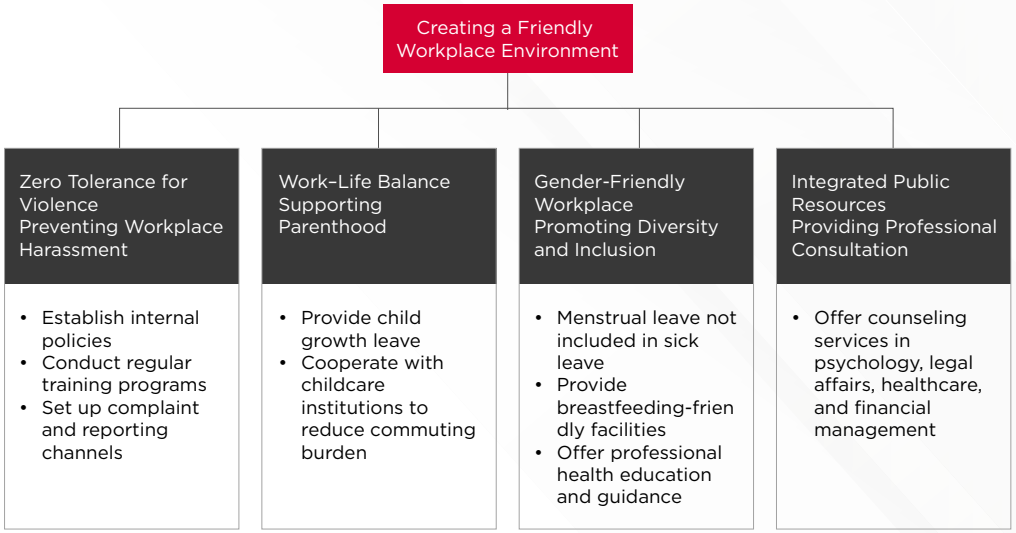


07 Social Inclusion

Human Resources Overview
Employee Turnover
Employee Rights and Compensation
Talent Attraction and Retention
Safe and Secure Workplace Environment
Workplace Health Services
Social Care for the Common Good

Human Resources Overview

CyberPower is committed to creating a diverse, equitable, and discrimination-free workplace. The company upholds the principle of placing talent in suitable positions as the foundation for recruitment, development, promotion, and retention. We are firmly committed to providing equal opportunities and ensuring that no employee is treated differently based on race, nationality, gender, age, political stance, or religious belief. Every employee is given equal conditions to fully realize their potential and contribute their strengths.
The company values talent development and the protection of compensation and benefits. Through a comprehensive training system and incentive mechanisms, we support employees in continuous learning and professional advancement, thereby strengthening overall organizational effectiveness. CyberPower encourages employees to grow together with the company and work hand in hand to create sustainable performance and long-term value.



Workforce Distribution

As of the end of 2024, CyberPower had a total of 381 employees in Taiwan, an increase of 10 from the previous year. The company is committed to building a diverse and inclusive workforce, with male and female employees accounting for 66.67% and 33.33%, respectively. Our employees represent multiple generations, ranging in age from 18 to over 60, and possess educational backgrounds from high school to doctoral degrees. CyberPower also ensures equal employment opportunities for individuals with disabilities, promoting diversity, mutual prosperity, and the overall competitiveness of the company.

Employee Types by Region

Employee Classification (Unit: Headcount)		Taipei Headquarters		Tainan Factory		Overseas Regions		Total		
		Male	Female	Male	Female	Male	Female	Male	Female	Total
By Contract	Permanent Employees (Indefinite Contracts)	203	111	34	14	17	2	254	127	381
	Contract Employees (Term Contracts)	0	0	0	0	0	0	0	0	0
By Working Hours	Full-time Employees	203	111	34	14	17	2	254	127	381
	Part-time Employees	0	0	0	0	0	0	0	0	0
	Employees without Guaranteed Working Hours (Temporary Employees)	0	0	0	0	0	0	0	0	0
Total Employees by Gender and Region		203	111	34	14	17	2	254	127	381

Note 1: Full-time Employees: Employees who work 40 hours per week as defined by the Taiwan "Labor Standards Act."
Note 2: Part-time Employees: Employees who work less than 40 hours per week.
Note 3: CyberPower does not employ temporary or other employees without guaranteed working hours.

Changes in the Number of Employees in the Past 3 Years

Employee Types	2022	2023	2024
Employees	354	371	381
Non-employees	1	1	1

Note 1: The total number of employees is based on the figures as of December 31 each year.
Note 2: Non-employees: This category includes workers not directly employed by the company but whose work is controlled by it. It covers temporary workers dispatched by labor agencies, contractors, and personnel from building management centers tasked with CyberPower's business. Main job types include environmental cleaning, gardening services, air conditioning maintenance, and security. This year, only non-employee data from the cleaning company is disclosed, but we will continue to improve statistics for relevant workers in the future.

Diverse and Abundant Employment Opportunities

CyberPower provides equal employment opportunities regardless of gender, age, or ethnicity, and complies with government regulations to ensure job opportunities for other minority groups, fostering workforce diversity.

According to the company's year-end employee statistics, female employees account for 33.33% of the total workforce, and female supervisors represent 31.25% of all supervisory positions. Employees aged over 50 make up 13.65% of the total workforce. In compliance with government regulations, CyberPower employs individuals with disabilities, currently hiring 6 such employees, accounting for 1.57% of the total workforce, exceeding the legal requirement of 4 employees.

In accordance with the regulations of the National Immigration Agency and local employment service authorities, the company is introducing foreign migrant workers. Dormitories located near the company are arranged to accommodate these workers, allowing them to live with fellow nationals and adapt more easily to their new environment. In addition, the company has enhanced internal systems and printed materials by adding English interfaces and instructions to protect the rights and working conditions of foreign migrant workers.

Employee Job Categories Overview

Job Categories		Gender		Age			Others
		Male	Female	Under 30	Between 30~50	Over 50	Individuals with Disabilities
Managerial Personnel (Total: 48)	Number	33	15	0	33	15	2
	Percentage	68.75%	31.25%	0%	68.75%	31.25%	4.17%
Non-managerial Personnel (Total: 333)	Number	221	112	51	245	37	4
	Percentage	66.37%	33.63%	15.32%	73.57%	11.11%	1.20%
Number of Employees in Each Diverse Category		254	127	51	278	52	6
Percentage of Total Employees		66.67%	33.33%	13.39%	72.97%	13.65%	1.57%

Note 1: There are 48 managerial personnel and 333 non-managerial personnel, bringing the total number of employees to 381.
Note 2: Managerial personnel include the president, division heads, and department heads, corresponding to the organizational chart of CyberPower.

Local Management Representation

Region		Manager	
		Local Personnel	Non-local Personnel
Taiwan	Number	48	0
	Percentage	100%	0%

Employee Turnover

New Hires

To meet the company's ongoing talent needs for continued growth, CyberPower hired 51 new employees in 2024. Among them, 32 were male and 19 were female. Of the new hires, 41.18% were under 30 years old, 56.86% were between 30 and 50 years old, and 1.96% were over 50 years old.

Statistics on the Gender and Age Distribution of New Hires

Category	Male		Female		Subtotal	
	Number	Percentage	Number	Percentage	Number	Percentage
Under 30	12	3.15%	9	2.36%	21	5.51%
Between 30-49	19	4.99%	10	2.62%	29	7.61%
50 and above	1	0.26%	0	0.00%	1	0.26%
Subtotal of New Hires	32	8.40%	19	4.99%	51	13.39%

Note: New Hire Rate = Number of new employees in each category ÷ Total number of employees at the end of the period (381 employees)

Statistics on the Regional and Age Distribution of New Hires

Age	Gender	Taipei Headquarters	Tainan Factory	Expatriate Employees	Group Total	
					Number	Percentage
Under 30	Male	8	4	0	12	3.15%
	Female	9	0	0	9	2.36%
Between 30-49	Male	12	5	2	19	4.99%
	Female	8	1	1	10	2.62%
50 and above	Male	1	0	0	1	0.26%
	Female	0	0	0	0	0.00%
Number of New Hires by Region		38	10	3	51	13.39%
New Hire Rate by Region		12.10%	20.83%	15.79%	13.39%	

Note 1: New Hire Rate by Region = Number of new employees in each category ÷ Total number of employees in that region at the end of the period (Taipei Headquarters: 314 employees, Tainan Factory: 48 employees, Overseas Regions: 19 employees)
Note 2: Group Total Percentage = Number of employees in that region ÷ Total number of employees at the end of the period (381 employees)

Resignation and Retention

In terms of employee retention, CyberPower had a total of 43 departing employees in 2024, comprising 23 males and 20 females, resulting in an overall turnover rate of approximately 11.29%. When employees submit their resignation requests, both the supervisor and the Human Resource Department conduct interviews to understand the reasons for their departure. If suitable internal transfer opportunities are available, we prioritize assisting employees with the transition. If no opportunities are available for retention, we encourage employees to provide feedback so we can optimize our management practices. Moving forward, unit supervisors and the Human Resource Department will maintain positive relationships and communication with departing employees to enhance rehire opportunities. The company will continue to strengthen work-life balance, plan incentive rewards and benefits, enhance supervisory skills, and provide career development opportunities to promote employee retention.

Statistics on Departing Employees by Gender and Age Distribution

Category	Male		Female		Subtotal	
	Number	Percentage	Number	Percentage	Number	Percentage
Under 30	8	2.10%	3	0.79%	11	2.89%
Between 30-49	15	3.94%	17	4.46%	32	8.40%
50 and above	0	0.00%	0	0.00%	0	0.00%
Subtotal of Departing Employees	23	6.04%	20	5.25%	43	11.29%

Note 1: Turnover Rate = Number of departing employees in each category ÷ Total number of employees at the end of the period (381 employees)
Note 2: Departing employees include those who leave the organization voluntarily or due to dismissal, retirement, or work-related fatalities.

Statistics on Departing Employees by Region and Age Distribution

Age	Gender	Taipei Headquarters	Tainan Factory	Expatriate Employees	Group Total	
					Number	Percentage
Under 30	Male	6	2	0	8	2.10%
	Female	3	0	0	3	0.79%
Between 30-49	Male	8	4	3	15	3.94%
	Female	16	0	1	17	4.46%
50 and above	Male	0	0	0	0	0.00%
	Female	0	0	0	0	0.00%
Number of Departing Employees by Region		33	6	4	43	11.29%
Turnover Rate by Region		10.51%	12.50%	21.05%	11.29%	

Note 1: Turnover Rate by Region = Number of departing employees in each category ÷ Total number of employees in that region at the end of the period (Taipei Headquarters: 314 employees, Tainan Factory: 48 employees, Overseas Regions: 19 employees)
Note 2: Group Total Percentage = Number of employees in that region ÷ Total number of employees at the end of the period (381 employees)
Note 3: Departing employees include those who leave the organization voluntarily or due to dismissal, retirement, or work-related fatalities.

Unpaid Parental Leave

CyberPower complies with the "Gender Equality in Employment Act" and supports employees' rights to raise their children, ensuring their entitlement to parental leave. Employees who have worked at the company for at least 6 months may apply for unpaid parental leave before their child turns 3 years old, with a maximum leave period of 2 years. During the parental leave, employees can continue to participate in the company's original social insurance programs.

Statistics on Unpaid Parental Leave

	Male	Female	Total
Number of employees eligible for unpaid parental leave[Note 1] (a)	21	10	31
Number of unpaid parental leave applications (b)	0	2	2
Unpaid parental leave application rate (b / a)	0.00%	20.00%	6.45%
Number of employees expected to reinstated from unpaid parental leave (c)	0	3	3
Number of employees reinstated from unpaid parental leave (d)	0	3	3
Unpaid parental leave reinstatement rate (d / c)	--	100.00%	100.00%
Number of employees reinstated from unpaid parental leave in 2023 (e)	0	1	1
Number of employees reinstated from unpaid parental leave in 2023 and stayed for 1 year[Note 2] (f)	0	0	0
Unpaid parental leave reinstatement rate (f / e)	--	0.00%	0.00%

Note 1: The statistics are calculated based on the number of employees who applied for maternity or paternity leave over the past three years (2022-2024).
Note 2: The actual date reinstated was in 2023, and they have remained employed for at least one year after returning.

Employee Rights and Compensation

2024 Material Topic: Management of "Human Rights Policy"

Material Topics	Human Rights Policy
GRI Standards	GRI 401-1 New employee hires and employee turnover GRI 401-2 Benefits provided to full-time employees that are not provided to temporary or part-time employees GRI 401-3 Parental leave GRI 402-1 Minimum notice periods regarding operational changes GRI 405-1 Diversity of governance bodies and employees GRI 405-2 Ratio of basic salary and remuneration of women to men GRI 406-1 Incidents of discrimination and corrective actions taken
SDGs	
Policy or Commitment	To protect employee rights, we establish a diverse and equitable work environment, ensuring that every employee enjoys basic benefits and fair treatment, thereby promoting harmonious labor relations.
Indicators and Goals	Short-term Goals (1-2 Years) • Provide vacation benefits exceeding the "Labor Standards Act" • Actively implement a process for explaining extended work hours and provide overtime pay in compliance with the law, creating a friendly and rights-respecting working hours system • Hold at least 3 health promotion activities annually to establish a balanced physical and mental health environment • Implement measures to create a friendly workplace, preventing workplace violence and sexual harassment, signing childcare service agreements, offering child growth leave, and providing a secure nursing room, ensuring employees work in a safe and reassuring environment • Plan and promote workplace experience activities for employees' children to help them gain early exposure to workplace culture Mid-term Goals (2-5 Years) • Establish a clear performance-linked reward system • Enrich benefits offerings and design a flexible selection platform Long-term Goals (5+ Years) • Maintain a diverse and flexible work environment, actively fostering a culture that promotes career development and enhances employee engagement
Effectiveness Tracking Mechanism	• Employee complaint hotline and performance feedback mechanism • Regular internal audits • External salary survey reports
Annual Actions and Measures	• Address employee complaints promptly by taking appropriate measures and conducting investigations, with ongoing follow-up after case closure • Optimize management processes to reduce risks associated with management • Adjust overall compensation based on external salary survey reports and improve retention rates of key talent • Based on individual performance evaluation results, the average salary increase from 2022 to 2024 was above 5% each year • According to the major resolution of the 2023 labor-management meeting, the company introduced foreign migrant workers as factory operators in 2024 • In accordance with government regulations, the company employed 6 individuals with disabilities in 2024, accounting for 1.57% of the total workforce, exceeding the legal requirement of 4 employees • In 2024, CyberPower received one complaint, which has been resolved

Human Rights and Labor Rights Protection

CyberPower respects the fundamental human rights of all employees, customers, and stakeholders, and recognizes and supports multiple international human rights conventions, including the Universal Declaration of Human Rights, the "United Nations Global Compact," and the "International Labour Organization Conventions." These principles cover freedom of association, care for vulnerable groups, the prohibition of child labor, the elimination of all forms of forced labor, and the elimination of employment and occupational discrimination.

In accordance with the "United Nations Guiding Principles on Business and Human Rights (UNGPs)", CyberPower has established a "Human Rights Policy" to define the scope of application and principles of implementation.

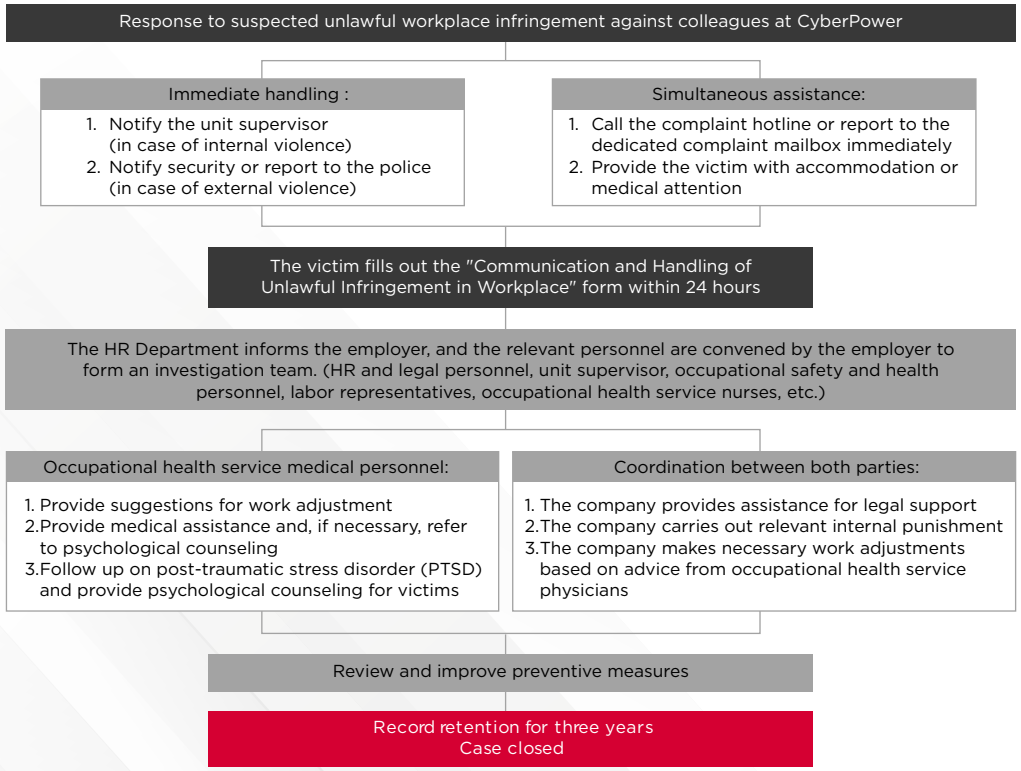
CyberPower values labor rights and complies with labor regulations and the "Gender Equality in Employment Act" set by governing authorities. We also reference international human rights conventions to establish "Work Rules" and related management procedures that protect various labor rights, including minimum wage, working hours (including overtime), insurance, leave, pension systems, and notice periods for contract termination. We provide equal employment opportunities and treatment, ensuring no discrimination based on race, color, gender, religion, political beliefs, nationality, or social origin. In 2024, the company did not encounter any significant risks or incidents related to child labor, forced labor, discrimination, or other violations of labor and human rights.

CyberPower is committed to creating a friendly and gender-equal workplace with a zero-tolerance policy for workplace violence. The company has established an internal complaint mechanism and formed a Sexual Harassment Complaint Committee, along with relevant policies and procedures to assist employees affected by workplace violence or sexual harassment in filing complaints and undergoing subsequent legal procedures. In addition, to safeguard employees' physical and mental well-being, the company has implemented a "Prevention Plan for Unlawful Infringement in the Performance of Duties" to prevent improper treatment of employees by employers, supervisors, colleagues, or clients — including verbal abuse, physical assault, and intimidation — thereby maintaining a safe working environment. In 2024, CyberPower received one complaint. Upon receiving the complaint, the company immediately initiated an investigation process in accordance with internal procedures, and the case has been closed.

The company's consultation and complaint channels for workplace sexual harassment and violence are as follows:

- Complaint Hotline: +886-8792-9510 ext. 3201
- Complaint Mailbox: tw.hr@cyberpower.com

Sexual Harassment and Workplace Violence Incident Handling Process



Labor Rights-related Measures

Working Hours	• Full-time employees work 8 hours per day and 40 hours per week • Under special circumstances requiring overtime, total daily work hours shall not exceed 12 hours, with a maximum of 46 overtime hours per month • According to the "Labor Standards Act," employees are entitled to overtime pay for work exceeding 8 hours in a day, and they cannot be forced to work overtime
Termination Procedures	• In the event that the company needs to terminate an employment relationship with an employee, we comply with Article 16 of the "Labor Standards Act" by providing advance notice of termination based on years of service, as well as severance pay and job-seeking leave
Labor-management Agreement	• Although the company does not have a labor union, we hold regular labor-management meetings every quarter in accordance with Article 83 of the "Labor Standards Act." Additional meetings may be convened as needed to promote labor-management cooperation, coordinate labor relations, improve working conditions, and discuss labor welfare, fostering two-way communication and negotiation • In 2024, there were no major resolutions made during the company's labor-management meetings
Significant Operational Changes	• If there are significant operational changes that may affect employee rights, the company will provide advance notice to the affected employees in accordance with the relevant provisions of the "Labor Standards Act" • During the reporting period, the company did not experience any significant operational changes

Compensation and Remuneration Standards

CyberPower offers competitive compensation, actively adhering to the "Articles of Incorporation" and labor laws. We also participate in salary surveys conducted by corporate management consulting firms to evaluate the reasonableness and competitiveness of our salary levels, serving as a reference for establishing or improving our compensation systems. Salary standards are determined based on job responsibilities, professional abilities, educational background, and years of experience, emphasizing the principle of equal pay for equal work and ensuring no gender-based disparities in overall compensation. In 2024, the ratio of basic salaries and compensation for men and women was 1:0.78. Additionally, compared to the previous year, the salary increase ratio between both genders was 1:1.10. Due to our salary confidentiality policy, the company does not disclose annual compensation-related information.

Furthermore, to attract, retain, and motivate outstanding talent, each employee's salary and bonuses are determined based on the company's profitability, the achievement of organizational goals, and individual performance, ensuring a strong positive correlation between each person's efforts and results. Since the company's establishment, there has been an annual salary adjustment. Depending on individual performance evaluation results, the average salary increase over the past three years has been above 5%.

Gender-based Compensation and Remuneration Ratios for Various Employee Categories in the Past 3 Years

Year	2022		2023		2024	
Employee Category	Male	Female	Male	Female	Male	Female
Managerial Positions	1	0.821	1	0.879	1	0.864
Non-managerial Positions	1	0.788	1	0.730	1	0.775

Note 1: Calculation: Average salary of female employees in each category ÷ Average salary of male employees in each category
Note 2: Compensation and Remuneration: Refers to annual compensation, including base salary, meal allowances, year-end bonuses, performance bonuses, and overtime pay.
Note 3: Managerial positions include division-level and department-level managers corresponding to the organizational structure of CyberPower.

Wage Level of Entry-level Staff's Key Operational Sites in the Past 3 Years

Year	Average Standard Salary for Entry-level Staff (NTD)		Average Standard Salary for Entry-level Staff / Local Minimum Wage	
	Male	Female	Male	Female
2022	39,351	46,393	1.558	1.837
2023	47,996	45,979	1.818	1.742
2024	55,029	48,896	2.003	1.780

Note 1: The "key operational sites" defined by the company refer to the operational boundaries disclosed in this report.
Note 2: The company sets the salaries of employees and other workers based on the Ministry of Labor's announced minimum wage for the year, ensuring they are not below the minimum wage.
Note 3: Entry-level Staff: Includes positions such as assistant engineer, assistant, and factory operators.
Note 4: Standard Salary: Includes base salary, meal allowances, overtime pay, and bonuses, and other regular compensations.
Note 5: The local minimum wages for 2022 to 2024 are NT$25,250, NT$26,400, and NT$27,470, respectively.

Welfare Activities

To protect the rights and interests of employees and enhance team cohesion, CyberPower provides a comprehensive benefits package for full-time employees and establishes an Employee Welfare Committee (Welfare Committee) elected by employees to manage various welfare matters. In addition to statutory benefits such as labor and national health insurance, annual leave, maternity leave, and parental leave, we also offer a wide range of employee benefits, including flexible working hours, annual employee health check-up, paid birthday leave, holiday bonuses, red envelopes during Lunar New Year, child growth leave, and team building funds, etc.

We are dedicated to improving employee well-being and creating a fulfilling workplace.

To enhance employees' well-being and promote physical and mental health, the Employee Welfare Committee provides travel and cultural activity subsidies, along with a variety of engaging events to strengthen employee satisfaction and foster a positive work environment. These initiatives not only boost team spirit and morale but also serve as a gesture of appreciation for employees' hard work and dedication.

Employee Benefits

Standard Benefits	Insurance	• Basic labor and health insurance, along with group insurance coverage for employees and their dependents (including life insurance, medical insurance, accident insurance, and travel insurance for business trips) • 16% of employees choose to include their dependents in the company's group insurance
	Leave	• Comply with the "Labor Standards Act" and provide employees with national holidays, annual leave, marriage leave, bereavement leave, sick leave, official leave, and parental leave • Paid Birthday Leave: Employees who have completed three months of service are entitled to one day of paid birthday leave during their birthday month • Child Growth Leave: Employees may apply for child growth leave on the registration day and the first day of school when their children enter elementary school • Public Welfare Leave: Employees participating in designated public welfare activities are entitled to a specified number of hours of public welfare leave
	Pension System	• Establish the "Employee Retirement Management Policy"; for employees covered under the old system of the "Labor Standards Act," the company allocates 2% of employees' monthly total salaries to their pension fund, which is deposited into a dedicated account at the Bank of Taiwan under the name of the Supervisory Committee of Business Entities' Labor Retirement Reserve; before the end of each year, if the account balance is estimated to be insufficient to cover payments for employees expected to meet retirement conditions in the following year, the company will make a one-time contribution by the end of March of the following year to cover the shortfall; for employees covered under the new system of the "Labor Pension Act," the company contributes 6% of each employee's monthly salary to their individual labor pension account, following the "Monthly Contribution Classification of Labor Pension" approved by the Executive Yuan
Working Hours	Flexible Working Hours	• In consideration of employees' family care needs and peak-hour commuting, the company offers flexible clock-in and clock-out times, allowing employees to adjust their schedules as needed - Flexible clock-in times: 08:30~09:30 - Flexible clock-out times: 17:30~18:30
Compensation and Benefits	Subsidies	• Club Activity Subsidy: To encourage employees' engagement in recreational activities, maintain physical and mental health, enrich life experiences, and foster team spirit, we provide an initial subsidy of NT$5,000 for establishing a new club along with a quarterly subsidy ranging from NT$3,000 to NT$7,500 depending on the number of club members • Travel Subsidy: Depending on the employee's length of service, each employee receives an annual subsidy ranging from NT$3,000 to NT$8,000 • Marriage, Funeral, and Congratulatory Subsidies: We provide a marriage subsidy of NT$2,000, a childbirth subsidy of NT$2,000, a funeral subsidy of NT$1,500, and a subsidy of NT$1,000 for hospitalization due to illness or injury • Arts Subsidy: Employees who have been employed for more than half a year can apply for a subsidy of NT$2,000 once a year • In addition to the subsidies provided by the Employee Welfare Committee, the company also offers allowances for marriage, childbirth, and bereavement to support employees and their families
	Holiday Bonuses	• Holiday bonuses and gift vouchers, birthday gift voucher, and Red Envelopes during Lunar New Year

Health Promotion	Annual Employee Health Checkup	• Different health check-up packages are provided based on employees' job positions. Employees can undergo health check-ups at designated medical institutions, which also conduct health analysis and follow-up tracking. In 2024, a total of 331 employees participated in health check-ups, with an investment of NT$2,640,800
Work Environment	Food and Beverage	• Freshly grounded coffee • Dining and rest areas • Snack and beverage vending machines
	Friendly Space	• Breastfeeding Room Certified by the Taipei Department of Health • Performance-oriented work autonomy and open for creativity • Promote a healthy workplace environment through tobacco hazard prevention and health promotion initiatives
Welfare Committee	Welfare Fund	• Funding Source: 0.5% of employees' monthly salaries and 0.05% of the company's total monthly revenue are deposited into a designated account, managed by the Employee Welfare Committee jointly established by both labor and management. In 2024, the total welfare fund allocation amounted to NT$5,216,525 • Scope of Expenditures: Allowances and subsidies for marriage, funerals, childbirth, insurance premiums, club activities, and company or departmental events
	e-Library	• Provides employees with access to over 110,000 e-books, magazines, and audiobooks in various categories for borrowing
	e-Gift Vouchers	• Traditional gift vouchers are limited to one channel, carry the risk of being lost, and must be collected in person. E-gift vouchers can be sent to employees via email at any time • Use the PayEasy gift platform to offer employees e-gift vouchers for department stores, supermarkets, retail shops, online malls, and more
	Annual Activities	• Birthday Celebrations: Restaurants are selected by the Welfare Committee, and all employees are invited to participate. In addition, a "Birthday Cake Application Program" is available, under which each employee receives a birthday cake during their birthday month each year to celebrate their special day • Movie Event: Employees vote to select the movie they wish to watch, and after the date is set, registration is opened for employees to attend the cinema screening • Michelin Star Dining Experience: To encourage employees to enjoy high-quality dining experiences with family and friends while promoting local ingredients, subsidies ranging from NT$1,500 to NT$8,000 are provided for employees to dine at Michelin-starred restaurants during the activity period, depending on their years of service • Static Activities: All employees can participate in company-organized activities such as handicraft workshops, competitions, and gift exchanges to strengthen camaraderie among colleagues • Outdoor Activities: Depending on the budget, one-day or two-day company trips are organized

A Date with Delicacies: 2024 Michelin Star Dining Experience

Food embodies life, taste, emotion, and happiness. The "Michelin Guide," first published in 1900, highlights exceptional restaurants and awards them one-, two-, or three-star ratings, earning its reputation as the "Bible of Gourmet Travel."

Enjoying fine cuisine is a cultural experience and an inspiration that helps relieve stress, enhance happiness, and cultivate a refined sense of taste. To allow employees to experience the charm of gourmet dining, CyberPower's Welfare Committee organized the Michelin Star Dining Experience from June 20 to October 22, 2024, providing subsidies ranging from NT$1,500 to NT$8,000 based on employees' seniority.

To satisfy employees' palates, the company carefully selected 25 Michelin one-star, two-star, Green Star, or Michelin Guide–listed restaurants in Taipei, as well as 9 selected restaurants in Tainan. CyberPower hopes that through this event, employees can take a break from their busy work schedules, enjoy exquisite meals with family and friends, and create lasting memories together.





Club Activities

To encourage employees to develop hobbies and exercise habits, CyberPower's Welfare Committee has established various clubs, including the Tabletop Game Club, Basketball Club, Running Club, Softball Club, and Yoga & Pilates Club. These clubs provide employees with opportunities to cultivate personal interests, stay active, and strengthen friendships in a relaxed setting. Through these club activities, the company aims to foster unity, expand employees' social circles, create a sense of belonging and personal growth, and enhance the vitality and cohesion of the workplace.



Basketball Club



Tabletop Game Club



Softball Club



Running Club



Yoga & Pilates Club

Talent Attraction and Retention

Diverse Training Channels

CyberPower values talent development as a means to enhance employees' professional skills, work efficiency, and overall self-worth. The company has established a comprehensive education and training system that offers diverse learning opportunities through in-person classes, online learning videos, and digital learning platforms to strengthen employees' capabilities. We have set core training policies and developed specific programs tailored to different job roles and levels. From new employee orientation and supervisory training to professional courses, dedicated personnel design tailored training initiatives to enhance the expertise of our global workforce.

In addition to implementing training programs in accordance with the annual education and training plan, CyberPower also conducts irregular internal management and professional training courses. The company provides funding and resources for external training to further enhance employees' professional skills, offering diverse learning opportunities. When necessary, employees are sent to participate in external training programs organized by external institutions to strengthen their professional competencies.

In 2024, the average internal training hours per employee were 5.7 hours, with male employees averaging 5.5 hours and female employees averaging 6 hours. The total external training hours amounted to 380.5 hours, with an annual external training expenditure of NT$148,085.

CyberPower is committed to cultivating talent and improving employee capabilities. The company encourages employees to serve as internal lecturers to share their experience and knowledge, facilitating personal career growth. A post-training feedback mechanism on teaching satisfaction is also in place to continuously improve the company's training programs.



New Employee Training

To help new employees better understand the company's operations, CyberPower provides a series of courses and post-training assessments upon onboarding. Through two days of intensive training, new employees are introduced to the company's systems, management practices, corporate brand, and products. At the end of the course, a Q&A session with the President is arranged, allowing new employees to ask questions and have face-to-face conversations.

In 2024, the total training hours for new employees amounted to 380 hours, with a completion rate of 97.4%.

Supervisory Training

In response to changes in international relations and the industrial environment, mid- and senior-level managers are expected to demonstrate strong sensitivity and problem-solving abilities. The company actively arranges management training courses to help managerial employee enhance their knowledge in areas such as patents, regulations, and organizational strategy.

In 2024, the total training hours for supervisors amounted to 188.5 hours, with a completion rate of 100%.

Professional Training Programs

At CyberPower, we aim to enhance the professional capabilities of employees at all levels by offering a series of employee-centered courses focused on job-related knowledge, skills, and behavioral development. These comprehensive, foundational, and inspiring courses are designed to motivate our employees and improve overall performance.

In 2024, CyberPower's total professional training hours amounted to 1,080.5 hours, with a completion rate of 92.2%.

Employee Training Status

Employee Category	Calculation Method	Male	Female	Subtotal
Managerial Positions	Total number of employees during the reporting period (A1)	31	15	46
	Training hours during the reporting period (B1)	130.5	58	188.5
	Average training hours per employee during the reporting period (B1 / A1)	4.2	3.9	4.1
Non-managerial Positions	Total number of employees during the reporting period (A2)	223	112	335
	Training hours during the reporting period (B2)	1276.5	701.5	1978
	Average training hours per employee during the reporting period (B2 / A2)	5.7	6.3	5.9
Total	Total number of employees during the reporting period (Q)	254	127	381
	Total training hours at the end of the reporting period (R)	1407	759.5	2166.5
	Average training hours per employee (R / Q)	5.5	6	5.7

Note: Managerial positions include the president, division heads, and department heads, corresponding to the organizational structure of the company.

On-the-job Training Courses and Participation Status

Course Category	Course Hours	Number of Participant	Completion Rate
R&D and Manufacturing	8	241	93.0%
Administrative Operations	5	788	94.5%
Legal Compliance	1.5	220	97.7%
Total	14.5	1,249	95.1%

Note: Completion Rate = Number of participants ÷ Number of intended participants

Performance and Career Development

CyberPower values employee career development and has established a comprehensive promotion and compensation system, along with regular performance evaluations, to encourage employees to continuously improve their work and pursue personal growth. New employees undergo a probationary assessment within their first three months, while employees with over three months of service are evaluated once a year. Performance reviews with supervisors focus on work performance, career aspirations, professional development, and plans for the upcoming year. We link evaluation results to human resource actions such as salary adjustments, promotions, rewards, transfers, or coaching to facilitate organizational management and human capital development. In 2024, 99.5% of CyberPower's employees completed their performance evaluations.

Performance Evaluation Process

Self-evaluation

- Set the performance review form with appropriate evaluation criteria according to employees' job responsibilities
- Concretely and clearly state this year's individual work achievements and next year's work goals and plans

Initial Review / Review

- Supervisors should conduct "performance interviews" and record key discussion points from the interviews in the online form.
- Two-way communication must be carried out if the assessment score difference is 10 points or more. Employees with scores of 90 or above should highlight their key contributions, while those with scores below 70 should engage in communication to specify the facts or reasons behind their scores and discuss improvement plans.

Approval

Employee Performance Review

Employee Category	Calculation Method	Male	Female	Subtotal
Managerial Positions	Total number of employees at the end of the reporting period (A1)	33	15	48
	Number of employees who receive regular performance and career development reviews (B1)	32	14	46
	Percentage (B1 / A1)	97.0%	93.3%	95.8%
Non-managerial Positions	Total number of employees at the end of the reporting period (A2)	221	112	333
	Number of employees who receive regular performance and career development reviews (B2)	221	112	333
	Percentage (B2 / A2)	100.0%	100.0%	100.0%
Total	Total number of employees at the end of the reporting period (R)	254	127	381
	Total number of employees who receive regular performance and career development reviews (Q)	253	126	379
	Proportion of employees who receive regular performance and career development reviews (Q / R)	99.6%	99.2%	99.5%

Note 1: The total number of employees during the assessment period is based on those employed as of December 31 of the reporting year (employees who joined in their first three months are excluded from the assessment).
Note 2: Managerial positions include the president, division heads, and department heads, corresponding to the organizational structure of the company.

Safe and Secure Workplace Environment

Occupational Health and Safety

CyberPower is committed to creating a safe, healthy, and inclusive workplace environment. Centered on prevention, the company proactively identifies and assesses potential risks in the work environment, implements health promotion and safety improvement measures, and ensures the physical and mental well-being of employees. Through a well-established occupational safety and health management system, CyberPower safeguards workplace safety while promoting a culture of work-life balance to enhance productivity and employee well-being.

The company continues to strengthen occupational safety and health management systems and procedures. In 2024, CyberPower maintained zero occupational injuries, with no occupational diseases or major workplace accidents reported. The voluntary participation rate in health promotion programs reached 68%, exceeding expectations. Annual activities include workplace inspections, hazard identification and risk assessments, employee health check-ups, and surveys to integrate health management resources and enhance employees' awareness and participation in workplace health initiatives. The company aims to fully implement the occupational safety and health management system by 2026 and obtain ISO 45001 certification by 2028.

CyberPower promotes a safe and healthy workplace through the following actions:

- Regular training for occupational safety and health personnel, while strengthening safety education for new employees;
- Continuous workplace hazard assessments and improvements to office and production environments, such as installing emergency call bells, motion-sensor lighting, assistive devices, and handling equipment;
- Promoting a culture of work-life balance through walking events and diverse health seminars;
- Achieving the goal of zero serious occupational injuries or diseases while maintaining a high participation rate in health promotion programs.

Through the dual approach of system implementation and cultural promotion, CyberPower aims to build a workplace where all employees participate actively, risks are effectively controlled, and a healthy, safe, and friendly environment is achieved.

Occupational Safety and Health Management System

At CyberPower, we prioritize the occupational safety and health of our employees. To ensure the safety and well-being of all staff members, we strictly adhere to all relevant laws and regulations, regularly conduct environmental safety and health inspections, and consistently evaluate their efficacy. Since 2016, we have insured our offices and business premises with a public liability insurance coverage of US$10 million, further bolstering the protection of workplaces.

We implement occupational safety management plans and initiatives in accordance with the "Occupational Safety and Health Act" and other relevant regulations. We have established the "Occupational Safety and Health Code of Practice" and the "Occupational Safety and Health Management Plan." The PDCA (Plan-Do-Check-Act) approach is applied across 6 key areas to ensure continuous quality management, with ongoing occupational hazard risk assessments and enhancements to the occupational safety and health management system. Each department, in compliance with regulations, establishes safety units, and appoints management personnel and first aid staff to comprehensively prevent occupational accidents.

Workers Covered by the Occupational Safety and Health Management System

Site	Number of Employees	Number of Non-employees	Coverage Rate
Taipei Headquarters	333	1	87.43%
Tainan Factory	48	0	12.57%
Total	381	1	100%

Note: Coverage rate calculation: Total number of people covered by the occupational safety and health system (number of employees + number of non-employees) ÷ Total number of company workers.

Occupational Safety and Health Management System

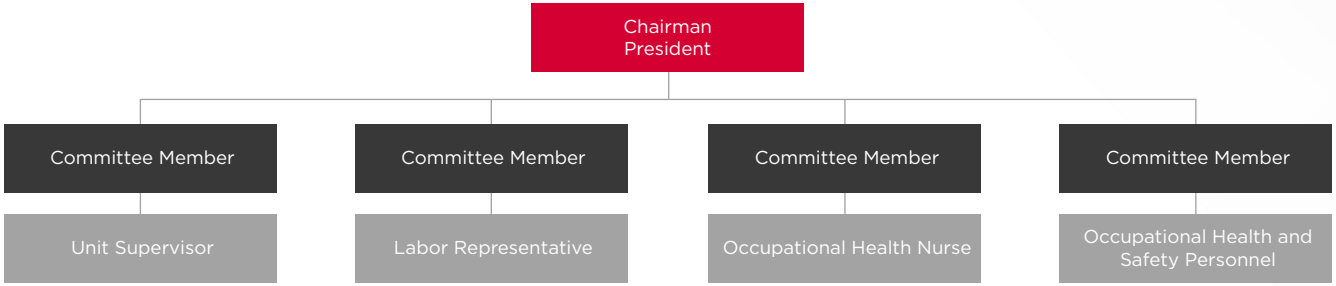
6 Key Aspects	Measures
Safety and Health Education and Training, and Disaster Prevention Drill	• Provide safety training and regular retraining for employees and contractors • Deliver education and training for first aid personnel and dedicated environmental safety personnel
Work Environment Improvement	• Assess and improve the work environment to reduce the risk of work-related injuries and diseases
Occupational Safety and Health Regulations Updates and Compliance	• Regularly review and update the company's occupational safety and health policies to ensure compliance with the latest regulatory requirements
Accident and Disaster Response	• Establish standard operating procedures (SOP) for reporting and handling accidents and disasters, analyzing incidents, investigating causes, and reviewing improvement items
Occupational Health Monitoring and Assessment	• Conduct regular occupational health check-ups for employees, with risk assessments and health promotion plans based on the results
Health Protection Measures for Specific Groups	• Maternity Health Protection Measures: Provide maternity health assessments and work adjustments for pregnant and postpartum women, ensuring the physical and mental health of female workers during pregnancy, childbirth, and breastfeeding periods. Additionally, facilities such as nursing rooms are provided. • Develop occupational safety and health management measures for contractors

Occupational Safety and Health Committee

To safeguard employee rights, CyberPower has established the Occupational Safety and Health Committee in compliance with the Occupational Safety and Health Management Regulations. The committee consists of 11 members, including 4 labor representatives, with labor representation exceeding one-third of the total members.

The committee is responsible for reviewing company regulations, rules, and plans related to occupational safety and health, and convenes quarterly meetings. Through the planning, implementation, evaluation, and improvement of workplace safety and health measures, the committee aims to enhance the company's safety management standards and achieve its safety objectives. CyberPower holds one regular Occupational Safety and Health Committee meeting each quarter, where topics such as safety and health reports, discussion items, and interim motions are reviewed and discussed.

Occupational Safety and Health Committee Structure



Occupational Safety and Health Committee Duties

Occupational Safety and Health Committee Duties	Improvements of the Occupational Injuries	Rectification of Deficiencies Identified during the Preliminary Fire Inspection	Occupational Accident Investigation	Occupational Accidents and Injuries Reported
Improvements of the Occupational Injuries	Carbon Dioxide Detection	Patrol at the Tainan Factory	AED Maintenance	Taipei Department of Health Certified Nursing Room

Occupational Safety and Health Committee Discussion Topics

First Quarter	Second Quarter	Third Quarter	Fourth Quarter
• Waste disposal and component recycling in compliance with office 5S management • Results of the blood donation activity for the first half of the year • Evaluation of the placement of tourniquets, triangular bandages, masks, gloves, and insulated gloves on each floor • Installation of AEDs on the 9th and 10th floors • Evaluation of AED deployment • Occupational safety and health education and training for the first half of the year	• Carbon dioxide testing report for the first half of the year • Occupational safety and health education and training for the first half of the year — fire prevention, earthquake safety courses, and smoke simulation experience • Installation of an additional AED on the 10th floor • Improvement of fire safety deficiencies • Power management in office areas • Hazard identification and restrictions for the constant temperature and humidity control area in the B1 floor • Promotion of health activities — aerobic dance, stress-relief crafts, and weight management	• Procurement of protective equipment • Noise level testing of machinery and procurement of earmuffs and earplugs • Tainan factory inspection at the end of June — verification of fire extinguisher validity and placement of surrounding items • Noise level testing in the Tainan testing and assembly area • Carbon dioxide detection in the Tainan office • Implementation of the unlawful infringement prevention plan • Progress of health promotion activities	• Carbon dioxide testing for the second half of the year • Occupational safety and health education and training for the second half of the year — prevention of electric shock hazards • Reinforcement of rodent-proof nets for laboratory tables • Training on the use of new official vehicles in Taipei • Application of anti-slip coating on driveways

Occupational Safety and Health Training

CyberPower regularly conducts occupational safety training for new hires and contractors, along with refresher courses for current staff, to ensure that employees acquire essential workplace safety knowledge and work in a safe and healthy environment. To prevent the recurrence of similar incidents, the company also conducts regular accident education training and uses incident investigation and analysis methods to help employees understand the root causes of accidents, thereby reducing workplace incidents and enhancing employee safety and health.

The company conducts at least one occupational safety education training every half year, covering topics such as administrative management guidelines, workplace gender equality, and prevention and management of unlawful infringement. Additionally, a fire drill is conducted once every half year, with the first drill of 2024 completed on May 21 and the second on October 29.

Occupational Safety and Health Training for Personnel

Worker Category	Training Category	Training Topic	Training Hours	Number of Participants	Total Training Hours
New Employees	General Training	Occupational Safety and Health Education Training	5	5	5
Current Employees	General Training	Fire and Earthquake Safety Awareness Course and Smoke Simulation Experience	1.5	28	42
		Prevention and Handling of Unlawful Infringement in the Workplace	1.5	219	328.5
		Fire Drill for the First Half of 2024	0.5	262	131
		Fire Drill for the Second Half of 2024	0.5	268	134
Service Contractors	General Training	Fire Drill Course	0.5	2	1
Total			9.5	784	641.5

Note: The fire drill for current employees includes all staff (supervisors, departmental personnel, and new employees), with no separate fire drill arranged for new employees.

Building a Safer Workplace Through Prevention and Preparedness

CyberPower's Taipei headquarters regularly conducts fire drills simulating building fire scenarios. Through coordinated actions such as emergency broadcasts, evacuation guidance, and staff collaboration, the company strengthens its emergency response procedures. The drills are jointly conducted by the building management center, employees from various departments, and building tenants, allowing participants to practice evacuation routes and the operation of fire doors.

During the exercise, employees follow instructions to evacuate via the emergency stairways to the ground-floor assembly point, where attendance is taken to ensure no one is left behind. Afterward, fire safety specialists provide hands-on training on the use of fire extinguishers and fire hoses to enhance practical response capabilities.

Through these drills, CyberPower demonstrates its commitment to workplace safety and continues to strengthen its disaster preparedness and emergency response capabilities.



Occupational Hazard Risk Control and Management

CyberPower conducts hazard identification and analysis, as well as risk classification based on occupational accident records. Common occupational hazards include highly repetitive movements, poor posture, or maintaining fixed positions for extended periods. To address these risks, the company provides targeted safety procedures, accident prevention training, and semi-annual emergency fire drills for operators. Workplace safety measures and work systems are continuously improved, such as providing protective equipment, establishing ergonomic workstations, and reducing work hours.

Employees who believe their work environment may pose risks of injury or illness are encouraged to report their concerns to the management unit. The relevant departments will then assess the environment and implement appropriate corrective actions.

Occupational Safety and Health Management: Hazard Identification, Analysis, and Improvement Measures

Hazard Identification	Hazard Analysis	Risk Level	Improvement Measures Mechanical Hazards
Mechanical Hazards	• Unsafe environments or facilities: Machinery lacking safety protection mechanisms • Clipping and rolling	High	Wear protective gear, improve ventilation, conduct regular health check-ups, and reduce work hours
Physical Hazards	• Hazards associated with high-temperature operations, noise, and repetitive tasks	Medium	Provide insulation equipment, earplugs, and schedule regular breaks
Ergonomic Hazards	• Musculoskeletal injuries caused by repetitive work postures	Low	Set up ergonomic workstations, and provide rest periods

Occupational Accident Response and Management

Accident Reporting and Handling Process

No.	Procedure	Execution Guidelines
1	Accident Occurrence	--
2	Accident Emergency Response	• On-site control or prevention of further incidents • Assist the injured in obtaining necessary first aid or medical treatment • In the event of a significant occupational disaster, except for necessary first aid and rescue, the scene may not be moved or destroyed without the permission of judicial authorities or inspection agencies; for general accidents or false alarms, the scene should also be preserved intact to facilitate the progress of the accident investigation.
3	Reporting and Other Related Matters	• In the event of a significant occupational disaster, the division manager of the affected department should immediately report to the President, notify occupational safety and health personnel, and submit the "Occupational Accident Reporting Form" to the Administration Department. If needed, phone or verbal notification may be made beforehand. • The Administration Department should report to the inspection agency within 8 hours and then update the president on the follow-up status. • For other occupational accidents, the division manager of the affected department should submit the "Occupational Accident Reporting Form"and report to the Administration Department within 3 days. If needed, phone or verbal notification may be made beforehand. • The Administration Department should compile monthly statistics on occupational accidents and report the data online.
4	Accident Investigation	• For significant occupational disasters, the division manager of the affected department should convene relevant personnel for investigation and hold an investigation meeting within 2 working days of the accident. • The division manager of the affected department should submit an "Occupational Accident Investigation Report" based on the investigation results within 2 weeks. • If the investigation cannot be completed by the deadline, an initial report on current status should be submitted first, followed by a complete report once the investigation is concluded.
5	Approval of Accident Investigation Report	• Once the investigation report is reviewed by the division manager of the affected department, it should be submitted to the Administration Department. • Once the Administration Department reviews and evaluates the report, it should be forwarded to the president for approval. Subsequently, relevant materials should be distributed to the affected department, responsible parties of corrective measures, and related personnel. • The Administration Department and each unit must promote the findings from the accident investigation, or incorporate them into safety and health training materials.
6	Implementation and Follow-up of Corrective Measures	• Each unit and personnel should strictly implement the corrective measures as planned. • The Administration Department is responsible for tracking the implementation of corrective measures and recording the results.
7	Case Closure and Accident Investigation Report Archiving	• The accident investigation report can only be closed and archived after all corrective measures have been completed. • The accident investigation report will be retained by the Administration Department for 10 years.

Accident Investigation Process

Accident Occurrence	In the event of a significant occupational disaster, immediate notification must be made to occupational safety personnel and the immediate supervisor. The contractors must report the incident to the supervising unit by phone within 30 minutes, and in accordance with relevant regulations, inform the fire department and medical unit to request assistance. For significant occupational disasters, notification must be made to the local labor inspection agency within 8 hours. We also adhere to Article 18 of the "Occupational Safety and Health Act," which protects workers' right to withdraw from unsafe situations. This right is reinforced during new employee training to ensure that personal safety and health are prioritized in all circumstances.
Incident Cause Investigation	The Administration Department shall, after a significant occupational disaster occurs, establish an "Occupational Accident Investigation Task Force," led by unit supervisors or designated personnel. The task force will promptly conduct a site inspection and verification with department heads, submit the "Occupational Accident Investigation Report" to the president, and convene a review meeting within one week to discuss the report. The occupational safety and health manager will act as the convener, inviting department heads, labor representatives, and others to attend the meeting, and Administration Department will explain the circumstances and handling of the significant occupational disaster.
Incident Review and Improvement Measures	Based on the improvement measures outlined in the incident investigation analysis report provided by the "Occupational Accident Investigation Task Force," each unit must monitor and track the implementation until improvements are completed. A comprehensive review of the improvements will be conducted to prevent the recurrence of similar incidents. For significant occupational disaster sites, photographic evidence should be collected and included in the investigation report, which will be submitted to the Administration Department as educational material to prevent similar incidents in the future.

Occupational Injury Statistics and Analysis

In 2024, CyberPower primarily recorded minor occupational injuries, with no incidents resulting in injuries classified as moderate or severe. During the year, the types of incidents included 11 cases of cuts or scrapes, 1 case of crush injury, 4 cases of falls, and 1 case of burn injury.
In response to the higher number of fall incidents occurring on the parking ramp, the Occupational Safety and Health Committee conducted an in-depth review of the causes and circumstances of these events. As a result, the committee resolved to strengthen communication on motorcycle tire tread checks and driving safety reminders, as well as to update the anti-slip coating on the parking ramp to reduce the likelihood of accidents and enhance employee safety.
Over the past three years, the company has not recorded any incidents resulting in high-consequence work-related injuries or disabilities.

Work-related Injury Statistics for Workers in the Past 3 Years

Year	2022		2023		2024	
Worker Category	Employees	Non-employees	Employees	Non-employees	Employees	Non-employees
Total Work Hours	705,326	2,000	722,731	1,984	762,000	2,000
Number of Fatalities	0	0	0	0	0	0
Fatality Rate	0	0	0	0	0	0
Number of High-consequence Work-related Injuries	0	0	0	0	0	0
High-consequence Work-related Injury Rate	0	0	0	0	0	0
Number of Recordable Work-related Injuries	0	0	0	0	0	0
Total Recordable Injury Frequency Rate	0	0	0	0	0	0

Note 1: Work-related injury refers to accidental injuries that occur to workers while performing their duties or within the workplace. This benchmark does not include commuting accidents (However, incidents that occur during transportation arranged by the organization, such as company vehicles or contracted transportation, are included).
Note 2: Total Work Hours: Calculated by adding the total annual work hours of all workers. For employees, the calculation includes both actual work hours and overtime; for non-employees (contractors and temporary staff), the annual data is estimated using the annual calendar's working days × 8 hours.
Note 3: High-consequence Work-related Injury: This refers to injuries resulting in disability or inability to return to pre-injury health status within 6 months (excluding fatalities).
Note 4: Fatality Rate = Number of fatalities due to work-related injuries ÷ Total work hours × 200,000.
Note 5: High-consequence Work-related Injury Rate = Number of high-consequence work-related injuries ÷ Total work hours × 200,000.
Note 6: Total Recordable Injury Frequency Rate (TRIFR) = Number of recordable work-related injuries (including high-consequence work-related injuries, fatalities, and other recordable injuries) × 200,000 ÷ Total work hours.
Note 7: Rate calculations for points 4-6: Calculate to two decimal places without rounding.
Note 8: The rate per 200,000 work hours indicates the number of work-related injuries per 100 full-time workers annually, based on the assumption that full-time workers work 2,000 hours per year (suitable for organizations with fewer than 500 employees).

Disabling Injury Frequency and Severity Rate Statistics for Workers in the Past 3 Years

Year	Worker Category	Lost Workday Due to Disabling Injuries	Disabling Injury Frequency Rate (FR)	Disabling Injury Severity Rate (SR)	Frequency-severity Indicator (FSI)
2022	Employees	0	0	0	0
	Non-employees	0	0	0	0
2023	Employees	0	0	0	0
	Non-employees	0	0	0	0
2024	Employees	0	0	0	0
	Non-employees	0	0	0	0

Note 1: Lost Workday: The number of days unable to work (rest days); the calculation benchmark includes work-related injury leave but excludes sick leave and menstrual leave.
Note 2: Disabling Injury Frequency Rate (FR) = Number of disabling injuries ÷ Total work hours × 200,000 (calculate to two decimal places without rounding).
Note 3: Disabling Severity Rate (SR) = Lost workday due to disabling injuries ÷ Total work hours × 200,000 (calculate to the nearest whole number without rounding).
Note 4: Frequency-Severity Indicator (FSI) = √[(FR × SR) ÷ 1,000].
Note 5: The rate per 200,000 work hours indicates the number of work-related injuries per 100 full-time workers annually, based on the assumption that full-time workers work 2,000 hours per year (suitable for organizations with fewer than 500 employees).

Workplace Health Services

Work-related Ill Health Prevention Management

To protect employees' physical and mental well-being, CyberPower conducts regular health check-ups for all employees and implements tiered health management in compliance with legal requirements. The results of the health examinations are reviewed by occupational health nurses and physicians, who provide follow-up monitoring and health guidance. When necessary, on-site assessments are conducted for suspected work-related illnesses. Employees classified as level 3 or above receive follow-up assessments in the following year, while level 4 employees are provided with consultations and guidance from professional physicians at the health center. As of the end of 2024, the company has no operations posing specific health risks, and no occupational diseases have occurred in the past three years.

Work-related Ill Health Statistics for Workers in the Past 3 Years

Year	2022		2023		2024	
Worker Category	Employees	Non-employees	Employees	Non-employees	Employees	Non-employees
Total Work Hours	705,326	2,000	722,731	1,984	762,000	2,000
Number of Cases of Recordable Work-related Ill Health	0	0	0	0	0	0
Number of Fatalities Due to Work-related Ill Health	0	0	0	0	0	0
Fatality Rate Due to Work-related Ill Health	0	0	0	0	0	0
Main Types of Work-related Ill Health	None					

Note 1: Total Work Hours: Calculated by adding the total annual work hours of all workers; for employees, the calculation includes both actual working hours and overtime; for non-employees (contractors and temporary staff), the annual data is estimated using 8 hours per day × (number of personnel entering the facility each month × number of working days per month).
Note 2: Fatality Rate Due to Work-related Ill Health: Number of fatalities due to work-related ill health × 200,000 ÷ Total work hours (calculate to two decimal places without rounding). It represents the rate of fatalities due to work-related ill health per 100 or 500 full-time workers within a year, based on the assumption that full-time workers work 2,000 hours annually.

Health Promotion and Care

CyberPower aims to help employees achieve a balance between work, health, and life. In 2017, the company introduced the spirit of Employee Assistance Programs (EAPs) and established an infirmary, along with the appointment of a full-time nurse. The nurse is responsible for integrating internal and external professional service resources to assist employees in addressing issues related to health, family, legal, and psychological matters that may affect work performance. The key aspects of employee assistance include:

Item	Details
Service System	Infirmary • Professional Staff: Full-time occupational health nurse and contracted occupational health physician • Equipment: Thermometer, blood pressure monitor, pulse oximeter, scale, medical bed, and wheelchair • Medical Supplies: Wound care and cleaning supplies • Emergency Treatment for Injuries and Illnesses: Provides emergency wound care and health consultations. • Medical Bed Availability: For employees experiencing sudden discomfort during work, requiring bed rest and regular monitoring of vital signs • Equipment Loan: Employees can register to borrow thermometers, blood pressure monitors, pulse oximeters, wheelchairs, and hot water bottles based on their needs

Item	Details
Professional Assistance	Occupational Health Nurse • Plan and implement measures to protect and promote employee physical and mental health • Work-related injuries and illnesses prevention, health consultations, and emergency care • Assist the occupational health physician with employee work selection, assignments, and return-to-work processes • Organize employee health check-ups • Facilitate employee health consultations and referrals for psychological counseling needs • Manage medical supplies, infirmary operations and nursing room • Prevention of infectious diseases • Conduct occupational health education, research, analysis, reporting, management, and record-keeping Occupational Health Physician • Assist in the drafting, planning, promotion, and execution of occupational health service programs • Identify and assess employee health hazard factors and risks • Based on the results of risk assessments, provide written notifications regarding risks, health education, preventive health guidance, job adjustments, reassignments, and other recommendations derived from the assessments • Assessment of occupational diseases and work-related illnesses, health check-ups for hazardous health operations, tiered health management assessments, and assistance with employee work selection, assignments, and return-to-work processes • Provide medical services and referrals for work-related injuries and illnesses, as well as those not related to work • Assist in reviewing the execution and effectiveness of occupational health services and related health hazard prevention initiatives • Regularly report on the status and performance of occupational health services and providing recommendations for improvement
Professional Assistance	• Health Consultations: Company's full-time nurse via extension and email • Workplace Violence and Sexual Harassment Prevention: - Complaint Hotline: +886-2-8792-9510 (Dedicated personnel of Human Resource Department) - Complaint Email: tw.hr@cyberpower.com
Health Hazard Prevention Surveys	• Abnormal Workload: Checklist for abnormal workloads • Ergonomic Hazards: Musculoskeletal symptom survey • Maternal Labor Protection: Self-assessment form for worker's health during pregnancy and up to one year postpartum
Information Sharing	• Health News: Regularly promote health knowledge through CyberPower's Welfare Committee e-newsletter and share information about health activities on the company intranet as needed. Examples include Health Promotion Administration's National Walking Competition, Taipei City Department of Health's free screenings for five types of cancers and adult health checks, and Taipei City Department of Health's prize incentive for booster vaccinations, etc. • Epidemic Disease Awareness: Based on the latest epidemic announcements from the Taiwan Centers for Disease Control, health education information is periodically posted in the Environmental, Health, and Safety section of the company's intranet. The company also promptly communicates epidemic prevention and control measures to strengthen employees' awareness of disease prevention
Health Promotion Activities	Health promotion activities and seminars are organized annually based on evaluations of employee health check-up data. • 2024 Health Promotion Activities - Step Challenge with Prizes: The activity was divided into two phases over four months, with a total of 79 participants. Among them, 63 employees achieved the monthly target for at least one month, and 49 employees met the target every month. - Weight Loss Challenge with Prizes: A total of 30 participants collectively lost 117.6 kilograms. • 2024 Health Seminars - Turkish Mosaic Lamp Workshop (Taipei) - Aerobic Dance Series (Taipei / Tainan) - 10-Minute Bedtime Stretching (Online) - Relax and Sleep Well! A Talk on Quality Sleep (Online) - Lunch with an Ophthalmologist (Taipei) In 2024, a total of 255 participants took part in health promotion activities, representing a 21% increase compared to 2023. Participation is expected to remain strong in 2025, with the company continuing to enhance employee engagement in health promotion through a diverse and effective curriculum plan.

Social Care for the Common Good

Donate Blood and Spread Love



A single bag of donated blood can save a life. By organizing regular blood donation activities, CyberPower encourages employees and community members to give back together, extending care from within the company to every corner of society.

In 2024, CyberPower organized two blood donation activities, setting up donation buses beside the Taipei headquarters plaza. Participants were granted volunteer leave, and all blood donors received a souvenir and raffle entry as a token of appreciation.

The first event, held on February 23, attracted 94 participants, including 78 successful donors, resulting in the collection of 111 bags of blood for the Taipei Blood Center (TBSF).

The second event, held on August 2, saw 109 participants, with 81 successful donors, collecting 114 bags of blood in total.

Through these ongoing charitable initiatives, CyberPower not only demonstrates its care for life but also strengthens its connection with the community—continuing to amplify positive social impact and spread love through every act of giving.



Speaking Up for the Planet Through Earth Hour

A simple act of turning off the lights represents a profound commitment to the planet's sustainability. CyberPower believes that environmental protection is not only a corporate responsibility but also an action that every employee can take in daily life.

Since 2021, CyberPower has participated annually in Earth Hour, a global lights-out initiative launched by the World Wildlife Fund for Nature (WWF). The company encourages all employees to join the campaign by reducing unnecessary electricity use and raising awareness of energy conservation and climate change issues. In 2024, CyberPower joined hands with over 591 companies and organizations across Taiwan, collectively reducing electricity consumption by 289,000 kWh and cutting approximately 143,055 kilograms of carbon dioxide emissions, equivalent to planting more than 13,000 twenty-year-old trees.

CyberPower will continue to drive green transformation through concrete actions—empowering both the company and individuals to contribute to a more sustainable, cleaner, and livable future.

Building Community Well-Being from Home: Workplace Experience for Employees' Children



"Shared prosperity" begins not only with the external community but also within the company itself. Through workplace experience activities for employees' children, CyberPower brings the younger generation closer to the industry while strengthening emotional bonds among family members.

To fulfill corporate social responsibility and foster family relationships and intergenerational dialogue, CyberPower's Human Resource Department organized the "Workplace Experience Activity for Employee' Children" during the summer of 2024. Employees' children were invited to visit the company and explore diverse professional functions. Through hands-on activities and career exploration courses, the program helped teenagers better understand industry trends and their parents' work, inspiring imagination and planning for their own futures.

The event attracted 11 high school participants and featured knowledge-sharing sessions across multiple professional departments. The curriculum combined theory and practice, covering topics such as 3D design and printing, UPS soldering experience, information security, and interview skills training. Participants expressed that the event was highly rewarding — they not only gained insight into their parents' work but also learned about industries rarely discussed in school. Some students developed strong interest in areas such as corporate operations, engineering practices, and brand marketing.

Through this cross-generational learning experience, CyberPower continues to embody a people-oriented corporate culture, extending care from employees to their families, and fostering a warm and inclusive workplace environment.



Promoting Power Education to Advance Public Energy Awareness

The widespread understanding of electricity is a vital foundation for building a sustainable society. When individuals develop proper awareness of power usage, they are empowered to make safer and more energy-efficient choices in their daily lives.

The widespread understanding of electricity is a vital foundation for building a sustainable society. When individuals develop proper awareness of power usage, they are empowered to make safer and more energy-efficient choices in their daily lives. To expand the reach of electrical knowledge, CyberPower has, as of 2024, released nine educational videos and twenty-one feature articles on topics such as fundamental electrical concepts, power management, and energy-saving technologies. Through animations and real-life examples, these materials help the public easily grasp the concepts of electrical safety and energy efficiency — bringing technical knowledge beyond factories and classrooms into everyday life.

This initiative not only strengthens electrical safety awareness among individuals and families but also fosters broader public understanding and engagement with energy issues. When knowledge is no longer confined within industries but shared and applied in daily life, it creates lasting and far-reaching positive impacts.

Appendix

GRI Sustainability Reporting Standards Index
- General Disclosures
- Material Topics Disclosures

Sustainability Accounting Standards Board Index

Task Force on Climate-related Financial Disclosures Index

Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies / Other Electronic Industries

Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies / Climate-Related Information of Listed Company

Independent Assurance Statement

GRI Sustainability Reporting Standards Index

General Disclosures

GRI Index	Disclosure	Chapter	Page
Version of the GRI Standards: GRI Universal Standards 2021			
Applicable GRI Sector Standard(s): None			
GRI 1: CyberPower published its Sustainability Report in accordance with the GRI Standards for the period from January 1 to December 31, 2024.			
GRI 2: General Disclosures 2021			
GRI 2-1	Organizational details	About CyberPower	20
GRI 2-2	Entities included in the organization's Sustainability Reporting	About This Report	05
GRI 2-3	Reporting period, frequency and contact point	About This Report	05
GRI 2-4	Restatements of information	None	--
GRI 2-5	External assurance	Main Responsible Team and Quality Management Method	05
GRI 2-6	Activities, value chain and other business relationships	Business Operations, Sustainable Value Chain	22 / 61
GRI 2-7	Employees	Workforce Distribution	81
GRI 2-8	Workers who are not employees	Workforce Distribution	81
GRI 2-9	Governance structure and composition	Board of Directors	30
GRI 2-10	Nomination and selection of the highest governance body	Board Nomination and Selection	31
GRI 2-11	Chair of the highest governance body	Conflict of Interest Avoidance	31
GRI 2-12	Role of the highest governance body in overseeing the management of impacts	Functional Committees	34
GRI 2-13	Delegation of responsibility for managing impacts	Sustainability Governance Framework	12
GRI 2-14	Role of the highest governance body in Sustainability Reporting	Sustainability Governance Framework	12
GRI 2-15	Conflicts of interest	Conflict of Interest Avoidance	31

GRI Index	Disclosure	Chapter	Page
GRI 2-16	Communication of critical concerns	Board of Directors	30
GRI 2-17	Collective knowledge of the highest governance body	Board of Directors Education and Training	32
GRI 2-18	Evaluation of the performance of the highest governance body	Board Performance Evaluation	33
GRI 2-19	Remuneration policies	Board Performance Evaluation, Unjust Enrichment Policy	33
GRI 2-20	Process to determine remuneration	Remuneration Policy for Directors and Executives	33
GRI 2-21	Annual total compensation ratio	Based on the salary confidentiality policy, the company does not disclose annual compensation-related information.	--
GRI 2-22	Statement on sustainable development strategy	Message from the Chair, Message from the President, Sustainability Roadmap	03 / 04 / 09
GRI 2-23	Policy commitments	Policy and Commitment	29
GRI 2-24	Embedding policy commitments	Policy and Commitment	29
GRI 2-25	Processes to remediate negative impacts	Complaint and Suggestion Channels	37
GRI 2-26	Mechanisms for seeking advice and raising concerns	Complaint and Suggestion Channels	37
GRI 2-27	Compliance with laws and regulations	Legal Compliance Training	37
GRI 2-28	Membership associations	Eligibility in Trade Unions / Associations	27
GRI 2-29	Approach to stakeholder engagement	About CyberPower	30
GRI 2-30	Collective bargaining agreements	None	--

Material Topics Disclosures

GRI Index	Disclosure	Chapter	Page
GRI 3: Material Topics 2021			
GRI 3-1	Process to determine material topics	Materiality Assessment Process	13
GRI 3-2	List of material topics	Materiality Assessment Results	15
Economic Performance (GRI 201: Economic Performance 2016 / GRI 207: Tax 2019)			
GRI 3-3	Management of material topics	02 About Us	19
GRI 201-1	Direct economic value generated and distributed	Economic Performance	24
GRI 207-1	Approach to tax	Approach to Tax	26
GRI 207-2	Tax governance, control, and risk management	Approach to Tax	26
GRI 207-3	Stakeholder engagement and management of concerns related to tax	Approach to Tax	26
Innovation and Research			
GRI 3-3	Management of material topics	04 Product Innovation and Service	46
GRI 3-3	Custom material topics	Innovation and Research	47
Product Quality (GRI 417: Marketing and Labeling 2016)			
GRI 3-3	Management of material topics	04 Product Innovation and Service	46
GRI 302-5	Reductions in energy requirements of products	Green Products and Services	52
GRI 417-1	Requirements for product and service information and labeling	Product Labeling	57
Ethical Management (GRI 205: Anti-corruption 2016)			
GRI 3-3	Management of material topics	03 Corporate Governance	28
GRI 205-1	Operations assessed for risks related to corruption	Anti-corruption and Anti-bribery Policies	36
GRI 205-2	Communication and training about anti-corruption policies and procedures	Anti-corruption and Anti-bribery Policies	36

GRI Index	Disclosure	Chapter	Page
Supply Chain Management (GRI 204: Procurement Practices 2016 / GRI 308: Supplier Environmental Assessment 2016 / GRI 414: Supplier Social Assessment 2016)			
GRI 3-3	Management of material topics	05 Supply Chain Management	60
GRI 204-1	Proportion of spending on local suppliers	Sustainable Procurement	62
GRI 308-1	New suppliers that were screened using environmental criteria	Sustainable Value Chain, Supplier Risk Assessment, Supplier Evaluation and Audit	61 / 63 / 64
GRI 414-1	New suppliers that were screened using social criteria	Sustainable Value Chain, Supplier Risk Assessment, Supplier Evaluation and Audit	61 / 63 / 64
GRI 414-2	Negative social impacts in the supply chain and actions taken	Sustainable Value Chain, Supplier Risk Assessment, Supplier Evaluation and Audit	61 / 63 / 64
Information Security (GRI 418: Customer Privacy 2016)			
GRI 3-3	Management of material topics	03 Corporate Governance	28
GRI 418-1	Substantiated complaints concerning breaches of customer privacy and losses of customer data	Information Security	40
Climate Change Adaptation (GRI 302: Energy 2016 / GRI 305: Emissions 2016)			
GRI 3-3	Management of material topics	06 Environmental Protection	65
GRI 302-1	Energy consumption within the organization	Energy Management	75
GRI 302-3	Energy intensity	Energy Management	75
GRI 305-1	Direct (Scope 1) GHG emissions	Greenhouse Gas (GHG) Emissions	74
GRI 305-2	Energy indirect (Scope 2) GHG emissions	Greenhouse Gas (GHG) Emissions	74
GRI 305-3	Other indirect (Scope 3) GHG emissions	Greenhouse Gas (GHG) Emissions	74
GRI 305-4	GHG emissions intensity	Greenhouse Gas (GHG) Emissions	74
GRI 305-5	Reduction of GHG emissions	Greenhouse Gas (GHG) Emissions	74

GRI Index	Disclosure	Chapter	Page
Talent Development (GRI 404: Training and Education 2016)			
GRI 3-3	Management of material topics	07 Social Inclusion	80
GRI 404-1	Average hours of training per year per employee	Diverse Training Channels	92
GRI 404-2	Programs for upgrading employee skills and transition assistance programs	Human Rights and Labor Rights Protection	87
GRI 404-3	Percentage of employees receiving regular performance and career development reviews	Performance and Career Development	93
Human Right Policy (GRI 406: Non-discrimination 2016)			
GRI 3-3	Management of material topics	07 Social Inclusion	80
GRI 202-2	Proportion of senior management hired from the local community	Diverse and Abundant Employment Opportunities	82
GRI 406-1	Incidents of discrimination and corrective actions taken	Human Rights and Labor Rights Protection	87

Sustainability Accounting Standards Board Index

Topic	Metric	Code	Chapter	Response Measure	Page
Product Security	Description of approach to identifying and addressing data security risks in products	TC-HW-230a.1	03 Corporate Governance	Product Information Security	46
Employee Diversity & Inclusion	Percentage of (1) gender and (2) diversity group representation for (a) executive management, (b) non-executive management, (c) technical employees and (d) all other employees	TC-HW-330a.1	07 Inclusion	Diverse and Abundant Employment Opportunities	82
Product Lifecycle Management	Percentage of products by revenue that contain IEC 62474 declarable substances	TC-HW-410a.1	--	CyberPower currently manages hazardous substances in accordance with the EU REACH Regulation and RoHS Directive. The company has not yet established a substance declaration system based on the IEC 62474 standard; therefore, relevant data are not available for disclosure	--
	Percentage of eligible products, by revenue, meeting the requirements for EPEAT registration or equivalent	TC-HW-410a.2	04 Product Innovation and Service	CyberPower's products are not included in the product categories applicable to EPEAT certification.	46
	Percentage of eligible products, by revenue, certified to an energy efficiency certification	TC-HW-410a.3	--	76% (calculated as the 2024 revenue from ENERGY STAR–certified products divided by the total 2024 revenue of uninterruptible power supply (UPS) products at Cyber Power Systems (USA), Inc.)	--
	Weight of end-of-life products and e-waste recovered; percentage recycled	TC-HW-410a.4	--	Given that CyberPower primarily adopts a B2B business model, the company is currently unable to directly collect comprehensive data on product recycling weights or recycling rates	--
Supply Chain Management	Percentage of Tier 1 supplier facilities audited in the RBA Validated Audit Process (VAP) or equivalent, by (a) all facilities and (b) high-risk facilities	TC-HW-430a.1	--	No data available for disclosure	--
	Tier 1 suppliers' (1) non-conformance rate with the RBA Validated Audit Process (VAP) or equivalent, and (2) associated corrective action rate for (a) priority nonconformances and (b) other nonconformances	TC-HW-430a.2	--	No data available for disclosure	--
Materials Sourcing	Description of the management of risks associated with the use of critical materials	TC-HW-440a.1	05 Supply Chain Management	Supplier Risk Assessment	63

Activity Metric	Code	Unit of Measure	Response Measure	
Number of units produced by product category	TC-HW-000.A	Number	Uninterruptible Power Supplies (UPS)	3,520,000
			Data Center Power Management Solutions	580,000
			Power Protection and Management Equipment	4,990,000
			Power Adapter and Computer Peripherals	1,280,000
			Total	10,370,000
Area of manufacturing facilities	TC-HW-000.B	Square metres (m^2)	Not disclosed due to business confidentiality	
Percentage of production from owned facilities	TC-HW-000.C	%	Not disclosed due to business confidentiality	

Task Force on Climate-related Financial Disclosures Index

Elements	Recommended Disclosures under the TCFD Framework	Chapter	Page
Governance	Describe the board's oversight of climate-related risks and opportunities	Climate Sustainability Governance	67
	Describe management's role in assessing and managing climate-related risks and opportunities	Climate Sustainability Governance	67
Strategy	Describe the climate-related risks and opportunities the organization has identified over the short, medium, and long term	Climate Risk Management, Climate Change Strategy	68 / 72
	Describe the impact of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning	Climate Risk Management, Climate Change Strategy	68 / 72
	Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario	Climate Risk Management, Climate Change Strategy	68 / 72
Risk Management	Describe the organization's processes for identifying and assessing climate-related risks	Climate Risk Management	68
	Describe the organization's processes for managing climate-related risks	Climate Risk Management	68
	Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the organization's overall risk management	Climate Risk Management	68
Metrics and Targets	Disclose the metrics used by the organization to assess climaterelated risks and opportunities in line with its strategy and risk management process	Climate Risk Management	68
	Disclose Scope 1, Scope 2, and, if appropriate, Scope 3 greenhouse gas (GHG) emissions, and the related risks	Climate Change Strategy, Climate Indicators and Targets	72 / 73
	Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets	Climate Indicators and Targets	73

Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies / Other Electronic Industries

In 2024, CyberPower disclosed sustainability disclosure indicators for the Other Electronic Industries in accordance with Article 4, Appendix 1-14, of the "Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies."

No.	Indicator	Indicator Type	Unit	Annual Disclosure	
1	Total energy consumption, percentage of purchased electricity, utilization rate (renewable energy)	Quantitative	Gigajoules (GJ), percentage (%)	Parent Company[Note 1] Purchased Electricity: 4966.2990 (GJ) Renewable Sources: 13.4525 (GJ) Percentage of Purchased Electricity: 99.73%	Other Subsidiaries[Note 2] Purchased Electricity: 34154.9403 (GJ) Renewable Sources: 1860 (GJ) Percentage of Purchased Electricity: 94.84%
2	Total water withdrawn, total water consumption	Quantitative	Thousand cubic meters (m^3)	Parent Company[Note 1] Total water withdrawn: 7881.8858 (m^3) Total water consumption[Note3]: 0 (m^3)	Other Subsidiaries[Note 2] Total water withdrawn: 88695.7262 (m^3) Total water consumption[Note3]: 0 (m^3)
3	Total hazardous waste generated and percentage recycled	Quantitative	Metric tons (t), percentage (%)	The Parent Company[Note 1] only generates general industrial waste and produces no hazardous waste in its operations.	Other Subsidiaries[Note 2] Total hazardous waste generated: 94.8135 (t) Percentage recycled: 5%
4	Types of, number of employees in and rate of occupational accidents	Quantitative	Percentage (%), quantity	Number of occupational accidents: 0 Occupational accidents rate: 0%	
5	Product Lifecycle Management Disclosure: including weights of scraps and electronic waste and percentage recycled[Note1]	Quantitative	Metric tons (t), percentage (%)	The company's electronic waste includes components scrapped during the production process (e.g., IC boards and PCB boards) and daily office equipment (e.g., discarded computers and monitors). All electronic waste is 100% recycled and processed by licensed local waste disposal contractors. Parent Company[Note 1] Total Electronic waste: 0.5250 (t)	Other Subsidiaries[Note 2] Total Electronic waste: 0.3619 (t)
6	Description of the management of risks associated with the use of critical materials	Qualitative description	Not applicable	Please refer to Chapter Supply Chain Management Policy	
7	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	Quantitative	Reporting currency	NT$0	
8	Production by product category	Quantitative	Varies by product category	Please refer to Chapter 02 About Us	

Note 1: The parent company includes CyberPower Systems, Inc. and CyberPower Systems, Inc. Tainan Plant.
Note 2: Other subsidiaries include Dongguan Cyber Energy Co., Ltd., Cyber Energy (Shenzhen), Inc., Cyber Power Technology (ShenZhen), Inc., Cyber Power (Shenzhen) Ltd, Best Top (Shenzhen), Inc., Ning Yuan Xian CyberPower, Inc., Cyber Power Systems Manufacturing, Inc., and Phisonic Technology Corporation.
Note 3: The company has no significant process water use or high water consumption demands. There is no substantial evaporation, adsorption, or other water loss during water usage. Therefore, water withdrawal and water discharge are estimated to be approximately equal, and water consumption can be considered zero.

Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies / Climate-Related Information of Listed Company

In 2024, CyberPower disclosed sustainability disclosure indicators for the Climate-Related Information of Listed Company in accordance with Article 4-1, Appendix 2, of the "Rules Governing the Preparation and Filing of Sustainability Reports by TWSE Listed Companies."

No.	Item	Implementation
1	Describe the board of directors' and management's oversight and governance of climate-related risks and opportunities	Climate-related Risks and Opportunities
2	Describe how the identified climate risks and opportunities affect the business, strategy, and finances of the business (short, medium, and long term)	
3	Describe the financial impact of extreme weather events and transformative actions	
4	Describe how climate risk identification, assessment, and management processes are integrated into the overall risk management system	
5	If scenario analysis is used to assess resilience to climate change risks, the scenarios, parameters, assumptions, analysis factors and major financial impacts used should be described	
6	If there is a transition plan for managing climate-related risks, describe the content of the plan, and the indicators and targets used to identify and manage physical risks and transition risks	
7	If internal carbon pricing is used as a planning tool, the basis for setting the price should be stated	
8.	If climate-related targets have been set, the activities covered, the scope of greenhouse gas emissions, the planning horizon, and the progress achieved each year should be specified. If carbon credits or renewable energy certificates (RECs) are used to achieve relevant targets, the source and quantity of carbon credits or RECs to be offset should be specified	
9	Greenhouse gas inventory and assurance status (separately fill out in point 1-1 below)	As shown in the table below.

Greenhouse Gas Inventory and Assurance Status in 2024

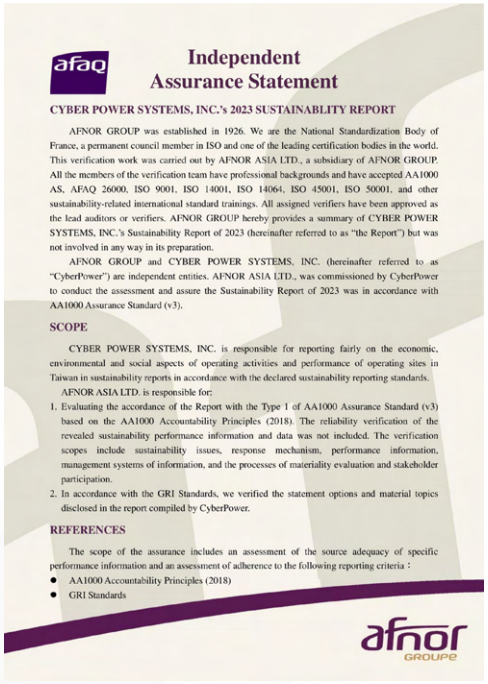
CyberPower is verified as a listed company with paid-in capital of less than NT$5 billion.	In accordance with the "Sustainable Development Roadmap for TWSE/TPEx Listed Companies," individual company data will be disclosed starting in 2026, and consolidated company data, including parent and subsidiary entities, will be disclosed starting in 2027. Assurance for individual company data will be completed by 2028, and assurance for consolidated company data will be completed by 2029.

Status of Greenhouse Gas Inventory and Assurance

		Total Emissions (tCO2e)	Intensity (tCO2e / NT$ million)	Institution	Status
Parent Company[Note 1]	Scope 1	143.1198	0.1288	AFNOR Asia	Cyber Power Systems, Inc. has gone through assurance engagement in 2024
	Scope 2	653.8960			
	Scope 3 (May be disclosed voluntarily)	176.8813			
Other Subsidiaries[Note 2]	Scope 1	329.4345	2.4881	AFNOR Asia	Cyber Power Systems, Inc. has gone through assurance engagement in 2024
	Scope 2	4,695.6190			
	Scope 3 (May be disclosed voluntarily)	2,620.3719			

Note 1: The parent company includes CyberPower Systems, Inc. and CyberPower Systems, Inc. Tainan Plant.
Note 2: Other subsidiaries include Dongguan Cyber Energy Co., Ltd., Cyber Energy (Shenzhen), Inc., Cyber Power Technology (ShenZhen), Inc., Cyber Power (Shenzhen) Ltd, Best Top (Shenzhen), Inc., Ning Yuan Xian CyberPower, Inc., Cyber Power Systems Manufacturing, Inc., and Phisonic Technology Corporation.

Independent Assurance Statement



Independent Assurance Statement

CYBER POWER SYSTEMS, INC.'s 2023 SUSTAINABLITY REPORT

AFNOR GROUP was established in 1926. We are the National Standardization Body of France, a permanent council member in ISO and one of the leading certification bodies in the world. This verification work was carried out by AFNOR ASIA LTD., a subsidiary of AFNOR GROUP. All the members of the verification team have professional backgrounds and have accepted AA1000 AS, AFAQ 26000, ISO 9001, ISO 14001, ISO 14064, ISO 45001, ISO 50001, and other sustainability-related international standard trainings. All assigned verifiers have been approved as the lead auditors or verifiers. AFNOR GROUP hereby provides a summary of CYBER POWER SYSTEMS, INC.'s Sustainability Report of 2023 (hereinafter referred to as "the Report") but was not involved in any way in its preparation.

AFNOR GROUP and CYBER POWER SYSTEMS, INC. (hereinafter referred to as "CyberPower") are independent entities. AFNOR ASIA LTD., was commissioned by CyberPower to conduct the assessment and assure the Sustainability Report of 2023 was in accordance with AA1000 Assurance Standard (v3).

SCOPE

CYBER POWER SYSTEMS, INC. is responsible for reporting fairly on the economic, environmental and social aspects of operating activities and performance of operating sites in Taiwan in sustainability reports in accordance with the declared sustainability reporting standards.

AFNOR ASIA LTD. is responsible for:

1. Evaluating the accordance of the Report with the Type 1 of AA1000 Assurance Standard (v3) based on the AA1000 Accountability Principles (2018). The reliability verification of the revealed sustainability performance information and data was not included. The verification scopes include sustainability issues, response mechanism, performance information, management systems of information, and the processes of materiality evaluation and stakeholder participation.
2. In accordance with the GRI Standards, we verified the statement options and material topics disclosed in the report compiled by CyberPower.

REFERENCES

The scope of the assurance includes an assessment of the source adequacy of specific performance information and an assessment of adherence to the following reporting criteria：

- AA1000 Accountability Principles (2018)
- GRI Standards



METHODOLOGY

- The inclusivity, materiality, responsiveness, and impact in the Report were assessed according to the principles of management process against AA1000 Assurance Standard (v3).
- The report is reported in accordance with the GRI Standards, and the content of the report is reviewed for general disclosures and specific topic disclosures that comply with the GRI Standards.
- The mechanism of communication and response to the interest of stakeholders was verified through discussion and interview with the management team, however, the assessment team did not make any direct contact with external stakeholders.
- The qualitative and quantitative information produced, collected, and disclosed by the Report was reviewed through a validated sampling plan.
- The documents, materials and information related to the report were examined and reviewed by interviewing the responsible persons of each group of CyberPower.
- Interviews with members of the organization related to sustainable development management and report writing, including representatives of all levels and departments.
- All documents, data and information related to the preparation of this report were checked by the verification team through interviews with relevant personnel.
- Check the sufficiency and completeness of supporting materials and evidence for the content of the report.

CONCLUSION

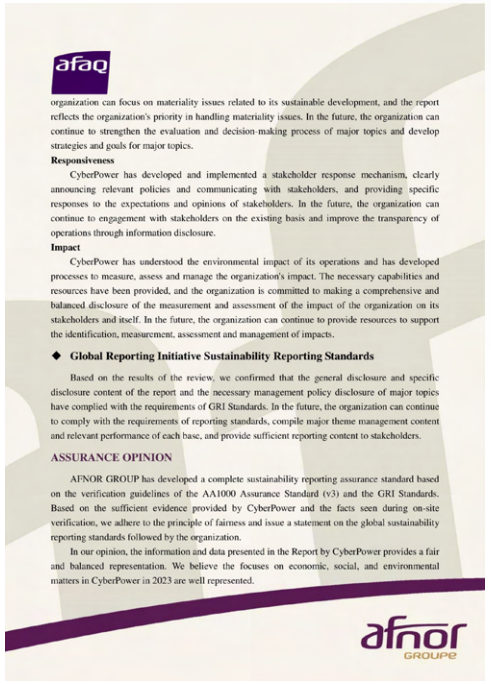
◆ **AA1000 Accountability Principles**

Inclusivity

CyberPower has identified stakeholders and maintained communication channels for stakeholders to participate in different important topics to understand the important information that stakeholders are concerned about. The report has fairly reported and disclosed relevant information on the economy, environment and society, and can provide effective information to its stakeholders. In the future, the organization can continue its stakeholder identification and communication process to respond to changes in the internal and external environments.

Materiality

CyberPower has established effective processes to identify issues of significance to stakeholders and operational performance. The decision-making mechanism implemented by the



organization can focus on materiality issues related to its sustainable development, and the report reflects the organization's priority in handling materiality issues. In the future, the organization can continue to strengthen the evaluation and decision-making process of major topics and develop strategies and goals for major topics.

Responsiveness

CyberPower has developed and implemented a stakeholder response mechanism, clearly announcing relevant policies and communicating with stakeholders, and providing specific responses to the expectations and opinions of stakeholders. In the future, the organization can continue to engagement with stakeholders on the existing basis and improve the transparency of operations through information disclosure.

Impact

CyberPower has understood the environmental impact of its operations and has developed processes to measure, assess and manage the organization's impact. The necessary capabilities and resources have been provided, and the organization is committed to making a comprehensive and balanced disclosure of the measurement and assessment of the impact of the organization on its stakeholders and itself. In the future, the organization can continue to provide resources to support the identification, measurement, assessment and management of impacts.

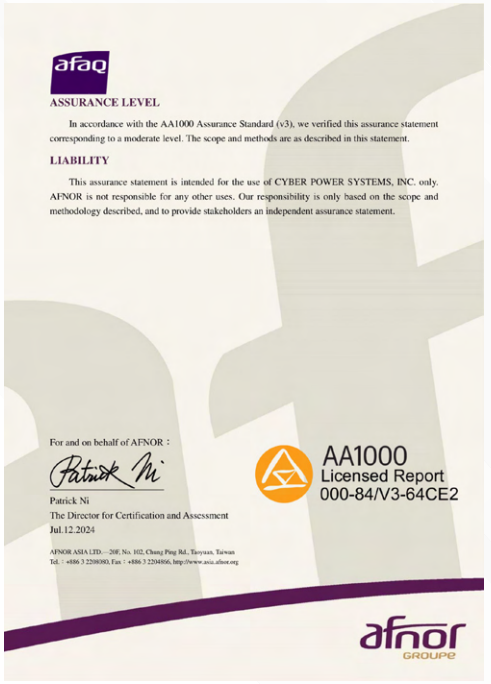
◆ **Global Reporting Initiative Sustainability Reporting Standards**

Based on the results of the review, we confirmed that the general disclosure and specific disclosure content of the report and the necessary management policy disclosure of major topics have complied with the requirements of GRI Standards. In the future, the organization can continue to comply with the requirements of reporting standards, compile major theme management content and relevant performance of each base, and provide sufficient reporting content to stakeholders.

ASSURANCE OPINION

AFNOR GROUP has developed a complete sustainability reporting assurance standard based on the verification guidelines of the AA1000 Assurance Standard (v3) and the GRI Standards. Based on the sufficient evidence provided by CyberPower and the facts seen during on-site verification, we adhere to the principle of fairness and issue a statement on the global sustainability reporting standards followed by the organization.

In our opinion, the information and data presented in the Report by CyberPower provides a fair and balanced representation. We believe the focuses on economic, social, and environmental matters in CyberPower in 2023 are well represented.



ASSURANCE LEVEL

In accordance with the AA1000 Assurance Standard (v3), we verified this assurance statement corresponding to a moderate level. The scope and methods are as described in this statement.

LIABILITY

This assurance statement is intended for the use of CYBER POWER SYSTEMS, INC. only. AFNOR is not responsible for any other uses. Our responsibility is only based on the scope and methodology described, and to provide stakeholders an independent assurance statement.

For and on behalf of AFNOR：

Patrick Ni

Patrick Ni
The Director for Certification and Assessment
Jul.12.2024

AFNOR ASIA LTD.—20F, No. 102, Chung Ping Rd., Taoyuan, Taiwan
Tel. : +886 3 2208080, Fax : +886 3 2204866, http://www.asia.afnor.org

AA1000
Licensed Report
000-84/V3-64CE2