NETGEAR

2023

Environmental Social Governance Report

ESG Report Overview

This report contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. The words "anticipate," "expect," "believe," "will," "may," "should," "estimate," "project," "outlook," "forecast" or other similar words are used to identify such forward-looking statements. However, the absence of these words does not mean that the statements are not forward-looking. The forward-looking statements represent NETGEAR, Inc.'s expectations or beliefs concerning future events based on information available at the time such statements were made. Goals and targets described in this report are aspirational and not guarantees or promises that the goals or targets will be met. Historical, current, and forward-looking ESG-related statements may be based on standards for measuring progress that are still developing, internal controls and processes that continue to evolve, and assumptions that are subject to change in the future. Numbers and percentages in this report include estimates or approximations and may be based on assumptions or incomplete data. We believe that the estimates employed are appropriate and reasonable; however, due to inherent uncertainties in making estimates and assumptions, actual results could differ from the original estimates.

The inclusion of information contained in this document should not be construed as a characterization regarding the materiality or financial impact of that information.

Website references and hyperlinks throughout this document are provided for convenience only, and the content on the referenced websites is not incorporated into this report. We assume no liability for any third-party content contained on the referenced websites.

Contents

Introduction

ESG Message from the CEO

At NETGEAR, we are pioneers. We've been innovating and leading the industry in the creation of advanced networking technologies for homes and businesses around the world for almost three decades. That's longer than any of our competitors and, in that time, we've pushed the boundaries of what can be experienced or accomplished in our increasingly wireless and connected world.

During this time, we also proved that our core values are critical to our success, helping us not only to exceed technological expectations, but also to solidify our place among the most trusted brands in our industry.
Our commitment to these ideals will continue to propel us as we embrace new technologies and economic realities while striving towards our mission: to use innovation to power connection. We empower our customers to collaborate and connect to a world of information through our high-performance networking solutions.

In 2021, we conducted our first materiality assessment to identify priority ESG topics that are the most material to our business and our stakeholders. We found that those priorities closely aligned with our most firmly held beliefs as well as our strengths. They include protecting our customers' data and privacy, maintaining an environmentally and socially responsible supply chain and holding professional integrity and inclusion at the core of all business operations.
As we progress on our ESG journey, we will focus our efforts on these topics to enhance sustainability throughout our organization.

Since the publication of our inaugural ESG report, we've made significant strides in each of these areas and are proud to be in alignment with Sustainability Accounting Standards Board (SASB) standards while working towards meeting the requirements of the Task Force on Climate-Related Financial Disclosures (TCFD). By 2025, we are committed to achieving net-zero greenhouse gas emissions across our scope one and two emissions sources. We recognize our responsibility to contribute to the environmental health of our world and I am confident that NETGEAR as a team and our long-standing partners can rise to this challenge.

ESG Message from the CEO Continued

We will rise to the occasion on other fronts as well, as our work continues to evolve with the shifting needs of our customers. The introduction of new wireless standards such as WiFi 7, the availability of exponentially increasing internet speeds to homes and businesses and the endless proliferation of wireless devices that connect and power our smart homes spur us to deliver ever more powerful solutions. Also, the cultural shift from recorded or broadcast content to live streaming which encompasses not just entertainment and sports, but also live events (from interpersonal to international) that hinge on speed, and, more importantly, near-zero latency, drives the need for our highly differentiated, technologically superior and secure devices to provide the right mix of power, performance and peace of mind.

And to conceive, create and deliver the highest quality audio visual content, professionals are transitioning from traditional infrastructures to AV-over-IP, moving vast amounts of data quickly, easily and seamlessly for unparalleled experiences. These implementations require best-in-class connected solutions designed specifically for this growing market. NETGEAR is at the forefront of these trends, on both the professional and consumer sides of the equation, and will continue to lead the industry with the most advanced products and services.

Global events, uncertain economies and the ever-changing cyberthreat landscape also have social and economic implications that demand our action. We believe that to meet these challenges and make a positive impact on the world around us, we must rely on the beliefs and practices that have contributed to our longevity and success.

An industry leader, NETGEAR's continued commitment to being a trusted brand that embodies our values can be seen across every aspect of our operation. As we innovate and build solutions that help our customers do more than they ever thought possible, so too will we apply that creative process to improve the way we do business with an eye to preserving our environment, protecting our customers and empowering our employees within a culture of trust and integrity.

Powering a future that connects us all,

Patrick Lo
NETGEAR CEO and Co-founder

Being a Trusted Brand

As an industry leader for over 25 years, we value our responsibility to promote a culture of integrity across our entire brand. We know that the majority of NETGEAR customers are repeat customers, so we work tirelessly to build a relationship founded in trust and listening, incorporating their voice and feedback into everything we do. Every day, both internally and externally, we work to engage in conversations that go far beyond product sales– from supply chain management, to data security, to product marketing life cycles, we prioritize responsible action in the long term.

Emphasizing the proactive nature of the company's data and cybersecurity challenges.

Respecting consumers' rights to data privacy.

Devoting internal resources to employee engagement and inclusion/diversity initiatives.

Managing environmentally and socially responsible supply chain to manage and mitigate associated risks.

Holding professional integrity at the core of all business operations.

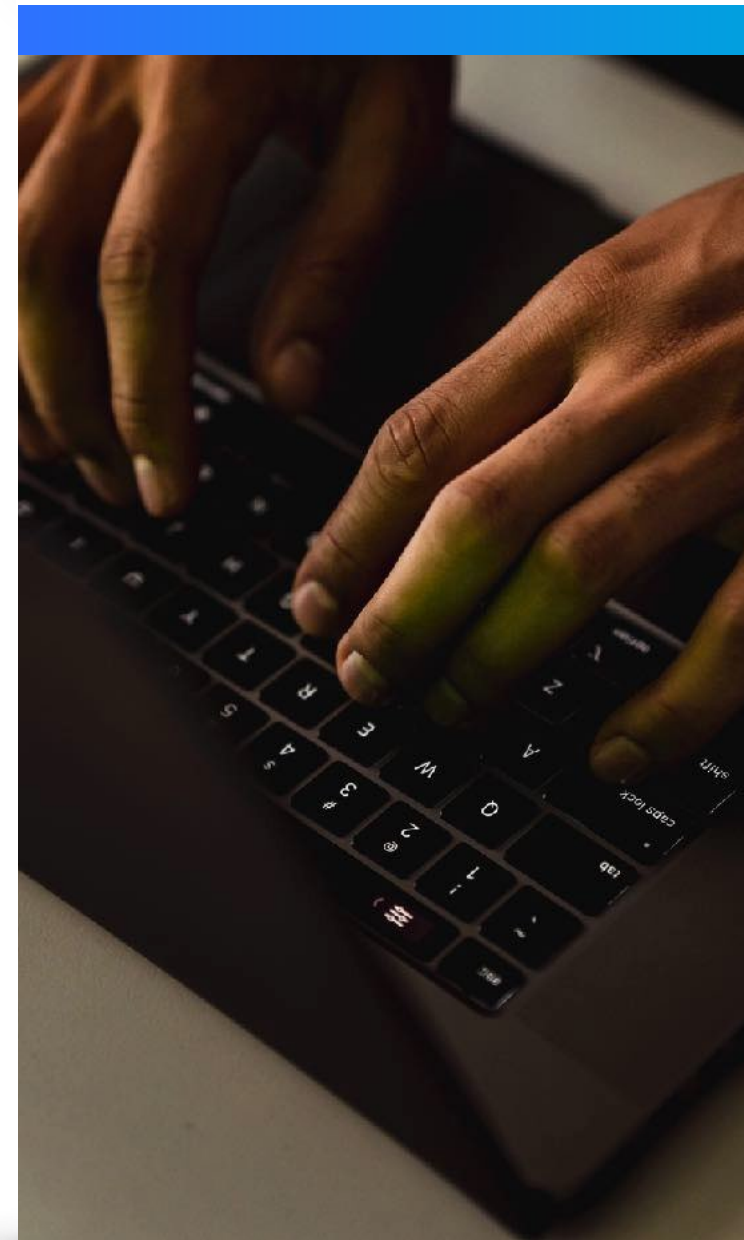Assessing our carbon footprint to mitigate our impact on the planet.

NETGEAR's Priority ESG Topics

Product Security

Data Privacy & Cybersecurity

Supply Chain Management

Employee Engagement, Diversity & Inclusion

Professional Integrity

GHG Emissions & Energy Management

Product Security

Product Security

At NETGEAR, we aim to safely connect people to the internet through innovation. Our team prioritizes building and maintaining trust with customers, providing products with enhanced security and privacy protection. Our commitment to securing your privacy includes integrating dependable security principles throughout our operations, complying with regional regulations, and ensuring that your products and data are safe.

Vulnerability Management

At NETGEAR, we take security concerns seriously and continuously monitor our products to stay ahead of emerging threats. We prefer taking a proactive approach to security, rather than waiting to react after an incident occurs. Our commitment to staying up-to-date with the latest security developments is demonstrated through our public bug bounty program and collaborations with security researchers, firms, regulators and standards bodies. Additionally, our team actively collaborates with partners to strengthen the security of our supply chain. We appreciate and value the efforts the security community is making together to create a more secure world.

To us, a Product Security Vulnerability (PSV) refers to any weakness in a product or service that could potentially be exploited, compromising its integrity, availability, or confidentiality, or that of the environments in which they are deployed. Such vulnerabilities could arise from integrations to third-party libraries and technologies we leverage, which is why we collaborate with our supply chain partners to secure products and services. At NETGEAR, we are committed to protecting our customers from malicious attacks that exploit security vulnerabilities in our products. We have established dedicated vulnerability management processes to support this commitment, which include the following:

• Centralized company-wide product vulnerability tracking and reporting

• Public bug bounty program and security community engagement

• Vulnerability classification, risk assessment, prioritization, and remediation service level agreements (SLAs)

• Product security incident and crisis response

• Hotfix and patch management

Moreover, our Product Security Team thoroughly investigates any reports of security vulnerabilities affecting NETGEAR products and services. To report a vulnerability, instructions can be found on our website at netgear.com/about/security/.

NETGEAR Product Security

Product Lifecycles

We integrate product security into our entire product development lifecycle, from product conception to production and deployment. Managing security throughout our products' lifecycle allows us to proactively detect and fix security issues, reducing the likelihood of a security breach. We thoroughly test products prior to launch based on each product's unique data and network access needs. As the final product is developed, risks and vulnerabilities are addressed through various security measures and are incorporated appropriately. We work to refactor products as they evolve, promoting relevant, informed, and advanced security features. While the lifecycle security of products may vary based on unique characteristics, an example of our approach consists of the following:

- Our security architects publish, review, and enforce secure coding and design guidelines.

- We design and test products to meet full security requirements, including penetration tests and security exception risk acceptance processes.

- Upon launch, products undergo formalized bug detection, reporting, and triage processes, which are coupled with NETGEAR's official procedure for publishing public reports of security related corrections.

- We produce security patches for 3 years after the last production date of each product.

For additional information, please visit the NETGEAR product security website: netgear.com/about/security/.

Incident Response Process

NETGEAR's cybersecurity team is committed to responding to incidents quickly and effectively to enhance security measures. With a strong incident response process in place, our team is able to swiftly address incidents and implement measures to prevent future attacks. This allows us to better safeguard our products and your data to protect against potential threats. Over the past year, we have improved our incident response time by expanding our incident response team. Looking forward, we aim to make continuous improvements to safeguard our products and your data.

Regulatory Compliance Policies

NETGEAR abides by the EU-US and the Swiss-US Privacy Shield Frameworks ("Privacy Shield"), which have been established by the U.S. Department of Commerce for the collection, use, and retention of Personal Information obtained from EU member countries, the United Kingdom, and Switzerland. As part of our commitment to these principles, NETGEAR certifies that we comply with the Privacy Shield principles related to notice, choice, accountability for onward transfer security, data integrity and purpose limitation, access, and recourse, enforcement, and liability. We limit transfers but currently leverage standard contractual clauses to transfer information if needed. We are awaiting further guidance as a Privacy Shield framework is developed and updated.

For more detailed information on our privacy policy, please visit our website at netgear.com/about/privacy-policy/.

Products & Services

We understand the importance of providing a safe browsing experience for your family and employees. That's why we're continually developing products and services to help protect your household and business online. Our products come equipped with built-in security features that enhance the security of your devices and keep your data private. NETGEAR products are designed with a variety of internal controls to mitigate cybersecurity risks, including secure password support, easy enablement and disablement of features, automatic firmware updates and patching, and more. Our goal is to offer you and your loved ones peace of mind while staying connected online.

NETGEAR®
ARMOR™

Available as an add-on, NETGEAR Armor® offers comprehensive internet security for your entire home. It goes beyond traditional anti-virus software by providing a superior protective shield for your connected devices. NETGEAR Armor® is integrated into our WiFi systems and routers and features automatic updates to safeguard your computers, mobile phones, smart TVs, door locks, security cameras, and more from potential hacking attempts. It also helps protect sensitive information, such as credit card and social security numbers, from being stolen, and helps keep your internet activity private.

NETGEAR®
SMART PARENTAL CONTROLS

Another premium NETGEAR add-on service, Smart Parental Controls helps parents manage kids' internet usage and promote good online habits. It is designed to provide a safe online experience by blocking access to inappropriate websites and allowing parents to monitor their children's online activity. Parents can easily view and manage internet usage across connected devices, including laptops, smart phones, tablets, gaming consoles and more. Smart Parental Controls also allow access and controls on kids' mobile devices when connected to LTE, so parents have complete peace of mind, whenever their kids are online.

Governance Structure

Our company takes product security very seriously and has taken several steps to improve our product security governance framework. We have adopted governance frameworks for security risk assessment and hardening product development. Additionally, we monitor our security policies to keep them aligned with industry best practices.

Supply Chain Security

As global reliance on supply chains expands, supply chain security is an increasing concern for organizations. We are closely involved with the manufacturing process of our products and incorporate product security into our supply chain where possible. To enhance the security of our suppliers, we conduct reviews and integrate automated tools including static and dynamic scanning into our product development process. We conduct an Open Web Application Security Project (OWASP) self assessment to pressure test and substantiate answers, and we leverage the security features of key partners. Going forward, we will continue to monitor the security of our supply chain partners and will work to implement processes and systems that increase security levels.

Product Security Trends

At NETGEAR, we actively work to monitor our external environment as technology expands and evolves. We regularly identify emerging product security trends to help implement appropriate measures to keep our products and services secure, reducing the risk of potential security breaches, and protecting your information.

As artificial intelligence, machine learning, and cloud security become more prevalent in product security, we are working to mitigate risks and provide secure experiences. To achieve this, NETGEAR builds access control, encryption, secure coding, and network security considerations into our products and services, and various offensive and defensive technologies at different layers.

Data Privacy & Cybersecurity

Data Privacy

NETGEAR places an emphasis on the protection and security of sensitive data. We strive to maintain openness and clarity in our practices related to the acquisition, dissemination, and utilization of personal data. Our organization only utilizes personal information for legitimate business objectives, such as optimizing our offerings, interpreting internal statistics, and preventing fraudulent behavior. We comply with data privacy regulations, including GDPR and CCPA. We acknowledge the significance of personal information and guarantee the confidentiality and security of all data in our possession.
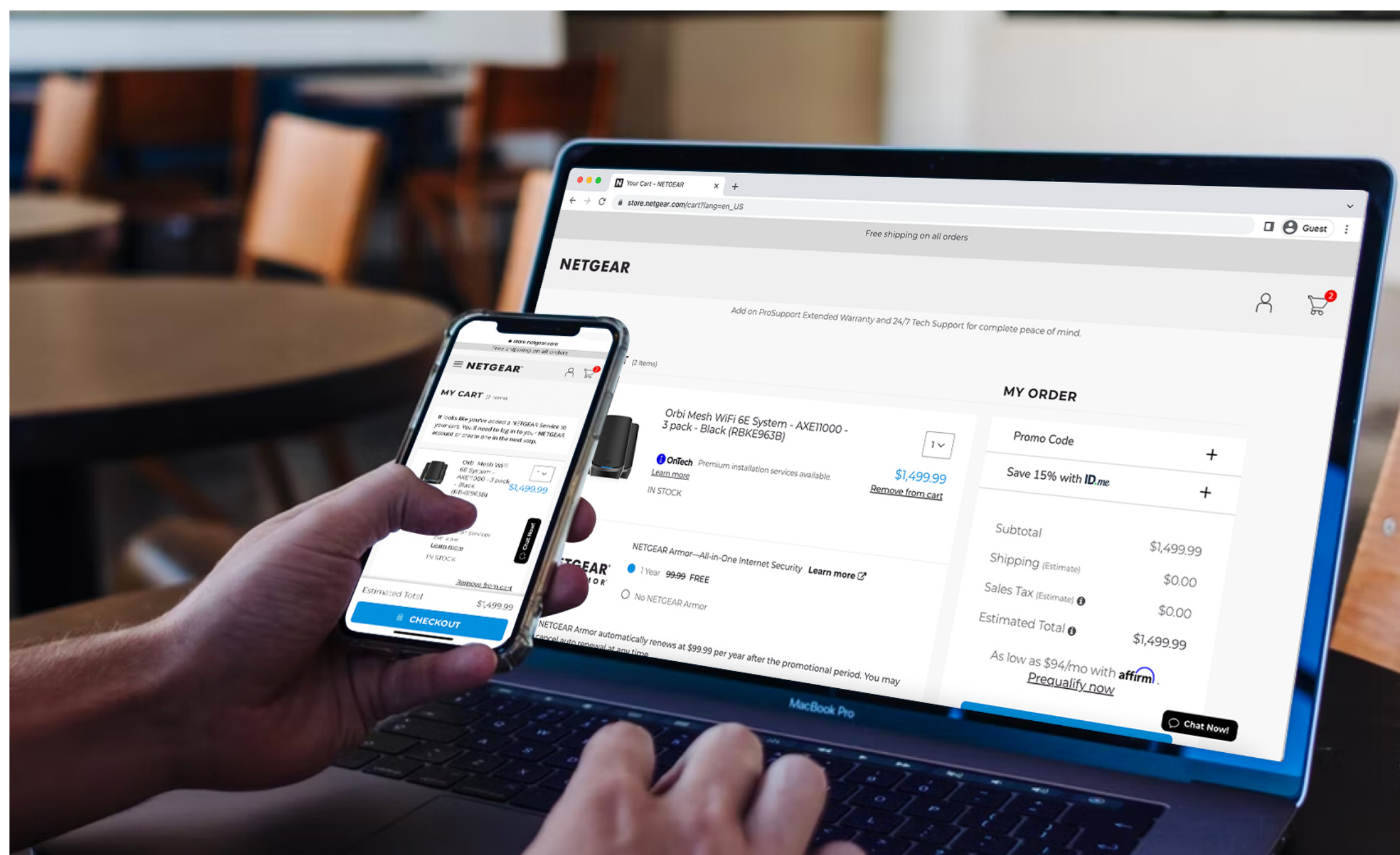
Privacy Policy

At NETGEAR Inc., we are devoted to safeguarding your privacy, which is why we don't sell your data to third parties. We uphold a meticulous privacy policy which highlights the significance of securing and preserving personal data, and we are transparent about the manner in which we collect, employ, and transfer this information. Our privacy policy is comprehensive and encompasses all domains of our enterprise, including the privacy of customer, partner, employee, and website data. It also details your rights concerning your personal information and provides information on how to reach us for inquiries and updates about our privacy practices. To review our complete privacy policy, please visit us at netgear.com/about/privacy-policy/.

Privacy Principles

NETGEAR has been providing connection solutions to people and businesses for over a quarter century. During this time, we have enabled individuals to achieve more at home and work, leading to an increase in productivity and happiness. We design our products with the goal of simplifying and enhancing lives by providing access to online entertainment and information and facilitating collaboration.

At NETGEAR, we care about our customers and their privacy. We do not participate in the monetization of customer data by selling it to third parties. We acknowledge the importance of privacy as a right, and we respect it. It is not our practice to access or analyze your private data, which consists of millions of megabytes of information transmitted over the internet each day. Your private data, which may include family photos, browsing history, social media updates, banking statements, and other data, is confidential, and we do not have access to it.

At NETGEAR, we employ measures to reduce the quantity of personal data collected from customers and restrict the information we obtain only to what is crucial for our technology to operate seamlessly. While we do collect some product-specific data, which is solely employed to enhance or recommend products and services, it is never shared with third parties.

Governance Structure

NETGEAR's comprehensive data privacy governance structure is built upon the concerted efforts of our customer care, IT, HR, engineering, and legal teams, ensuring cross-functional collaboration. Our VP of Product Security and the dedicated Cybersecurity Committee of the Board of Directors manage product security and data privacy, ensuring continuous monitoring and oversight.

Customer Data Protection

Protecting our e-commerce platform is important to NETGEAR, and we take precautions to protect customer data from unauthorized access and data corruption. We only collect the most vital data that is needed for operations. We do not collect sensitive customer Personal Identifiable Information (PII) such as date of birth, social security number, health or financial information. We have an active cybersecurity program and strictly enforce privacy safeguards within the company through the use of access management and access controls commensurate with the risk to data to ensure access to data is associated with a business need, such as providing customers with support. We also have defense-in-depth security and maintain compliance with Payment Card Industry (PCI) standards, General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA).

For more information please refer to our privacy policy at netgear.com/about/privacy-policy/privacy/.

Data Protection Policy

At NETGEAR, safeguarding your privacy and data is our top priority. Our Analytics Data Policy describes the types of data we collect, how and why we use it, and your options regarding our data processing.

We invite you to review our complete policy at netgear.com/about/analyticsdatapolicy/.
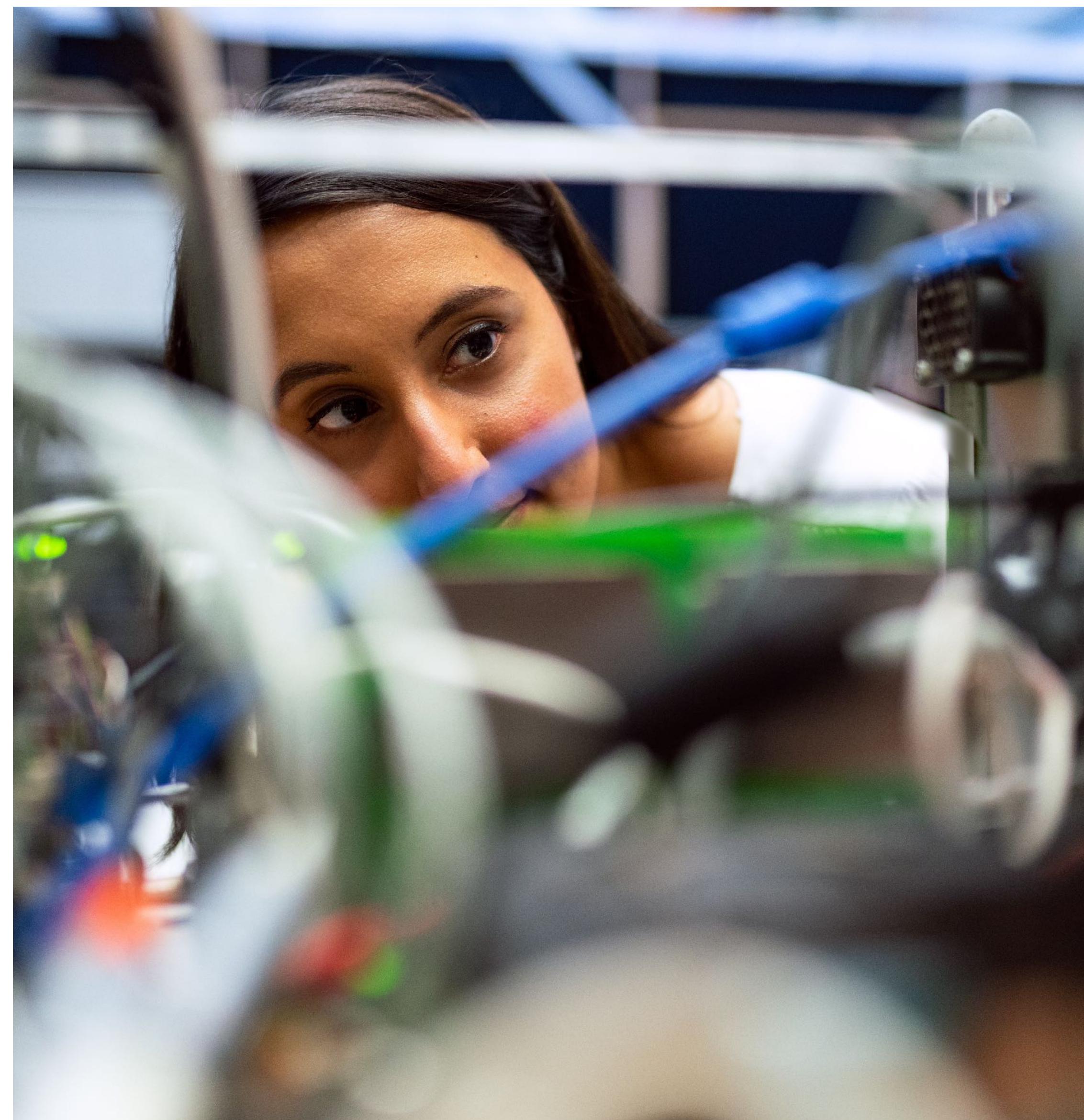
Cybersecurity

At NETGEAR, we optimize our cybersecurity programs to match continuously evolving technological trends. We uphold strong practices through our people and processes, dedicating internal efforts towards our cross-functional cybersecurity team, data protection controls, vulnerability management, and incident response procedures. At NETGEAR, our products are backed by trusted internal operations, reinforcing reliable cybersecurity systems throughout our business. We strive to continuously improve our cybersecurity processes and program effectiveness to align with industry best practices.

Cybersecurity Governance

NETGEAR has a holistic approach to Cybersecurity that leverages our people, processes, and technology to guarantee security is carried out to meet specific corporate needs. Cybersecurity is overseen by the Board of Directors' Cybersecurity Committee. NETGEAR also maintains a Cybersecurity Governance Committee comprised of Executive staff, IT, Audit, and Cybersecurity along with various working groups that meet regularly to discuss our Corporate and Product Security Programs, including reviewing metrics and discussing open vulnerabilities, system hygiene, and remediation plans. We provide our Board with quarterly updates of these Corporate and Product Security Programs.

Our cybersecurity framework is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and team objectives are aligned to each area of the NIST CSF so that we can continuously measure our program and progress of related objectives. Underpinning NETGEAR's cybersecurity framework is a governance and continuous improvement model that includes ongoing measurement and evaluation of the effectiveness of the program, assessing priorities and objectives to continuously improve the program, and regularly reviewing program priorities and performance with executive leadership and the Board of Directors

Security Awareness and Training

To establish a strong culture of cybersecurity at NETGEAR, we focus on enhancing security awareness and training across the organization. We require employees to complete cybersecurity trainings, including new hire security training, annual security refresher trainings, and role-based security trainings. Throughout the year, we reinforce core cybersecurity principles through quarterly phishing exercises and ongoing awareness campaigns. We've found that these trainings help to reduce error, increase awareness, and enhance security for NETGEAR employees.

Vulnerability Management & System Hygiene

NETGEAR takes infrastructure vulnerability management and system hygiene seriously. We've developed a formal vulnerability management program, which includes conducting routine vulnerability assessments on our infrastructure and tracking findings. We also welcome feedback on our security practices via our public bug bounty program, known as our Security Researcher Recognition program. When concerns are reported to us, our cybersecurity team thoroughly investigates and addresses any issues.

Product Design
& Manufacturing

Product Design & Manufacturing

NETGEAR's mission is to offer customers innovative, high-performance, long-lasting products that minimize environmental impact throughout their life cycle.

Sustainable Product Design

At NETGEAR, design plays a prominent role in creating new, sustainable products. Our environmentally friendly packaging eliminates the use of petroleum-based inks and expanded polyethylene. Through design and packaging changes, we have also reduced single-use plastics in new packaging by up to 25%. NETGEAR is committed to developing sustainable and responsible products. Greater than 90% of NETGEAR's retail products meet the Small Network Equipment Voluntary Agreement (SNEVA) power efficiency standards.

Commitment to Responsible Products

We are dedicated to protecting our environment and customers by controlling hazardous substances in our products and complying with relevant regulations. We fulfill our Extended Producers Responsibility (EPR) obligations by participating in various waste schemes, including Waste Electrical and Electronic Equipment (WEEE), Battery (BAT), and Packaging (PACK), to monitor and control the disposal of our products and packaging.

Waste Management

NETGEAR is committed to reducing the amount of e-waste that ends up in landfills as a result of the sale of our products. Across facilities in North America, EMEA, and APAC regions, we recovered 551.3 metric tons of scrap waste. Out of the recovered waste, a portion of the parts are refurbished into new products, and the remainder is sent for further recycling. We partner with a sustainable and innovative recycling company to do what is best for the environment by filtering out different materials and containments.

As electronic waste continues to grow, NETGEAR is responding by reducing or eliminating hazardous materials in our products including decreasing the use of plastics and increasing re-used materials. We are striving for using high renewable energy and achieving carbon neutral in our operations. We are excited to help protect the health and safety of our employees, our customers, and the environment.

Responsible Packaging

At NETGEAR, responsible packaging is a core aspect of our product design strategy. We operate in compliance with all relevant local laws and regulations and prioritize the recycling, reuse, and reclamation of our products and packaging materials. Our commitment to sustainable practices is deeply rooted in our company values.

Our approach to product packaging is guided by a strong focus on sustainability. To reduce our use of plastic packaging, we have phased out foam for all new products. In addition, we have ended the use of poly bags that contain documents and accessories for all new products. In line with circular economy principles, we have established ambitious targets for Post-Consumer Waste (PCW) to divert waste from landfills. By 2025, we aim to use 20% PCW for product packaging and 60% PCW for master cartons. Going forward, we will actively work to integrate sustainable packaging initiatives into our broader environmental strategy.

Materials Sourcing

Conflict Minerals Policy

Conflict minerals, such as tin, tungsten, tantalum, and gold (3TG), are often sourced from conflict-affected and high-risk areas, such as the Democratic Republic of Congo (DRC) and surrounding countries and may extracted by armed groups using forced labor and other human rights abuses. As a producer of network products that contain 3TG, we understand the importance of avoiding conflict minerals and taking responsibility for responsible material sourcing within our supply chain. We comply with all legal requirements related to conflict minerals and are committed to respecting human rights and promoting corporate responsibility. We strive to ensure that the 3TG used in our products do not directly or indirectly finance or benefit armed groups in the DRC or adjoining countries while continuing to support responsible mineral sourcing in the region. To achieve this goal, we have been working closely with the Responsible Business Alliance (RBA), Responsible Minerals Initiative (RMI), Smelter Engagement Team (SET), and our direct suppliers to trace the origin of 3TG and ensure responsible sourcing. We continuously monitor our supply chain operations and take appropriate actions to engage our suppliers in measurable risk mitigation efforts consistent with the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas. For more information, please read our full Conflict Minerals Sourcing Policy.

Critical Materials Risk Analysis

NETGEAR does not have direct contractual relationships with smelters and refiners. Instead, we rely on our direct suppliers and our supply chain to gather and provide specific information on 3TGs used in our products. Every year, we conduct a Conflict Mineral analysis to determine whether the necessary 3TG in our products originated in Covered Countries.

We engage with all of our Tier 1 suppliers and instruct them to provide information on 3TG smelters or refiners (SOR) using the RMI Conflict Minerals Report Template (CMRT). We provide training and education to guide suppliers on best practices and the use of this template. To manage supplier communications, we validate and assess the quality of each relevant response from our suppliers, aligning with OECD Guidance expectations.

After gathering information from our Tier 1 suppliers, we screen 3TG SORs in our supply chain using the RMI's Responsible Minerals Assurance Process (RMAP) and Reasonable Country of Origin (RCOI) data. We identify and manage conflict mineral risks based on the declarations from our suppliers. To mitigate relevant risks, we contact non-RMAP facilities to encourage them to participate in the program and undergo an audit, as well as request that certain suppliers remove specific smelters or refiners from their supply chain that we deem to be high-risk or invalid.

In 2022, we achieved a 100% response rate from all of our Tier 1 suppliers. More information can be found in our SEC filings, available on our website.
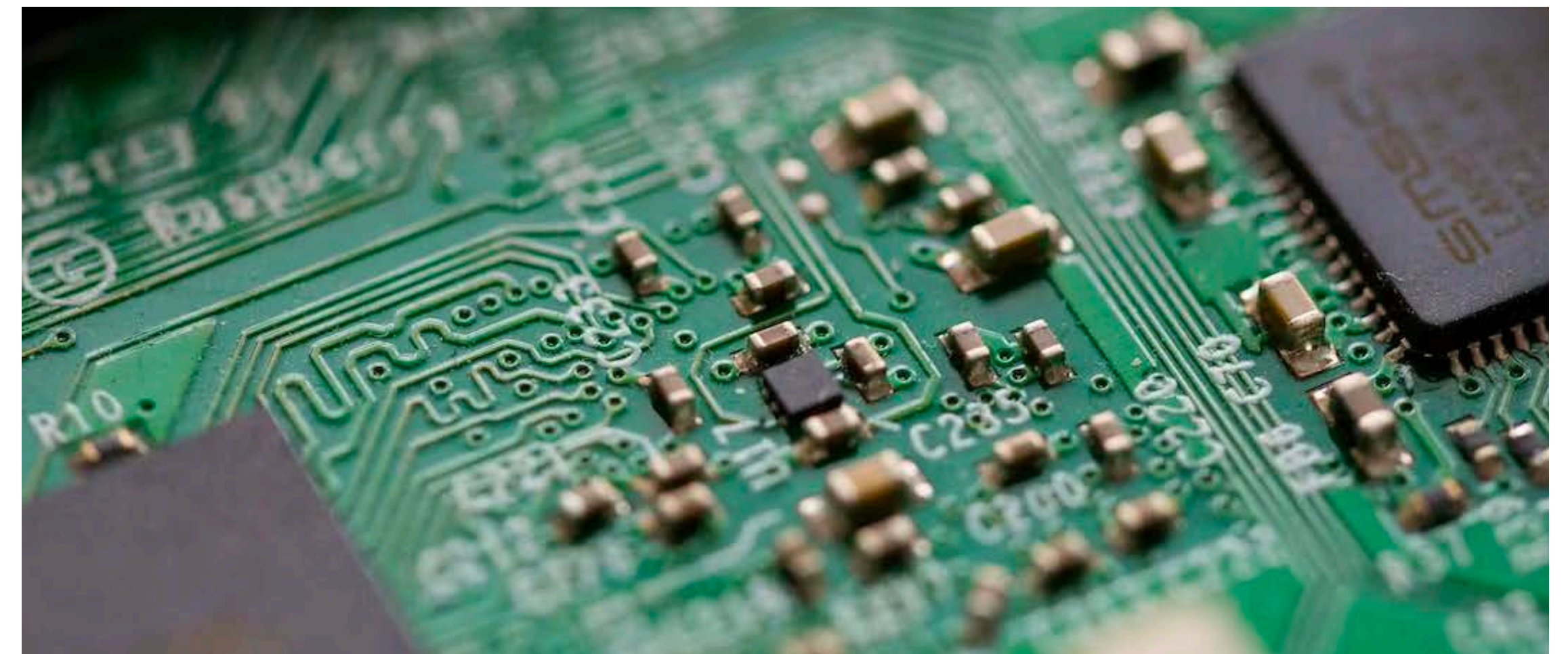
Supply Chain Management

Supply Chain Management

NETGEAR works to build trust through all stages of our product lifecycle, starting in our value chain. We understand that emerging global, social, and environmental factors are increasingly impacting operations and supply chain management. We are committed to promoting the humane treatment of workers, and we hold our suppliers to high standards of ethics through our Supplier Code of Conduct. We regularly audit suppliers to mitigate any potential risk and disclose audit information to promote transparency across our supply chain.

RBA Compliance

NETGEAR has been a long-standing member of the Responsible Business Alliance (RBA), a global industry coalition that works to promote responsible practices in the electronics and other industries. Complying with these standards helps us to demonstrate our commitment to responsible and sustainable business practices, including a more resilient supply chain. Our compliance also increases supply chain transparency, allowing us to identify and address potential risks such as forced labor or environmental violations.

NETGEAR completed the Responsible Business Alliance (RBA) mid-year member compliance reporting in January 2023, covering results from the 2H '22 audits. We noted no critical violations of policies and standards which require immediate escalation in the audits completed. All planned audits in 2022 covered over 80% of production volume, complying with our annual CSR commitment and RBA membership requirement. All audits were carried out remotely throughout 2022 to ensure the safety of our partners and auditors.

Supply Chain Audits

We actively manage the impacts of our supply chain and execute comprehensive RBA Validated Assessment Program audits of our suppliers. NETGEAR is committed to identifying and mitigating high risk activities in our supply chain through these audits. In FY22, our audits covered over 96% of the production volume, complying with our annual CSR commitment and RBA membership requirement. Our FY22 audits identified a total of 212 issues, including 3 critical non-conformances and 117 major non-conformances and 92 minor non-conformances.

We believe in open communication and collaboration with our suppliers by establishing regular follow ups and reviews. NETGEAR holds quarterly business review meetings to help foster stronger relationships between the company and its suppliers, improve communication and collaboration, and drive continuous improvement and optimization of supply chain operations.

Supplier Code of Conduct

NETGEAR is dedicated to ensuring the highest levels of social responsibility are maintained wherever our products are manufactured. We hold a strict policy of zero tolerance towards both forced labor and human trafficking.

To achieve this, NETGEAR has implemented a Supplier Code of Conduct that outlines our expectations from our partners. Our Supplier Code of Conduct mirrors the Responsible Business Alliance (RBA) code and includes guidelines around labor and human rights, health and safety, environmental sustainability, ethical business practices and management systems to monitor and enforce compliance with these requirements. In an effort to combat slavery and human trafficking, NETGEAR conducts a thorough assessment of supply chain risk, social compliance audits of suppliers, and requires compliance with our Supplier Code of Conduct.

Based on the outcome from the assessment, we determine appropriate audit procedures. Through our auditing program, we assess compliance and proactively work with our suppliers to drive change when necessary.

Additionally, we engage third-party on-site supplier audits and conduct internal training on the Supplier Code of Conduct. For more information on this subject, please refer to our Statement Regarding the California Transparency in Supply Chains Act of 2010, the UK Modern Slavery Act of 2015 and our Supplier Code of Conduct.

To read our full transparency statement, please visit: netgear.com/be/about/corporate-social-responsibility/
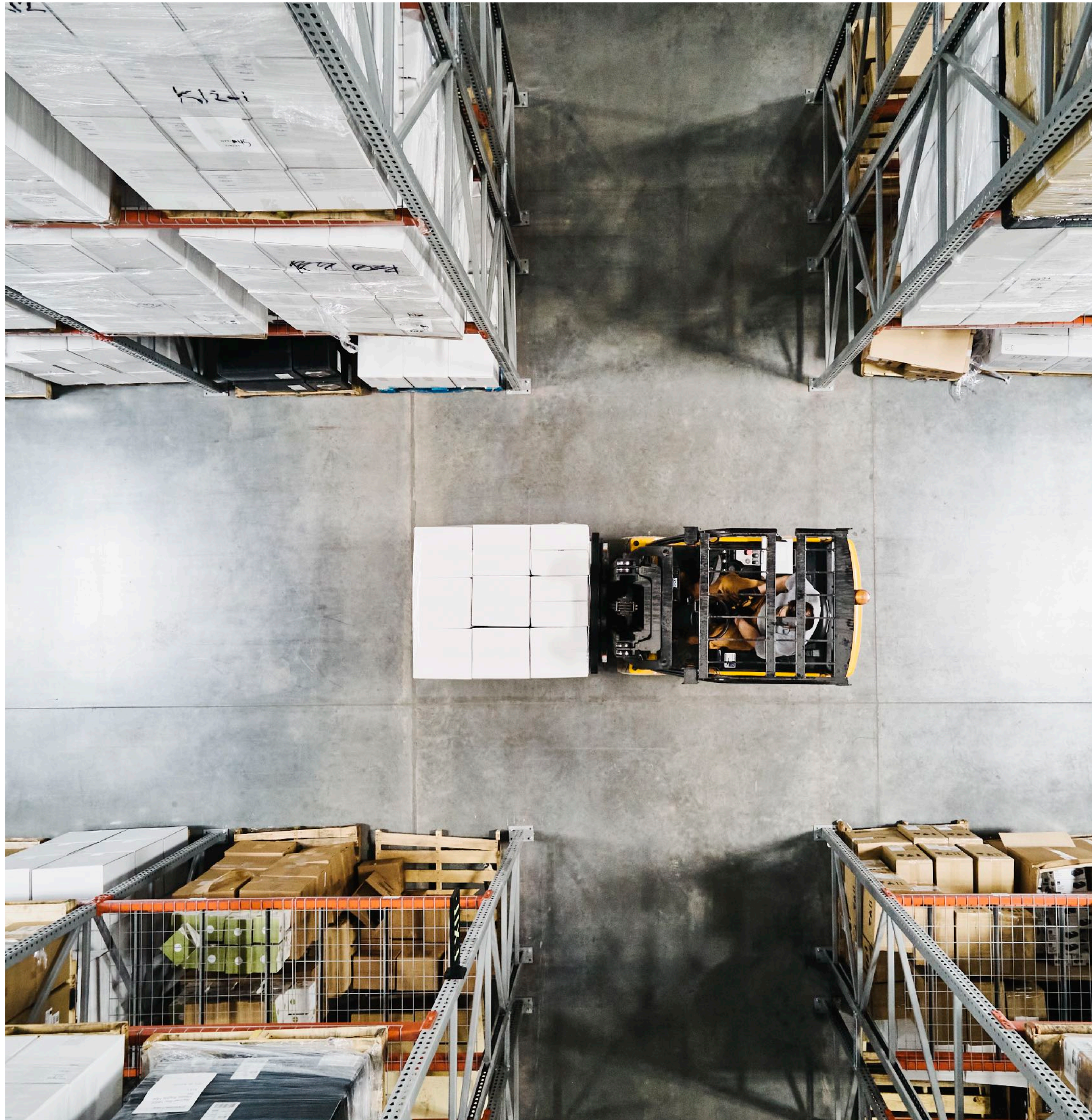
Potential Labor and Environmental Risks

NETGEAR promotes equitable, humane treatment within our business and that of our partners. We work with our employees and suppliers closely to resolve any concerns regarding recruitment, working hours, compensation, discrimination, and freedom of association, hence ensuring a respectful working environment internally and externally. We continuously assess risk related to our supply chain and direct commercial suppliers, and we undertake corrective actions when policies are violated. In 2022, we identified labor violations within our supply chain and, in response, shifted operations to lower risk suppliers. We will continue to monitor similar risks across our global partners to promote labor with dignity.

We have also identified potential environmental risks in our supply chain, including extreme weather events such as floods, tornadoes, typhoons, drought, and snowstorms, that could disrupt our operations, delay the delivery of products and services to customers, and potentially impact our revenue. We plan to conduct associated climate and transition risk analyses in 2023 aligned with the Task Force on Climate-related Financial Disclosures (TCFD). This analysis will provide valuable insights into potential financial implications and enable us to implement measures to ensure our operational resiliency.

Our efforts towards compliance and risk identification reflect our commitment to sustainability and our values. We remain vigilant in monitoring and complying with all existing regulations to avoid any potential financial implications and to minimize the impact of new regulations on our business. We believe that our commitment to sustainability and our proactive approach to risk management will enable us to better serve our customers and access key markets.

Employee Engagement, Diversity & Inclusion

Employee Engagement, Diversity & Inclusion

NETGEAR seeks to foster a diverse working environment, representing a broad spectrum of backgrounds and cultures that promotes innovative ideas and products. We believe that it takes true diversity and inclusion to unleash the power of each of our employees' fullest potential. We are committed to promoting a culture that welcomes and celebrates everyone without bias, reflecting the importance of diversity in our communities. We file the Employment Information Report (EEO-1) annually which provides a demographic breakdown of our workforce by race and gender. To access our EEO-1, please use the following link: Netgear ESG Environmental, Social, and Governance | NETGEAR.

SASB Diversity Metrics

Global Employees	Female	Male
Management	37%	64%
Technical Staff	24%	78%
All Other Employees	53%	47%

U.S. Employees Only	Asian	Black or African American	Hispanic or Latino	White	Other
Management	59%	2%	2%	33%	4%
Technical Staff	64%	4%	5%	26%	1%
All Other Employees	42%	5%	7%	41%	5%

Leadership Diversity

NETGEAR is proud to demonstrate diversity, equity, and inclusion at the highest levels of our company. As of December 31, 2022, approximately 55% of our executive management team self-identify as an underrepresented minority, in terms of race, ethnicity, or gender. In addition, 57% of our independent directors were female. Furthermore, women represented approximately 24% of technical positions worldwide and approximately 36.5% of leadership roles worldwide.

Employee Resource Groups

We work every day to support and cultivate diversity. We offer ongoing development programs, such as Employee Resource Groups (ERG): the Black Employee Resource Group and the Women in the Workplace Resource Group. In addition, we are a proud member of CEO Action for Diversity and Inclusion.

Employee Health & Safety

Health and safety is a top priority at NETGEAR. Providing a safe and clean environment is critical to the success of our employees and business overall. We consistently monitor our workplace with the lens of Health and Safety to maintain a clean environment, practice emergency preparedness, minimize injury and illness, promote industrial hygiene, provide ergonomic training and equipment, machine safeguarding, and more. Our Corporate Emergency Response Team and Return to Work Committee along with our Business Continuity Program equip employees and visitors with essential knowledge and supplies in case of emergency. NETGEAR is also dedicated to updating safety guidelines for all our products. Health and Safety is covered under our Responsible Business Alliance (RBA) guided audit program and corporate workplace operations.

Employee Experience Surveys

Employee engagement surveys help NETGEAR identify areas where we can improve our policies, maximizing the experience and performance of our employees. NETGEAR monitors employee engagement by conducting surveys every two years. We are proud of the fact that our participation rates have never fallen below 95% since initiating the survey in 2014. Our most recent experience survey was conducted in 2021 and had a 99% participation rate.
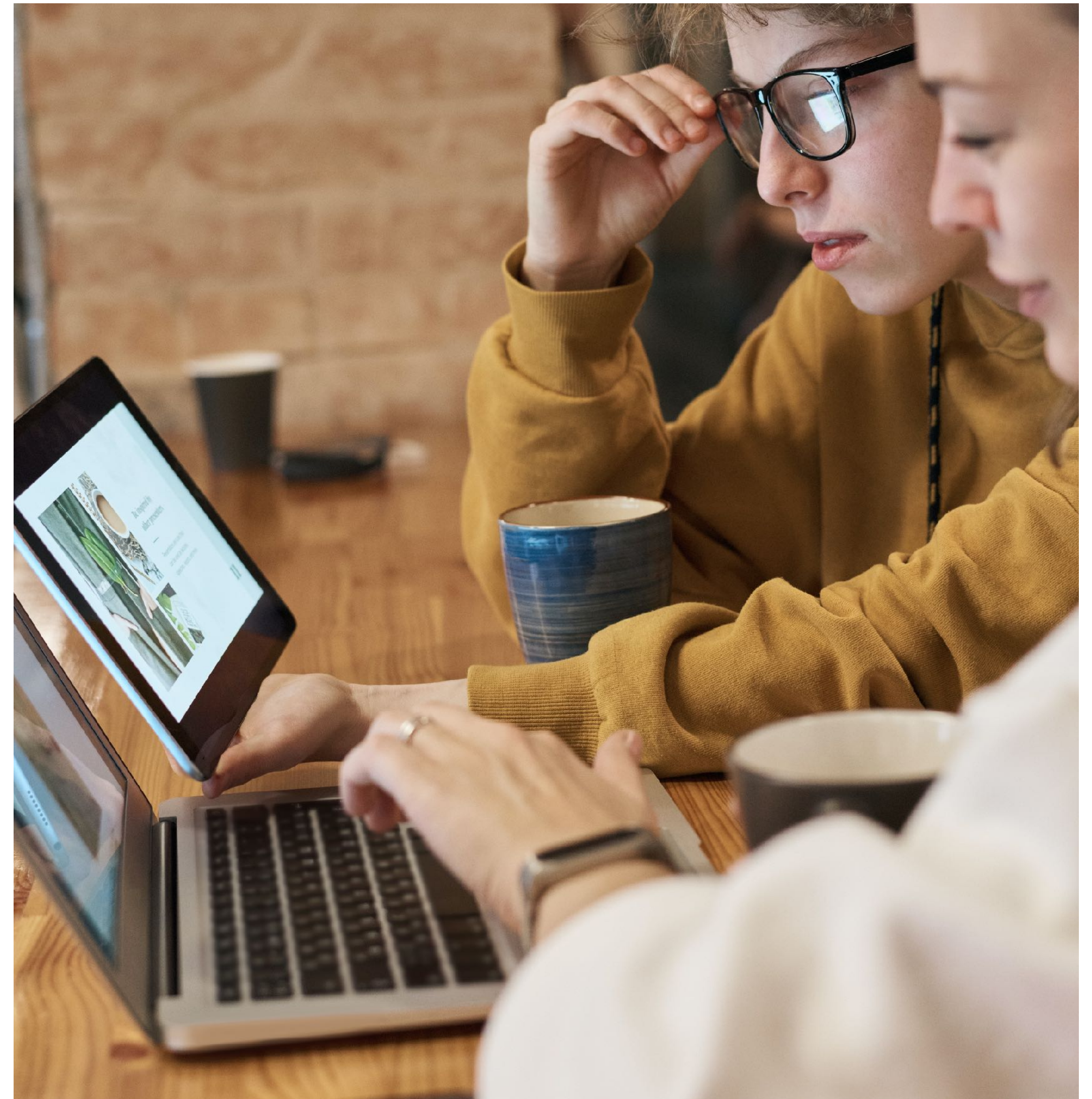
Diversity & Inclusion Training

Providing employees with training on Diversity, Equity and Inclusion (DEI) is a key component of fostering a culture of respect within our workplace. We educate employees on belongingness, empathy, and on our internal efforts toward a more diverse workforce. For example, our Diversity and Inclusion course, required by all employees, helps to ensure that all personnel understand NETGEAR's diversity and inclusion goals, from recruitment to team development. In addition, our Reflection on Bias course helps employees recognize, deal with, and prevent bias through understanding the needs of diverse groups at NETGEAR. Equipping our employees with the tools they need to be an ally brings us closer to our goal of a more inclusive operation.

Pay Equity and Promotion Percentage Analysis

The average annual salary for females and males is 96% and 103%, respectively, of the total company average annual salary. Female directors are paid 110%, female VPs are paid 99%, and female managers are paid 108%. Management monitors and addresses all statistical outliers on a periodic basis.

Community Engagement

As part of our commitment to building a more inclusive environment, NETGEAR works to enrich our global community through charitable contributions and community engagement initiatives. In 2022, NETGEAR's CEO personally matched all employee donations to the Red Cross in support of Ukraine. Our Canada office participates in the Shoebox Project, empowering displaced and estranged women, and donates to the Black Youth Helpline. Our Ireland office raised funds for the Cork University Hospital, participated in the "Giving Tree" program for underserved children, and donated unwanted furniture and office items to St. Vincent De Paul. Employees in our India office collaborate to volunteer and donate to their local community.

Professional Integrity

Professional Integrity

NETGEAR's commitment to professional integrity is a fundamental aspect of our Environmental, Social, and Governance (ESG) practices. Our history and future aspirations are grounded in the belief that 'doing the right thing' is essential to our business operations. To uphold this value, we have established a robust governance structure, regulatory compliance policies, and ethical codes of conduct to promote an honest and ethical working environment. However, we recognize that policies alone are not sufficient, and it is our actions that ultimately define our commitment to professional integrity. Therefore, we aim to ensure that all employees understand and adhere to applicable legal, regulatory, and ethical standards when performing their duties. We actively strive to foster a culture of professional integrity through everything we do, and this includes integrating these principles into our core operations to improve our overall ESG performance.

Ethical Codes of Conduct

At NETGEAR, we take pride in providing our customers with high-quality and innovative products with integrity and honest conduct. NETGEAR's high standards of ethics are outlined in our Code of Ethics and Conflict of Interest Policy, which serves both internal employees and external partners. In 2022, 100% of NETGEAR employees and Board members and over 80% of key suppliers signed our Code of Ethics certification.

NETGEAR's Supplier Code of Conduct helps to ensure that working conditions in our supply chain are safe, that workers are treated with respect and dignity, and that manufacturing processes are environmentally and socially responsible.

Our Anti-Corruption Compliance Program, led by the Governance Risk and Audit and Legal teams, meets on a monthly basis and monitors anti-corruption compliance regulations, including the US Foreign Corrupt Practices Act and the UK Bribery Act. The program executes regular risk assessments (both for internal operations and the supply chain), conducts compliance research, promotes company awareness of key regulatory matters, and communicates regulatory information to our external stakeholders.

Ethics Training

NETGEAR provides numerous ethics-related courses to our employees, including Workplace Harassment Prevention, Security Awareness Essentials, Data Privacy, and Global Anti-Bribery & Corruption trainings. In 2022, 100% of Board members and 99% of employees completed the anti-corruption training. Biennially, NETGEAR's suppliers must complete the anti-corruption training as well. Employees in EMEA, Australia, and India also participate in trainings for Cartels and Dealing with Competitors.

Regulatory Compliance Policies

NETGEAR's goal is to adhere to all regulatory laws, standards, and industry requirements, and our Legal team remains vigilant in assessing the impact of any new regulations to ensure proper consent and disclosure measures are in place. Prior to release, all NETGEAR products undergo thorough testing and certification processes to meet regulatory compliance requirements such as electromagnetic compatibility (EMC), safety, wireless, and telecom. NETGEAR is committed to complying with all applicable laws, directives, standards, and industry regulations, and marks products to meet a variety of country-specific marking requirements, including but not limited to US Federal Communication Commission (FCC) standards, European Union Directives (CE Mark), Japan's VCCI, Australia's RCM, and other marking requirements.

Declarations of Conformity are kept on record and available for viewing, along with other regulatory compliance comments at: netgear.com/about/regulatory.

Board of Directors

The Board's primary responsibility is to monitor and assist management in creating long-term value for NETGEAR's stockholders in an ethical and socially responsible manner. The committees of our Board, specifically the Audit Committee, Compensation Committee, Cybersecurity Committee, and the Nominating, and Corporate Governance Committee, provide governance over these endeavors.

Whistleblower Protection

We take the privacy and protection of whistleblower complaints seriously. NETGEAR provides a reporting hotline for employees and suppliers to anonymously report incidents. To access our anonymous reporting hotline, please use the following link: netgear.com/about/corporate-social-responsibility/ethics/whistleblower-protection/.

In addition, for all new hires and during our quarterly All Hands Meetings, our Legal team includes a presentation on ethics for each global region with a reminder of the Whistleblower hotline.

ESG Charter

We recognize the distinctive importance of governance in enabling the success of our ESG program. At NETGEAR, our ESG program is overseen by our Nominating and Corporate Governance Committee. As part of our commitment to sustainability and corporate responsibility, the Committee regularly reviews and reports to the Board on our ESG performance. The Committee supports NETGEAR in upholding its high standards of ESG governance and integrating ESG principles across all levels of our operations. For more information on the Committee and ESG governance, please see our Nominating and Corporate Governance Committee Charter.

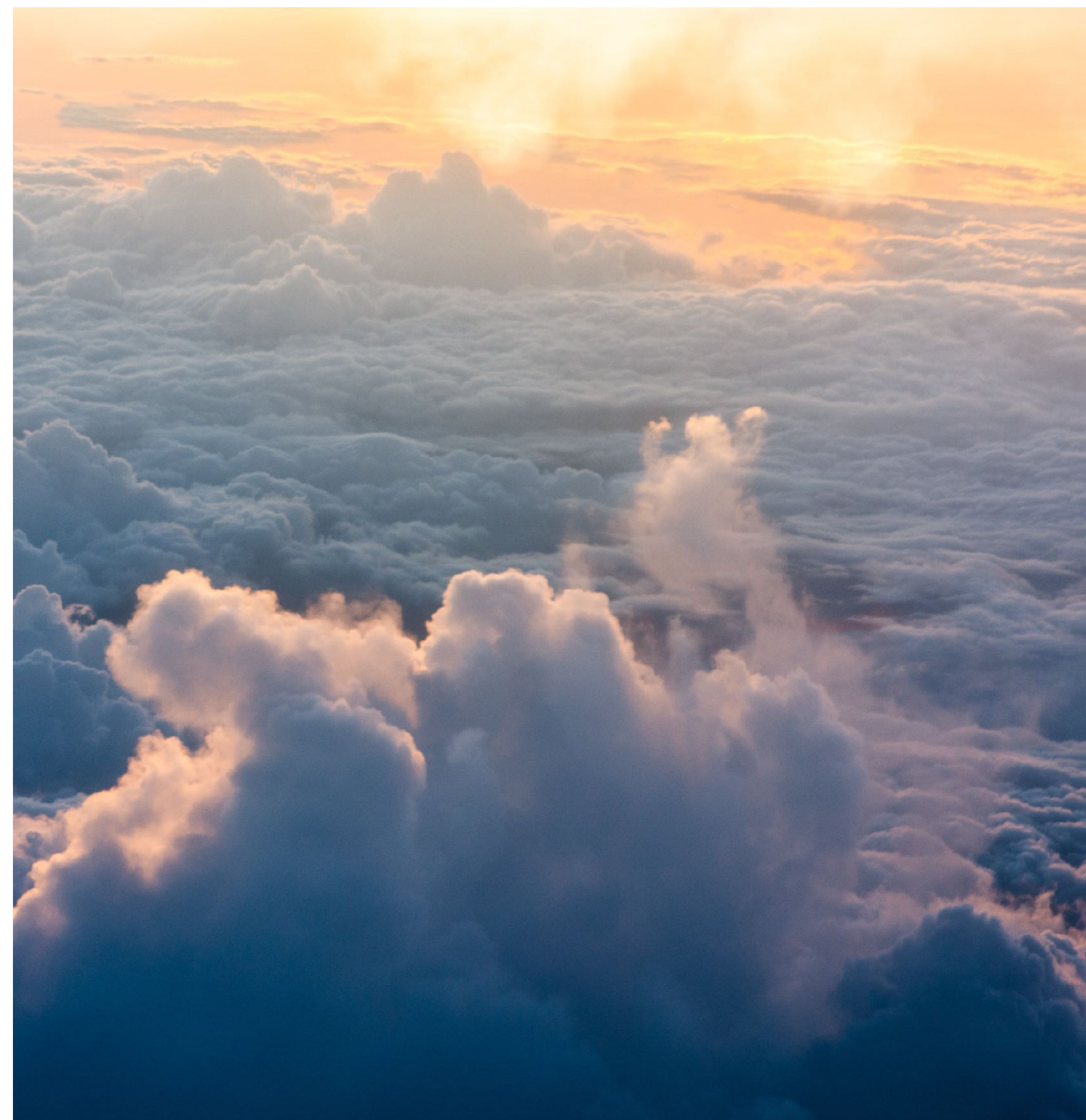# GHG Emissions &
Energy Management

GHG Emissions & Energy Management

NETGEAR strives to make products that are not only high quality but also environmentally responsible. We carefully consider the full lifecycles of our products and packaging, from material extractions to end-of-life disposal, recycling, and reuse. We are constantly striving to become more sustainable for the benefit of our employees, customers, manufacturing partners, communities, and the environment. Our dedication to sustainability is deeply rooted in our company's fundamental beliefs and drives all of our decisions and actions.

Net Zero Target

NETGEAR's vision is to create a sustainable future, and achieving net zero emissions is a crucial step in that direction. We aim to decarbonize all greenhouse gas emissions from Scope 1 and Scope 2 to reach net zero across direct operations and electricity consumption by 2025. Our plan to reach this emissions target prioritizes reducing energy, transitioning to renewable energy, then neutralizing remaining emissions through investment in projects that reduce or avoid greenhouse gas emissions.

We calculate NETGEAR's operational and value chain emissions in accordance with the GHG Protocol. By continuously monitoring our Greenhouse Gas (GHG) inventory process, we are prepared for any potential regulations and can pinpoint areas for improvement, when possible. As we collect environmental data and calculate emissions, we continue to make methodology improvements to advance the completeness and accuracy of our GHG inventory.

Operational Emissions

NETGEAR's operational emissions are divided into two main categories, Scope 1 (direct operations) and Scope 2 (electricity consumption) emissions. In FY22, our Scope 1 emissions from stationary and mobile combustion were estimated to be 387 mt of CO_2e, making up 0.02% of our total carbon footprint. Our Scope 2 emissions from purchased energy were estimated to be 1,219 mt of CO_2e and accounted for 0.07% of our total carbon footprint.

We strive to use precise activity data, instead of estimated or allocated data. This year, we increased our collection of environmental data from global facilities to enhance precision of our Scope 1 and 2 emission calculations. We also used regionally specific emissions factors where possible.

Value Chain Emissions

We have accounted for the following relevant Scope 3 categories linked to our supply chain in our operations: Purchased Goods & Services, Upstream Transportation & Logistics, Operational Waste Generation, Business Travel, Employee Commuting, Downstream Transportation & Logistics, Use of Sold Products, and Final Disposal of Sold Products. We apply tailored calculation methodologies based on the available data for each of these Scope 3 categories. We are continuously enhancing the accuracy and comprehensiveness of our emissions data, ensuring we provide precise GHG estimates.

Our estimated FY22 Scope 3 emissions amount to 1,763,026 mt of CO_2e, representing 99.91% of our total carbon footprint, with a 37% decrease from the previous fiscal year largely due to the methodology changes discussed below. Among the Scope 3 categories, the greatest source of emissions is the Use of Sold Products, accounting for 88.71% of our total GHG emissions. The complete GHG emissions breakdown can be found in the Appendix.

At NETGEAR, improving the accuracy of our environmental data is an ongoing effort. After analyzing our FY21 emissions data, we identified that the majority of Scope 3 emissions originate from the Use of Sold Products. In FY22, to focus on increasing the accuracy of this metric, we assessed our methods for calculating the power consumption of our products by end-users.

Our analysis considered power consumption in various of NETGEAR's modes and product types. We also gathered valuable insights through a customer preference survey on the lifespan and usage patterns of our products. Additionally, we applied regionally specific emissions factors to reflect the power usage by region. These methodology and calculation updates allow us to understand where our emissions are coming from so that we are better able to reduce them going forward.
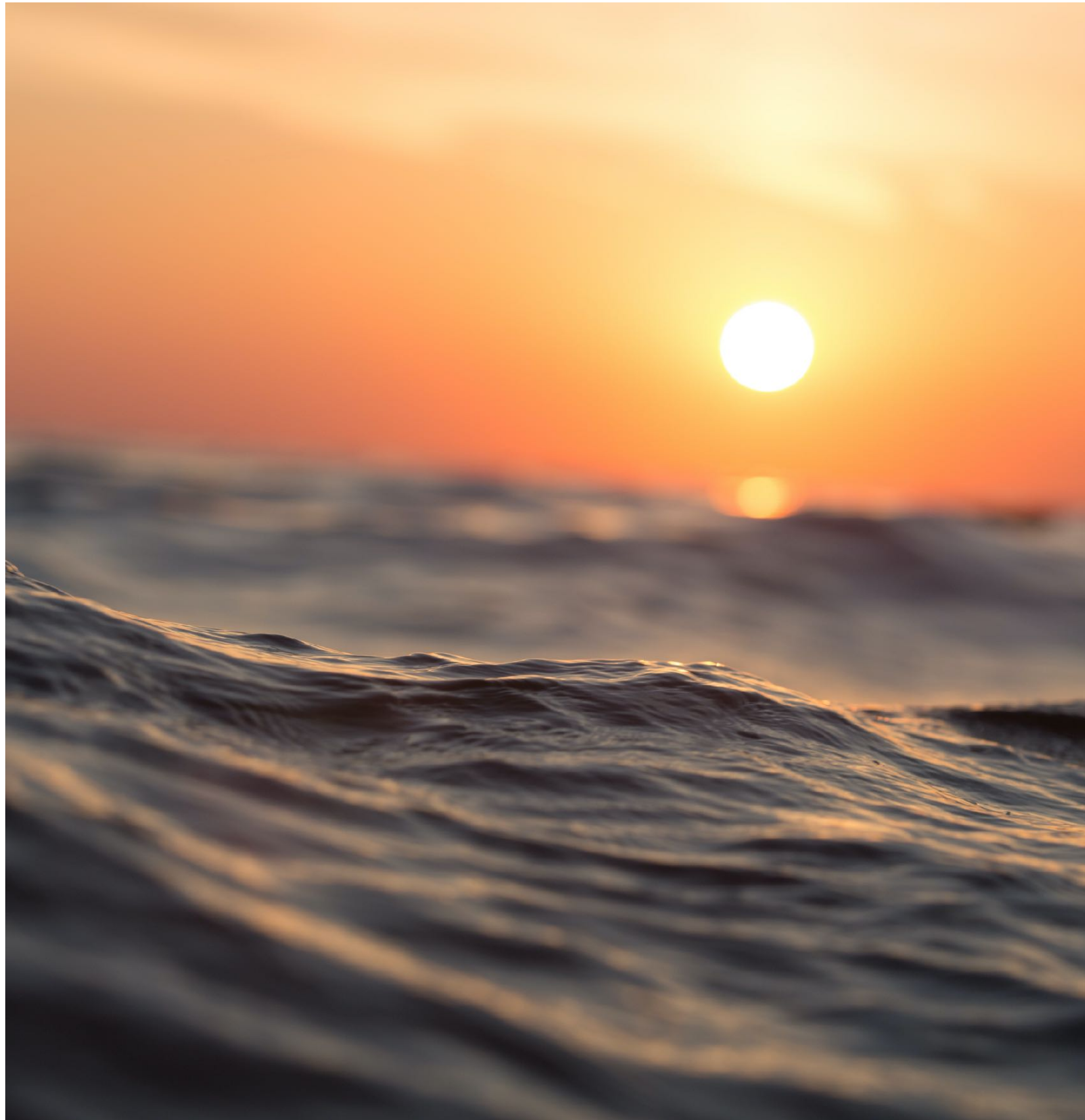
Renewable Energy Usage

We are committed to reducing NETGEAR's environmental footprint by increasing our use of renewable energy in all global facilities. During FY22, we procured 60% renewable and 95% carbon-free electricity for our San Jose headquarters, showing a respective growth of 10% and 15% from FY21. We aim to transition to 100% renewable energy use in our headquarters in 2023. Our Spain and Netherlands offices currently procure 100% renewable electricity, and we recently relocated our Ireland location to an office powered solely by renewable energy as well. We will continue to prioritize the use of renewable energy in our facilities at a global level.
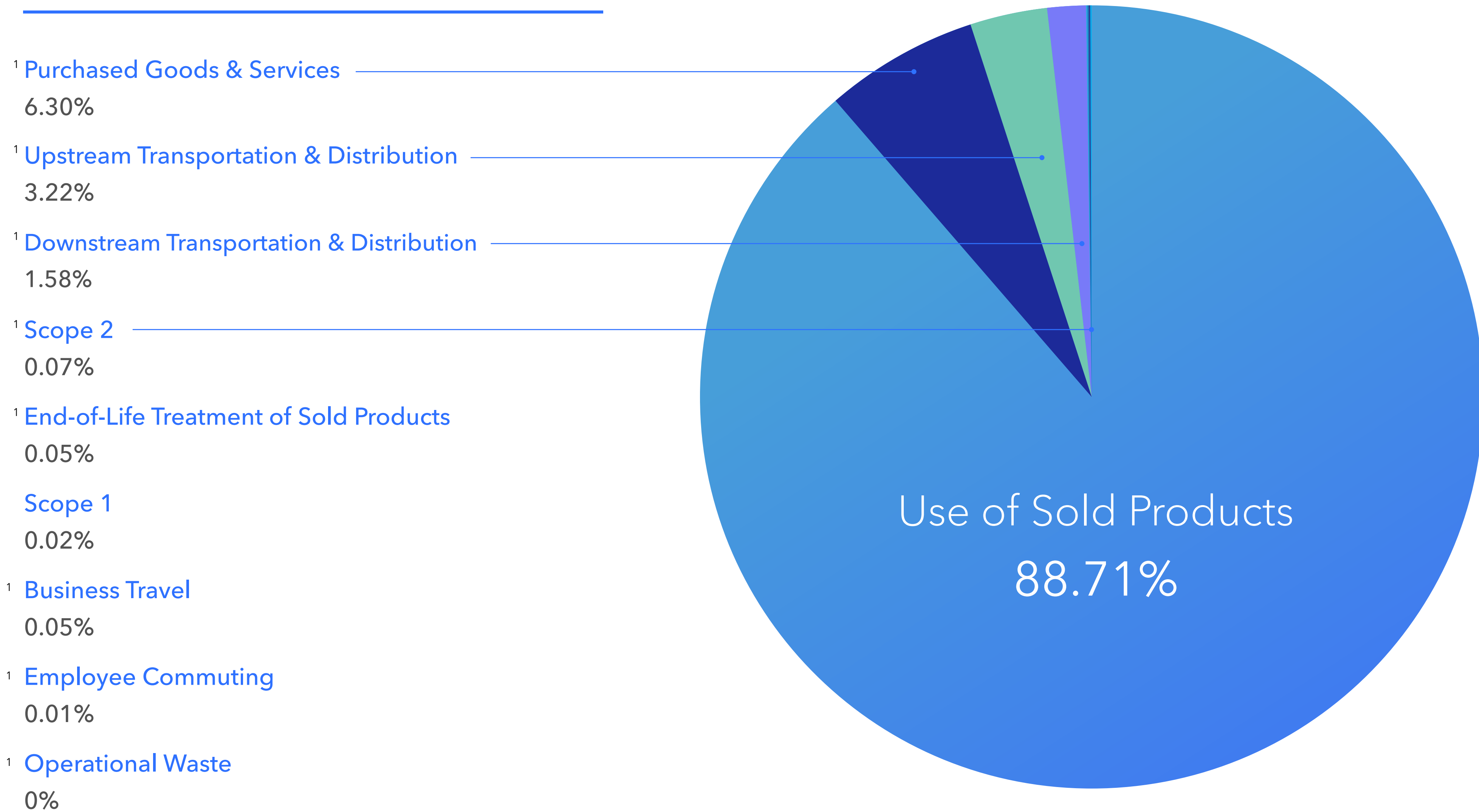
Environmental Targets & Initiatives

We are dedicated to reducing the impact of our operations on the environment. To that end, we have been participating in the Carbon Disclosure Project (CDP) since 2014 and are taking steps to align our future reporting with the recommendations of the Taskforce on Climate-Related Financial Disclosures (TCFD). We continually strive to understand, assess, and minimize our environmental footprint.

Water Usage

NETGEAR's facilities' water consumption amounted to 3,226,494 gallons in FY22. With increasing water scarcity and degradation of water resources, it is becoming increasingly important for us to ensure that we have access to a secure and reliable source of water. We continuously monitor and control water usage to sustainably improve water security.

NETGEAR FY22 Greenhouse Gas Emissions

[1] Purchased Goods & Services
6.30%

[1] Upstream Transportation & Distribution
3.22%

[1] Downstream Transportation & Distribution
1.58%

[1] Scope 2
0.07%

[1] End-of-Life Treatment of Sold Products
0.05%

Scope 1
0.02%

[1] Business Travel
0.05%

[1] Employee Commuting
0.01%

[1] Operational Waste
0%

Use of Sold Products
88.71%

1 Refer to appendix for all categories of Scope 3

ESG Report
Appendix

SASB Disclosures

Hardware Industry Alignment

Topic	SASB Code	Metric	NETGEAR FY22 Disclosure
Product Security	TC-HW-230a.1	Description of approach to identifying and addressing data security risks in products	See the Product Security section of our ESG Report for information on our identification and management of security risks in our products.
Employee Diversity & Inclusion	TC-HW-330a.1	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	See the Employee Engagement, Diversity & Inclusion section of our ESG Report for information on our diversity metrics.
Product Lifecycle Management	TC-HW-410a.1	Percentage of products by revenue that contain IEC 62474 declarable substances	100% of NETGEAR's products may contain a small amount of some of IEC 62474 declarable substances, and we ensure that these amounts comply with applicable regulations. Our products are designed and manufactured with a commitment to comply with the regulations listed in IEC 62474, including RoHS, REACH, Prop 65, TSCA, POPs, etc., and we are constantly working to improve our compliance efforts.
	TC-HW-410a.2	Percentage of eligible products, by revenue, meeting the requirements for EPEAT registration or equivalent	Our products are not eligible for EPEAT registration. However, in 2022 we joined the Small Network Equipment Voluntary Agreement (SNE VA) to improve the energy efficiency of our consumer products sold in the US, and we have met the energy efficiency targets set by the agreement.
	TC-HW-410a.3	Percentage of eligible products, by revenue, meeting ENERGY STAR® criteria	We do not pursue ENERGY STAR certification for our products.
	TC-HW-410a.4	Weight of end-of-life products and e-waste recovered, percentage recycled	We are dedicated to minimizing e-waste generated from our products and strive to implement sustainable practices throughout our operations. Please refer to the Waste Management and Responsible Packaging sections in our ESG Report for further details.

Hardware Industry Alignment

Topic	SASB Code	Metric	NETGEAR FY22 Disclosure
Supply Chain Management	TC-HW-430a.1	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	FY22 audits covered over 96% of NETGEAR's production volume, complying with our annual CSR commitment and RBA membership requirement. No high risk facilities were identified.
	TC-HW-430a.2	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 non-conformances and (b) other non-conformances	FY22 audits identified a total of 212 issues, including 3 critical non-conformances and 117 major non-conformances and 92 minor non-conformances. For all priority non-conformances identified, NETGEAR re-audits the facilities within six months.
Material Sourcing	TC-HW-330a.1	Description of the management of risks associated with the use of critical materials	See the Materials Sourcing section, under the Product Design and Manufacturing portion, of our ESG Report or our Conflict Minerals Sourcing Policy for a description on our management of critical materials, such as tantalum, tin, tungsten, and gold, in our supply chain and operations.

Activity Metrics

Topic	SASB Code	Metric	NETGEAR FY22 Disclosure
Number of units produced by product category	TC-HW-000.A	Number	11,114,929 products across SMB and CHP product categories

GHG Inventory Data

Scope	Category	FY22 (mt CO2e)	% of Total GHG
Scope 1	Stationary Emissions	332	0.02%
	Mobile Emissions	55	0.00%
	Total Scope 1	**387**	**0.02%**
Scope 2	Purchased Electricity	1,217	0.07%
	Purchased Heat	3	0.00%
	Total Scope 2	**1,219**	**0.07%**
Scope 3	Purchased Goods & Services	111,115	6.30%
	Upstream Transportation & Distribution	56,815	3.22%
	Operational Waste	11	0.00%
	Business Travel	805	0.05%
	Employee Commuting	194	0.01%
	Downstream Transportation & Distribution	27,810	1.58%
	Use of Sold Products	1,565,425	88.71%
	End of Life	851	0.05%
	Total Scope 3	**1,763,026**	**99.91%**
	Total Emissions	**1,764,633**	**100.00%**