Responsible Business Update

2024

verizon

About this update

This report details our responsible business performance and contains non-financial disclosures covering the period from January 1, 2024, through December 31, 2024, unless otherwise stated. The inclusion of information contained in this report should not be construed as a characterization of the materiality or financial impact of that information. Our financial disclosures for this period can be found in our **2024 Annual Report on Form 10-K**.

This report covers all of Verizon's operations included in the 2024 financial statements, unless otherwise stated. Where relevant, data measurement techniques, the bases of calculations and changes in the basis for reporting or reclassifications of previously reported data are included as footnotes.

Note on non-financial reporting

Non-financial information is subject to measurement uncertainties resulting from limitations inherent in the nature of, and the methods used for determining, such data. Some of our disclosures in this report are estimates and/or based on assumptions due to these inherent measurement uncertainties. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

Forward-looking statements

Given the inherent uncertainty in predicting and modeling future conditions, caution should be exercised when interpreting the information provided. In this report, we have made forward-looking statements, including statements regarding our goals, targets, commitments and other business objectives. These statements are based on our estimates and assumptions and are subject to risks and uncertainties. Forward-looking statements include information about our possible or assumed future results of operations and include statements using words such as "aims," "anticipates," "believes," "estimates," "expects," "forecasts," "may," "plans," "strategy," "target," "goal" or similar terms. For those statements, we claim the protection of the safe harbor for forward-looking statements contained in the Private Securities Litigation Reform Act of 1995. We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements. For a list of important factors that could affect future results and could cause those results to differ materially from those expressed in the forward-looking statements, refer to Verizon's Annual Report on Form 10-K. Certain information contained herein relating to any goals, targets, intentions or expectations is subject to change, and no assurance can be given that such goals, targets, intentions or expectations will be met. Similarly, there can be no assurance that Verizon's responsible business initiatives, policies and procedures, as described in this report, will continue.

Data assurance

Annually, Verizon obtains independent assurance of select responsible business indicators and analyses. Read the **Independent Accountants' Review Reports** for more information. For other information or claims that are not specifically identified as being independently assured, Verizon relies on the application of internal policies (including those requiring the creation and maintenance of accurate records and the establishment of internal controls over externally reported financial and non-financial information) and compliance with data quality standards and verification procedures set forth in our information governance and control frameworks to validate such information or claims. While the third-party sources of information we use are believed to be reliable, Verizon makes no representation or warranty, express or implied, with respect to the accuracy, fairness, reasonableness, fitness for use or completeness of any of the information contained herein, and expressly disclaims any responsibility or liability therefor.

Responsible business governance

Responsible business at Verizon is built upon four pillars: governance, integration, engagement and reporting. Each of these pillars dynamically supports the others, providing us with a foundation for informed decision-making, transparent communication and effective governance over and accountability for Verizon's most impactful responsible business risks and opportunities.

Board oversight

Our Board of Directors oversees Verizon's responsible business risks and opportunities with the assistance of four standing committees composed solely of independent Directors. Each Verizon Director brings to the boardroom skills or experience in one or more of our priority responsible business issues. While the Corporate Governance and Policy Committee has primary responsibility for overseeing our responsible business commitments, stakeholder engagement and reporting, the full Board regularly addresses responsible business issues during business operations reviews and strategy discussions. Each Board committee oversees the responsible business risks and opportunities that fall under that committee's purview, with each committee chair regularly updating our full Board on its responsible business activities. Topics frequently included on committee agendas or addressed during management updates are listed in the table to the right.

For more information on Board oversight, see our **2025 Proxy Statement**.

Board-level responsible business oversight

Audit Committee	• Business ethics • Sustainability-related business risks • Cybersecurity • Data privacy
Corporate Governance and Policy Committee	• Responsible business commitments, engagement and reporting • Human rights • Political activities and lobbying • Public policy and technology issues impacting corporate reputation • Social impact and community initiatives
Finance Committee	• Capital allocation strategy • Green finance strategy • Renewable energy exposure
Human Resources Committee	• Human capital management • Employee health and safety • Talent acquisition, retention and development

Management councils and committees

To appropriately assess risks and opportunities when making important company decisions, we maintain a number of cross-functional management committees and councils composed of subject matter experts. These councils meet regularly to address a range of matters and oversee our implementation of policies and programs governing accessibility, artificial intelligence (AI), business continuity, sustainability, cybersecurity, global supply chain management and privacy.

Reporting

Our responsible business reporting is aligned with leading sustainability disclosure frameworks and informed by emerging ESG-related laws and regulations, our stakeholder engagement and the results of our prioritization assessment. Our responsible business reporting and policies can be found on our Responsible Business Reporting **website**.

Reporting Center of Excellence

Our Reporting Center of Excellence, composed of teams from Enterprise Risk Management, Legal and Accounting Policy, is implementing an expanded internal control framework for ESG information to facilitate our compliance with ESG-related laws and regulations.

Four pillars approach

Governance

We deliver on our corporate purpose and our commitment to accountability through robust Board oversight and management governance structures.

Integration

We conduct strategic internal and external assessments and implement policies and programs to address identified responsible business-related impacts, risks and opportunities.

Engagement

We aim to build trust through transparency by engaging with a broad range of external stakeholders to obtain a holistic view of our responsible business impacts and strategy.

Reporting

We publish decision-useful information for investors and other stakeholders, leveraging insights from our integration and engagement efforts.

Stakeholder engagement

We proactively engage with our investors, customers and other key stakeholders on Verizon's responsible business activities and priorities. These engagements may include participation, when requested and appropriate, from one or more of our independent Directors. We believe that these transparent and collaborative exchanges strengthen corporate accountability, improve decision-making and ultimately create long-term value. We regularly share what we learn with our Board and senior management.

We also seek to develop meaningful partnerships with external stakeholders to help ensure that Verizon's policy positions are informed by the communities we serve. Our Consumer Advisory Board (CAB), a varied group of stakeholders that advises Verizon on a range of consumer and policy issues, continued to meet throughout 2024. CAB members serve as an informal focus group to test out new policies, practices and products and offer fresh thinking and key consumer insights on discrete business projects, pilots and case studies.

Prioritization assessment

We have been conducting periodic third-party assessments for over 10 years to identify the responsible business issues that are the most relevant and impactful to our business and our four key stakeholders – our shareholders, customers, employees and society. We use the results of these assessments to guide our reporting and stakeholder engagement and prioritize our responsible business integration efforts.

In 2023, we partnered with a third-party consultant to refresh our prioritization assessment. Our latest assessment was conducted with the understanding that operational integrity – namely our robust business ethics, governance and human rights policies and programs – is foundational to our responsible business approach. We have categorized our assessment results into high-priority, priority and emerging issues, all of which we actively manage.

Ethics and compliance

We are committed to operating responsibly and with integrity. We have adopted enterprise-wide policies to reinforce ethical business conduct and provide mechanisms for accountability.

Code of Conduct

Our **Code of Conduct** is a powerful tool that helps employees put our core values into action. It provides employees with clear standards, helpful examples and information on where to go for guidance about ethical decision-making or to raise compliance concerns – including the **Verizon Ethics hotline**, which allows for anonymous reporting or "whistleblowing."

All Verizon employees receive mandatory training on our Code of Conduct at their time of hire, and its provisions are continually reinforced through annual training and periodic communications. The Code is available to employees in 11 languages.

The current version of the Code, like every prior iteration, features extensive coverage of anti-corruption issues, including Verizon's absolute prohibition on bribery, our policy requirement to obtain legal approval before providing anything of value to any government official, the need for adequate controls over third parties who may interact with government officials on our behalf and the importance of maintaining records that fully and accurately document all business transactions.

Verizon's Internal Audit team conducts a variety of annual audits to ensure business and control functions are compliant with the Code of Conduct.

Enterprise-wide compliance program

Verizon's enterprise-wide compliance program is overseen by the Audit Committee of our Board of Directors and managed by our Chief Compliance Officer. We design our compliance program to promote a culture of integrity and accountability throughout Verizon, including its subsidiaries, by:

- Establishing standards of conduct, including the Code of Conduct, corporate policy statements and other guidelines
- Educating employees on ethical decision-making, legal obligations and compliance risks through training and communications
- Assessing legal and ethical risks and providing insights regarding those risks to business leaders
- Providing subject matter expertise and advice regarding specific risk areas
- Surveying management employees annually regarding integrity issues
- Providing employees and third parties with mechanisms to seek guidance, raise concerns and report allegations of misconduct
- Investigating instances of potential misconduct
- Ensuring appropriate corrective action for substantiated cases of misconduct
- Providing regular reports to the Audit Committee of the Board of Directors

Verizon conducts regular compliance risk assessments. These assessments are led by our Chief Compliance Officer, who reports directly to the Audit Committee of the Board of Directors. Annual compliance executive risk assessments of business units and corporate functions are designed to identify and assess existing, evolving and emerging risk areas and develop appropriate risk mitigation plans. The Chief Compliance Officer also oversees periodic risk assessments of specific compliance risk areas, such as anti-corruption.

Third-party risk is assessed by the **Third Party Risk Management Program**, which maintains a formal process to analyze risk and appropriately mitigate concerns involving suppliers and partners. Additionally, Verizon Internal Audit, an independent function that also reports directly to the Audit Committee of the Board, conducts a wide range of audits each year, including audits focused specifically on Verizon's compliance with applicable laws and regulations.

Ethics team

Verizon's integrated ethics and compliance organization delivers consistent guidance on integrity issues, so that as we power and empower how people live, work and play, we do it the right way. Verizon Ethics serves as the primary resource for employees seeking ethics guidance and has two primary functions: fielding questions about ethics issues and responding to concerns and complaints about potential misconduct. The team:

- Provides a confidential online portal and a 24/7 global ethics hotline that can accommodate calls in numerous languages for anyone who wants to seek guidance or report ethics concerns
- Triages concerns and allegations raised and, when appropriate, makes sure that they are assigned to the correct teams in the Finance, Human Resources and Legal organizations
- Provides ethics advice to employees seeking guidance in applying the Code of Conduct and company policies to business decisions or outside interests
- Manages the International Ethics Advisors network, which acts as a force multiplier to provide local, in-country ethics support to employees outside the U.S.
- Administers the annual conflict of interest questionnaire

Verizon thoroughly investigates all claims of misconduct. Teams within the Human Resources and Legal organizations are specially trained to probe potential violations of the Code and provide updates and case resolutions, as appropriate, to reporters of ethics concerns. Our Internal Audit and Enterprise Risk Management teams provide additional support with investigations as needed. Verizon consistently reinforces to all employees that retaliation against anyone submitting complaints or cooperating with an investigation is strictly prohibited, and anyone engaging in retaliation is subject to discipline, up to and including termination of employment. This prohibition is reiterated in training, in communications and during investigatory interviews. We also ensure transparency in investigations by having our Chief Compliance Officer regularly report serious Code violations to the Audit Committee of the Board of Directors.

Anti-corruption

Verizon's anti-corruption program is designed in accordance with the U.S. Department of Justice's corporate compliance program guidance. We enforce a zero-tolerance policy for bribery or corruption of any kind and maintain strong anti-corruption standards designed to prevent, detect and remedy such risks. Employees in relevant operational roles receive targeted anti-corruption training and communications that clearly articulate our expectations, core principles and zero tolerance for any corrupt practices. Our training helps employees understand and comply with various anti-bribery laws, including the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act. We require employees to obtain legal approval before giving anything of value to a public official, including requests by government officials for Verizon to make "expediting" or "facilitating" payments. We have internal controls in place, such as the monitoring of travel, gifts and expenses, to help deter and detect high-risk transactions.

Every two years, we formally review and assess our anti-corruption program in order to identify areas for improvement. Our Chief Compliance Officer reports the findings to the Audit Committee of the Board of Directors. Risk assessments of individual programs, groups and activities within the company are conducted as needed. These assessments identify risks, including corruption-related risks, and recommend process improvements to address those risks in all areas of the business.

Verizon's Third Party Risk Management team oversees our third party due diligence efforts to confirm that all anti-bribery and anti-corruption laws and regulations are followed.

Antitrust compliance

Verizon consistently promotes a culture of antitrust compliance across the enterprise. Our dedicated in-house Antitrust team continually monitors the business and regulatory environment, assesses risk and dynamically refreshes our global antitrust program for maximum reach and effectiveness. The Antitrust team embeds antitrust flags and reporting mechanisms into product development and review processes to scale and systematize identification of potential competition issues by design.

We provide tailored antitrust trainings and require all employees at the manager level and above, as well as lower-level employees in certain teams, to take an antitrust foundations course at their time of hire. We periodically refresh this training. We make the antitrust foundations course, as well as numerous more in-depth courses, available to all Verizon employees on-demand.

Our Code of Conduct mandates compliance with applicable antitrust laws. The Antitrust and Compliance teams investigate any conduct suspected to violate antitrust laws and the Code of Conduct. Employees in violation face repercussions ranging from retraining to termination.

Political contributions and engagement

We participate in the policymaking process at the federal, state and local levels in order to inform public officials of Verizon's views on policy issues. Government policies can have a significant impact on our business, whether they involve decisions on taxes, technology regulation or consumer issues like protecting user privacy and stopping illegal robocalls. We participate in these conversations so that government decision-makers understand how these policies could affect Verizon and our customers, employees and shareholders.

Lobbying

As part of our advocacy, we engage in lobbying at all levels of government through our own employees and through outside consultants. Our Public Policy and Government Affairs organization approves any engagement of lobbyists on behalf of Verizon, and we strictly comply with all lobbying laws requiring disclosure of our activities and expenses.

Political contributions

Political contributions are one way we support the democratic electoral process and participate in the policy dialogue. Verizon makes political contributions where law permits and also operates several political action committees (PACs) that support candidates at the federal, state and local levels. All contributions by Verizon and our PACs are made to promote the interests of the company, our shareholders and our customers and without regard to the personal political interests of Verizon executives. We support candidates of any political party who share our key strategic business and policy priorities, even if we do not agree with them on every issue. We do not make corporate political contributions or PAC contributions to presidential candidates or federal SuperPACs.

Third-party organizations

Verizon supports trade associations and advocacy organizations for a number of reasons, including to reflect our interest in the community, acquire valuable industry and market expertise and support our common goals and interests on strategic policy and business issues. We recognize that we may not always agree with every position of each organization or its members and that these groups often have a variety of members, interests and viewpoints that may not always reflect Verizon's views or priorities. Verizon maintains a policy requiring that our participation in these types of organizations advance core business objectives, and regularly review our participation in these organizations to confirm ongoing alignment with our corporate values and goals. When we disagree with a position of an organization we support, we communicate our concerns through the senior executives who interact with these organizations.

Governance, transparency and disclosure

Verizon participates in policy dialogues with appropriate governance, oversight and transparency mechanisms to mitigate reputational risk. Verizon's political activity is directly overseen by the Legal and Public Policy and Government Affairs organizations. All of our political activity is subject to robust internal controls set forth in our **Code of Conduct** and other corporate policies. The Corporate Governance and Policy Committee of our Board of Directors oversees our participation in the political process, including political giving, memberships in trade associations and reputational risk, and receives a comprehensive briefing on these activities at least annually.

Verizon understands that transparency regarding our political engagement is critical to maintaining the trust of our employees, shareholders and the public, so we publish our **Political Engagement Report**. This report describes our current policy priorities, provides information about lobbying activities and our Public Policy and Government Affairs organization's significant memberships in trade associations and issue advocacy organizations, and lists all of our PAC contributions, corporate political contributions, support for ballot initiatives and independent expenditures for the period covered.

Global tax policy

Verizon is a responsible taxpayer that timely and accurately files all applicable tax returns, pays all applicable taxes and accurately reports taxes in our financial statements. We are committed to maintaining a transparent and positive working relationship with tax authorities in the jurisdictions in which we operate. We also partner with tax authorities and governments to advocate for tax guidance and legislation that provides clarity, is administrable, reduces tax disputes and is socially and fiscally responsible.

Verizon has implemented formal tax governance policies, procedures and controls that strive to meet or exceed best practices on tax governance. Our tax control framework is SOX-compliant and subject to periodic review by the Senior Vice President & Deputy General Counsel – Corporate Taxes, Verizon Internal Audit and our external auditors. Verizon's tax principles, and compliance with them, are overseen by the Audit Committee of our Board of Directors, as well as the Chief Financial Officer and Chief Legal Officer.

Verizon's **Global Tax Policy** provides that Verizon only engages in transactions that are supported by a non-tax business purpose. As such, we only operate in jurisdictions based on the needs of the business and the requirements of our multinational customers. We do not utilize zero or low tax jurisdictions outside the U.S. to minimize our taxes, and we do not engage in tax shelter transactions or transactions that have been identified as "listed transactions" or "transactions of interest" by the U.S. Internal Revenue Service and other taxing authorities. In addition, Verizon's transfer pricing policies are based on the arm's length principle and compliance with guidelines and documentation requirements set by the taxing authorities in the jurisdictions in which we operate.

Supply chain

Verizon's supply chain is the foundation of our secure network. Our suppliers range from the world's largest original equipment manufacturers to smaller providers of equipment, hardware, software and various services. We have implemented risk mitigation processes and an active supplier engagement program to build a resilient and responsible supply chain.

Supply chain management

Third Party Risk Management Program

Verizon's Third Party Risk Management Program supports the company's responsible sourcing efforts. Managed by a dedicated team, the program enables Verizon to identify, assess, monitor and manage a range of supply chain risks, including those that may be associated with the social and environmental impacts of supplier activity. The Third Party Risk Management team works closely with teams across the company to implement a risk management framework and make recommendations regarding future supplier engagement. This work happens throughout the supplier life cycle, including during planning, due diligence, contracting, ongoing monitoring and termination. The Third Party Risk Management team is responsible for providing program oversight, coordination and support to stakeholders across Verizon. Supply chain risk management is reviewed with the Audit Committee of the Board of Directors as part of business risk reviews held throughout the year.

Supply Chain Resilience Management Program

Verizon's Supply Chain Resilience Management (SCRM) Program identifies, assesses, monitors and manages supply chain risks, including disruptions caused by natural and human-induced events, to better coordinate our supply chain activities and aid the effectiveness of our controls. The program monitors how Verizon employees and business partners manage the life cycle phases of our physical products, software, firmware and services.

The program also assesses whether stakeholders need to improve their procedures to more effectively mitigate supply chain risks as they relate to four key categories: security, integrity, resilience and quality. This work is guided by our corporate policy statement on supply chain resilience management and overseen by our cross-functional Global Supply Chain Resilience Governance Council.

When a sourcing request indicates that hardware or software is being acquired, an SCRM due diligence questionnaire (DDQ) may be triggered. The DDQ asks for further details on the products being acquired, such as information about component parts, manufacturer and manufacturing location and any relevant human rights considerations. If any issues are found during the DDQ process, they are resolved prior to the request being fulfilled.

Business partner standards of conduct

Suppliers. Verizon expects all of our suppliers to comply with our **Supplier Code of Conduct** (Supplier Code) and maintain policies and procedures to guard against illegal activity such as corruption, extortion, embezzlement and bribery. Our Supplier Code also forbids the use of child labor and forced labor, protects employees' rights to freedom of association and collective bargaining, as permitted by local laws, and prohibits discrimination on any basis prohibited by applicable law. We reserve the right to review or audit our suppliers' compliance with the Supplier Code.

Sales agents. We recognize that our reputation is affected by the actions of the agents authorized to participate in the sale of our services and equipment to customers. Our Sales Agent Standards of Conduct (Sales Agent Standards) detail the behavior and values that we expect our sales agents to uphold. The Sales Agent Standards also require our sales agents to implement an appropriate management process to ensure ongoing compliance with applicable laws, regulations and customer requirements, as well as with the standards. We reserve the right to review or audit our sales agents' compliance with the Sales Agent Standards.

Promoting compliance. Verizon provides mandatory training on our Supplier Code and Sales Agent Standards for our key suppliers and sales agents. We have established processes for parties to promptly report questions or concerns relating to our Supplier Code and Sales Agent Standards. Any party can raise questions or concerns or report potential or actual violations by contacting Verizon Ethics via email or through our confidential portal and hotline, available on our **website**.

Supporting small businesses

In 2025, Verizon announced a $5B commitment over the next five years to continue investing in America and supporting small businesses through our new Small Business Supplier Accelerator.

The Small Business Supplier Accelerator builds on the comprehensive support that Verizon has provided to small businesses and the communities we serve for years. On top of the $5B in supplier spend, the program aims to empower American small businesses to work with Verizon and other large corporations through targeted training and flexible solutions such as faster payment terms, modified insurance requirements and adjusted indemnification requirements. We are working to make it easier for small businesses to join Verizon's supplier network.

Supplier assessments

We leverage third-party platforms and industry partnerships to monitor supplier environmental performance and strengthen responsible business practices throughout our supply chain.

EcoVadis

In addition to submitting our own annual EcoVadis response, we use the EcoVadis assessment tool to evaluate our key suppliers' responsible business performance. We monitor and assess supplier performance in four areas: environment, labor and human rights, ethics and sustainable procurement. Since 2013, we have assessed 764 key suppliers through our partnership with EcoVadis. When we identify elevated risk through the assessment, we request that the supplier prepare a corrective action plan to improve their current activities, benefiting both Verizon and the supplier.

Joint Alliance for CSR

Verizon is a member of the Joint Alliance for CSR (JAC), an association of telecommunications operators that collaboratively audits common suppliers and looks for opportunities to improve supplier responsibility across our industry. JAC audits are based on a common verification, assessment and development methodology, including the generation of corrective action plans. Topics covered by these audits include child labor, forced labor, worker health and safety, freedom of association, non-discrimination, disciplinary practices, working hours, wages and compensation, environmental protection and business ethics. Through 2024, 1,210 supplier audits had been completed since JAC's inception in 2010, with 150 audits completed in 2024.

Responsible procurement

Verizon is dedicated to responsible sourcing practices that support human rights, ethical conduct and supply chain resilience. We collaborate with suppliers and industry partners to strengthen responsible sourcing practices around the world.

Modern slavery and human trafficking

Verizon is committed to assessing and addressing the risk of modern slavery and human trafficking within our business operations and supply chain. Our Business & Human Rights Program and our Business Risk, Sourcing and Third Party Risk Management teams review the nature and extent of our exposure to the risk of modern slavery on an ongoing basis, focusing on areas of Verizon's supply chain that may be at higher risk. Our efforts are also informed by engagement with industry peers through organizations such as JAC.

Our Business Risk team is trained on modern slavery and human trafficking risk and carries out reputational risk due diligence on new and existing suppliers. The team escalates any potential risk factors to the Third Party Risk Management and appropriate legal teams for review. We describe our efforts in more detail in our country-specific **human rights due diligence statements**.

Conflict minerals

Verizon's conflict minerals due diligence framework was designed to align with the Organization for Economic Cooperation and Development's Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas. Our approach takes into account our position in the conflict minerals supply chain and the fact that Verizon does not typically contract to manufacture the products associated with our business. We require our suppliers, when appropriate, to take steps to verify that their products do not include materials that either directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or in any adjoining country. We also participate in industry initiatives to support responsible raw material sourcing in high-risk countries and regions, including through our membership in the Responsible Business Alliance's Responsible Minerals Initiative. Our Chief Financial Officer is the signatory on our Conflict Minerals Report, whenever such filing is required.[1]

Digital responsibility

We recognize that we have a responsibility to our customers, employees, business partners and shareholders to guard against the risks that come with operating in an increasingly digital world.

Cybersecurity

Verizon's comprehensive cybersecurity program is designed to identify and protect against cybersecurity risks and to position Verizon to rapidly detect, respond to and recover from cybersecurity incidents that impact our company. The program is built on the following pillars:

- **NIST Cybersecurity Framework.** Our program is aligned to the National Institute of Standards and Technology's Cybersecurity Framework, which outlines the core components and responsibilities necessary to sustain a healthy and well-balanced cybersecurity program.
- **Risk identification.** We continually assess the cybersecurity threat and vulnerability landscape using various commercial, government and publicly available information sources.
- **Risk detection.** We use both manual and automated detection methods on a scheduled and ad-hoc basis to identify vulnerabilities within, and threats to, our operations and network infrastructure.
- **Risk evaluation.** Once a cybersecurity vulnerability is detected, we assign a threat severity classification based on the risk profile associated with the vulnerability.
- **Remediation.** Verizon's Information Security team reports all cybersecurity vulnerabilities and their associated threat classification to the appropriate business team for remediation. Deadlines for remediation are set based on the severity of the threat and closely tracked in a central system of record. In the instances when a remediation deadline cannot be met, the Information Security team and the business team work together to deploy appropriate mitigating or compensating controls until the remediation work is complete.
- **Metrics and analysis.** We track the performance of our cybersecurity program by collecting, retaining and analyzing a broad range of data related to our threat identification, detection and response activity. We use this data to assess threat trends, for strategic planning purposes and to enhance management accountability for cybersecurity.

Our processes for assessing, identifying and managing cybersecurity risks include tabletop exercises to test and reinforce our incident response controls, control gap analyses, penetration tests, data recovery testing, internal and external security assessments and threat intelligence monitoring. We also maintain a robust cybersecurity insurance program.

In addition to our in-house cybersecurity capabilities, we also engage assessors, consultants and other third parties to assist with various cybersecurity matters. For example, Verizon periodically validates enterprise cybersecurity maturity through a third-party maturity assessment. This assessment measures Verizon's ability to identify, prevent, detect, respond to and recover from threats to systems, assets and data. The results of the assessment serve as the baseline for enterprise cybersecurity across the company. Annually, we are assessed by an external Qualified Security Assessor across the payment card industry data security standard (PCI DSS) requirements. Our Network Cybersecurity Center is ISO 9001:2015 and ISO 27001:2022 certified and is subject to annual surveillance audits by a third-party assessor.

Verizon has a comprehensive enterprise cybersecurity incident response plan, which is activated in the event of a cybersecurity incident. The plan is a detailed playbook that specifies how Verizon classifies, responds to and recovers from cybersecurity incidents and includes notification procedures that vary depending on the significance of the incident. When warranted by the severity of the incident, our Chief Executive Officer and other senior executives are part of the notification chain.

Integrated cybersecurity risk management

Verizon's Senior Vice President and Chief Information Security Officer (CISO) has responsibility for the management of cybersecurity risks at the company. The CISO and her team are responsible for Verizon's information security strategy, policy, standards, architecture and processes.

Verizon effectuates cybersecurity management by providing for close cooperation among the CISO's team and other teams within the company, as well as by integrating cybersecurity risk into our overall enterprise risk management structures and processes. Each of our business units and certain functional groups have a Business Information Security Officer, who is an integral member of that unit or group but reports to the CISO. This structure provides the CISO with line of sight across the enterprise. The CISO and members of her leadership team also meet regularly with business unit senior leaders, including the CEO and the Chief Financial Officer, to discuss business priorities, emerging threats and trends and the performance of the cybersecurity program.

The Verizon Executive Security Council (VESC) oversees and evaluates the work of the CISO and her team. The VESC is jointly sponsored by the head of Verizon Global Services and the President of Global Networks and Technology and includes Verizon's Chief Compliance Officer, Chief Legal Officer, Senior Vice President of Internal Audit and senior executives in business and technology functions. The VESC provides oversight of all aspects of Verizon's cybersecurity program and, at regular intervals throughout the year, evaluates key cybersecurity metrics as well as planned and ongoing initiatives to reduce cybersecurity risks.

The Verizon Management Audit Committee (VMAC) is responsible for overseeing components of our overall risk management strategy. The VMAC receives quarterly updates from the CISO on Verizon's cybersecurity program.

Verizon also operates a robust internal audit program. Each year, Verizon's Internal Audit team conducts an overall business risk assessment, which includes an evaluation of cybersecurity risks. The results of the assessment are presented to the leaders of the relevant business teams, who are responsible for prioritizing and addressing the risks identified.

Board oversight of cybersecurity risk

The Audit Committee of the Board of Directors has primary responsibility for overseeing our risk management and compliance programs relating to cybersecurity and data privacy. As part of the Board's oversight of risks from cybersecurity threats, the CISO leads an annual review and discussion with the full Board dedicated to Verizon's cybersecurity risks, threats and protections. The CISO provides a mid-year update to this annual review to the Audit Committee and, as warranted, additional updates throughout the year. The Audit Committee also receives a report from senior management on Verizon's cybersecurity posture and related matters at each of its other meetings during the year at which the CISO is not present.

Third-party risk management

We have implemented processes to identify and manage risks from cybersecurity threats associated with our use of third-party service providers. Verizon's Third Party Risk Management Program establishes governance, processes and tools for managing various supplier-related risks, including information security. As a condition of working with Verizon, suppliers who access sensitive business or customer information are expected to meet certain information security requirements.

Data Breach Investigations Report

Verizon's perspective on data security is based, in part, on our annual **Data Breach Investigations Report** (DBIR), a comprehensive study of data security incidents from around the world. In 2024, the DBIR analyzed over 30,450 cybersecurity incidents. This actionable intelligence helps companies large and small better understand the threat environment and plays an important role in shaping Verizon's own cybersecurity efforts.

Data privacy

Verizon recognizes that protecting the privacy of customer, employee and business partner data is an essential part of operating and growing our business. We have established measures to protect the privacy and security of the data entrusted to us and to support compliance with current and emerging international, federal and state data privacy legislation. Our Chief Privacy Officer oversees this work and reviews data privacy risks and mitigating actions with the Audit Committee of our Board of Directors at least annually.

Verizon has adopted corporate policies and operating procedures governing the use, retention and protection of the data we collect. Detailed information about Verizon's privacy policies and practices can be found at our **Privacy Center**, which contains links to our Privacy Policy, supplemental policies for some of our apps and services and privacy policies maintained by our affiliated companies. We update our privacy policies to reflect developments in products, services and technologies. We do not use personal information in a manner that is materially different from the terms of the privacy policy that was in place at the time that information was collected without providing notice and obtaining consent.

Our policies and procedures are subject to numerous controls. We utilize internal audits and employee, contractor and supplier training to promote ongoing compliance. Verizon has implemented a privacy governance framework to map privacy requirements to specific operational controls, which are assigned to appropriate owners. As part of the framework, Verizon tests and monitors the controls and develops remediation plans where necessary. Key employees' annual performance agreements include terms related to their ownership of controls.

Verizon continuously monitors for legislative and regulatory developments and updates our policies and processes as needed. We continue to advocate for a uniform federal privacy framework that would apply to all participants in the technology ecosystem.

Our stewardship of personal information

We are committed to handling the personal information we collect from and about our customers, employees and business partners appropriately throughout every phase of the data life cycle, including collection, use, disclosure, retention and destruction. We disclose our practices and have in place policies related to each phase. We conduct privacy reviews when we develop and modify products, systems or other initiatives and purchase or sell assets. Our privacy impact assessment process discussed on the next page provides a platform for formalized review of initiatives that involve the personal information entrusted to us. We have also implemented a third-party risk management process that identifies, assesses and mitigates risks throughout the life cycle of our engagement with suppliers.

Collection and use. We collect and use personal information as we describe in our publicly available privacy policies and in some cases, for business customers, in accordance with contractual requirements. We seek to minimize the amount of personal information that we collect and retain, and we provide customers several ways to review and keep their account information up to date. We provide customers with easy-to-understand privacy choices based on the sensitivity of the personal information and how it will be used or disclosed. We have implemented specific controls around consumers' most sensitive data.

Disclosure. We share personal information within Verizon and with suppliers, contractors and partners for a variety of purposes as described in our privacy policies. We require suppliers and contractors that process personal information to use it only for the purpose for which it was provided or otherwise as permitted by law and to put in place data security measures that provide the same material protections as those we use at Verizon. We enforce these requirements through binding contractual provisions that are put in place before personal information is shared.

Data retention and destruction. We maintain corporate policies governing data retention and destruction and review relevant practices as part of our privacy impact assessment process. We retain personally identifiable records only as long as reasonably necessary for operational, legal, tax, audit, investigative or security purposes. We meet the requirements of our enterprise customers by contractually agreeing to custom data retention timelines and data destruction practices when needed.

Our employees are responsible for cooperating with and assisting business owners in fulfilling the obligations and requirements of Verizon's Information Security Framework, as well as in complying with applicable laws. We impose our information security requirements on suppliers who handle customer data, as well as additional privacy requirements on suppliers who handle personal data.

Training. Verizon's annual Code of Conduct training, which is mandatory for all full- and part-time employees, has substantial privacy and information security content. For targeted groups of employees, we supplement this general course with training on the handling of customer proprietary network information and other privacy and information security topics. We provide periodic reminders and communications to employees highlighting information security and privacy issues. Verizon also provides privacy and information security training to employees of third parties who have access to certain Verizon customer information. We are focused on continued improvement of the quality, quantity and cadence of third-party training.

Customer and data subject rights. Customers and other individuals in the U.S. can generally obtain from Verizon the personal information we have collected from or about them. We honor requests to delete personal information except to the extent such information is needed to provide service to the customer or for legal, tax, audit, investigative or security purposes.

Our wireless and wireline customers can use the **Verizon Privacy Dashboard** to request data access, correction or deletion. Where provided by law, consumers have the right to appeal decisions. Outside of the U.S., data subjects may ask to access or delete personal data consistent with local laws.

Consumer inquiries. Customers and others can contact Verizon's Privacy Office electronically and by postal mail. Dedicated Privacy team members review these inquiries and respond to questions related to our privacy practices around specific products, services or programs and help customers exercise their privacy and marketing choices.

Privacy impact assessment processes

We utilize a privacy impact assessment process to understand how a new product or system collects, uses, retains and shares data and to identify applicable legal, regulatory and policy requirements. This process aligns in many respects with the policies outlined in the U.S. Office of Management and Budget's Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB M-03-22). We also evaluate certain activities through a data protection assessment process designed to identify risks for certain types of activities that present heightened privacy impacts.

Children's privacy

We comply with applicable laws related to the privacy rights of minors, including the Children's Online Privacy Protection Act (COPPA) and state age-appropriate design codes. When Verizon operates online services covered by COPPA, we do not knowingly collect personal information from children under age 13 without parental consent, except where such collection is expressly permitted under COPPA for purposes of internal operations. We provide parents with information about their rights under COPPA, including instructions about how they can review information collected from children.

Privacy and security by design

To consider and mitigate privacy, security and human rights issues from the earliest stages of new product development, we apply a "privacy and security by design" approach. We take other appropriate steps to provide our customers with meaningful post-launch privacy and security protections.

Requests from law enforcement

Verizon publishes semi-annual reports that present the number of demands for customer information we receive from law enforcement in the U.S. and other countries in which we do business. To learn more about how we handle these requests, see our most recent **Transparency Report**.

Responsible AI Program

Verizon, like many companies, uses AI to improve our products, services and business operations. We understand that poorly governed AI applications can result in unintended consequences, including potential bias or discrimination, whether in design, implementation or the data sets used to train AI models. Responsible AI is the practice of designing, developing and deploying AI to engender trust and scale AI with confidence.

Verizon's Artificial Intelligence and Data organization, together with our Data and Analytics Office, manages and implements Verizon's centralized, enterprise-wide Responsible AI Program. Our Responsible AI Program is overseen by a high-level leadership council and a dedicated team with support from other internal subject matter experts, including our Privacy team and Business & Human Rights Program. This program is governed by a risk-based approach and informed by emerging global definitions, concerns, frameworks, regulations and legislation in AI and related fields. We continue to update our AI risk analysis to address emerging risks, including those associated with generative AI.

We are committed to a set of foundational principles that provide direction to the many V Teamers using AI and align Verizon's use of AI with the values of our company, as summarized in the table to the right. While these principles do not represent the full breadth of AI issues, they are intended to inform common terminology for AI-related efforts, guide our efforts to leverage new AI technologies in ways that positively impact our stakeholders and establish Verizon as a trusted brand and partner with respect to AI.

Verizon's Responsible AI Principles

Governance	Verizon employs a risk-based framework for developing, using and overseeing AI. We have processes to oversee Verizon's development and use of AI, and our highly skilled employees have an important role to play in considering the risks, impacts and benefits of using AI.
Respect for privacy	Verizon recognizes that AI systems must incorporate a privacy-by-design approach, including consideration of the data used to train models and the data used to make business decisions. Verizon's use of AI must comply with our privacy policies and applicable laws.
Respect for human rights & responsibility to society	We design and train Verizon systems using strategies to identify and reduce potential bias or other harms. We address the risk of unlawful or unintended bias in AI systems with appropriate governance and mitigation measures.
Technical robustness	Verizon uses industry-accepted metrics to evaluate AI solutions' ability to generate accurate, reliable and reasonably consistent outputs. We employ a security-by-design approach, which proactively and holistically monitors for and mitigates against security threats.
Transparency	Verizon understands that in order to provide reliable and positive user experiences, our use of AI systems requires transparency. Verizon is committed to clearly explaining its governance, use and monitoring of AI systems.

Digital accessibility

Verizon provides products and services that are accessible to the broadest range of customers. Our team of accessibility professionals continuously works to make each customer's experience the best it can be. Our commitment to "accessibility by design" means that we are constantly working to incorporate the needs of people with disabilities into our initial design process of new products, services, digital information systems, web content, physical spaces and other facilities. We collaborate with our ADVANCE employee resource group, as well as industry partners, to remain informed about accessibility issues and improve user experiences. Our Disability Advisory Board, an external board of trusted leaders from disability organizations, met with senior Verizon leaders throughout 2024 to support our accessibility journey by providing expert advice on key strategic relationships and initiatives.

Verizon's dedication to providing a digitally accessible experience begins with compliance. To optimize the digital experience for all of our customers, we strive to meet or exceed the online accessibility standards recommended by the World Wide Web Consortium in its Web Content Accessibility Guidelines (WCAG 2.1 AA). For more information, see our **Accessibility Resource Center**.

Our services and tools are made for the way our customers communicate and include support like visual assistance, accessible content, auditory support and mobility tools. We continually test the accessibility of our products using the same assistive technology as our users: screen readers, keyboard-only navigation and alternate-input devices. We also check color contrast, closed captioning and transcriptions. We have standardized processes and procedures for proactive and reactive testing to resolve accessibility bugs across our products. These initiatives are critical to our ongoing efforts to level the digital playing field.

Verizon's National Accessibility Customer Service Center and Center for Customers with Disabilities have trained staff to provide services and customer support for existing consumer wireless customers and FIOS residential/traditional phone service customers, respectively.

Digital safety

Helping parents keep children safe online

Verizon provides parents with products and services that empower them to make the best decisions about how to guide and moderate their children's online experiences.

We work to keep parents up to date on the latest online safety advice through our **Parenting in a Digital World portal**, which features guidance for parents of children of all ages. Parents can easily find practical advice on topics that range from screen time for toddlers to teen driver safety. Information on the portal is carefully vetted and comes from a variety of expert sources.

Verizon also offers parents a portfolio of products and services that gives them the ability to customize their children's digital experience through robust parental controls and differentiated product offerings. **Verizon Family** gives parents the tools to monitor their child's online activity, block harmful content, track location and view driving behavior. Verizon also offers a suite of products designed specifically for children, which is featured on Verizon's **Family Tech hub**.

Combating online child exploitation

We recognize that we have an important role to play in combating the use of the internet to exploit children. As a leading provider of internet access services and cloud storage, we understand that the same tools that empower our customers to communicate with family and friends and safeguard their digital memories can also be misused to disseminate child sexual abuse material.

Verizon's work to combat online child sexual abuse and exploitation begins with close partnerships with two organizations on the frontline of the fight: the National Center for Missing and Exploited Children (NCMEC) and the Technology Coalition. We voluntarily report offending images and videos to NCMEC, along with attribution information, each time we encounter child exploitation material on our digital platforms or in our stores.

We also serve on the Board of Directors of the Technology Coalition, the leading industry working group fighting online child exploitation.

Through our work with the coalition, Verizon has helped enable Project Protect, an ambitious and multifaceted plan to eradicate online child sexual exploitation and abuse through investments in technology, collective action, transparency and accountability, information and knowledge sharing and independent research.

In addition to our strong partnerships, we have implemented measures to protect our platforms from child predators. These measures include:

- Scanning images and videos uploaded to Verizon Cloud with PhotoDNA and CSAI Match, technology products that enable us to match uploaded media against databases of known child sexual abuse material
- Conducting human reviews to evaluate the material flagged by our scanning technology and take action on user reports of child sexual abuse material. All confirmed child sexual abuse material is reported to NCMEC, which acts as a clearinghouse for law enforcement

Robocalls

We provide our customers with ways to directly protect themselves from robocalls. A robocall is an automatically generated and/or prerecorded phone call that can be a nuisance, and in many cases, a threat. Learn more about Verizon's tools to identify and filter robocalls **here**.

Radio frequency emissions

Verizon equipment complies with Federal Communications Commission requirements that all wireless communication devices sold in the U.S. meet guidelines for safe human exposure to radio frequency energy. We provide more information on radio frequency emissions on our **website**.

Network resilience

Verizon is an industry leader in operating reliable and resilient networks that support our customers' needs and keep them connected. Our networks in the U.S. include design elements, technologies and business processes that work together to enhance the reliability of our services. For more information about Verizon's business continuity planning and disaster response efforts, see our **latest TCFD Report**.

The resilience of our networks reflects many years of significant investment that supports our commitment to serving our customers even in times of crisis, from extreme weather to other emergency events. We make enhancements to our facilities and networks based on assessments of the relevant geographic area and corresponding types of risks, for example:

- **Fire.** In fire-prone areas, we proactively eliminate brush and waste that could fuel fires around our buildings and cell sites.
- **Hurricanes.** In Florida, our "super switch" facilities can withstand Category 5 hurricane winds to enable us to continue to serve our customers.
- **Tornadoes.** In Missouri, our underground storage unit protects emergency vehicles and network equipment.
- **Blizzards.** Our sub-zero switch in North Dakota is housed in a building designed to withstand extreme snow, ice and flooding.
- **Rising sea levels and flooding.** Along the coast, we have elevated our cell towers and base stations to shield our power supply, generators, cooling systems and transport interface from rapidly rising waters.

To mitigate the impact of power disruptions on our operations, we have battery backup at every switch and every macro cell. We also utilize backup generators at a majority of our macro cells and at every switch location. In addition, we have a fleet of portable backup generators that can be deployed as needed. In the case of fiber damage resulting from severe weather events, we may deploy satellite and microwave links to serve as alternative paths while the original infrastructure is repaired or replaced. For more information, see Managing systemic risks from technology disruptions in our **SASB Standards index**.

Business continuity and event management

Our Business Continuity and Event Management (BCEM) organization identifies risks, develops action plans and coordinates response and recovery efforts for all major disasters. An executive steering committee, composed of senior executives from across the enterprise, oversees our BCEM framework and programs. The BCEM framework, which follows Verizon's corporate policy statement on national security emergency preparedness, is designed to protect and support Verizon personnel, critical operations and infrastructure during emergencies and disasters, including human-induced and weather-driven events. The framework supports operational preparedness, mitigation, response and recovery by weaving BCEM into Verizon decision making; focusing on internal and external partnerships; optimizing BCEM tools and technology and developing a comprehensive training program for the BCEM team, strategic partners and employees.

The BCEM organization operates our Global Event Management Center (GEMC), which actively monitors and assesses potential threats to Verizon's operations around the world. When a potential threat or significant event has been identified, the GEMC performs a risk assessment, consulting with internal and external subject matter experts, and disseminates situation information and intelligence to key response groups within Verizon. The GEMC leverages Verizon's in-house weather monitoring platform that uses multiple sources of weather data to identify potential impact areas and conduct pre-storm risk preparation activities. Restoration teams and equipment are then stationed in those areas to protect our facilities and personnel. The GEMC also leads our event response efforts, including our crisis management teams.

As a global company, Verizon aligns our internal business continuity program with several domestic and international industry standards, including, but not limited to, ISO 22301:2019, ISO 22320:2018(E), FEMA NIMS and OSHA 29 CFR 1910.38.

Disaster response

During times of crisis, Verizon stands ready to support our first responders, communities, customers and employees with disaster response and recovery efforts. **Verizon Frontline**, our advanced network and technology product offering for first responders, provides on-demand emergency assistance to government agencies, first responders and public safety officials nationwide during crisis situations. Verizon has a collection of nearly 600 deployable assets to assist public safety teams, including mobile emergency calling centers, mobile cell sites, generators and repeaters, tethered and AI-enabled drones and satellite communication capabilities. Our Tactical Humanitarian Operations Response vehicle serves as a mobile command center capable of deploying Verizon Frontline technology, including Verizon 5G Ultra Wideband and other high-quality communications and applications, under nearly any condition. We have partnered with the National Oceanic and Atmospheric Administration (NOAA), which is leveraging high-level aerial imagery of storm-damaged areas from our drones to improve the accuracy of future storm forecasts.

After major natural disasters, teams across Verizon Frontline Crisis Response, Major Emergency Incident Response, Dedicated Incident Response and Emergency Response are on-site conducting network restoration and supporting our affected customers and communities. The public can access real-time updates on Verizon's relief and recovery efforts through our **Emergency Resource Center**.

Managing natural resources and waste

We have implemented policies and programs designed to responsibly manage the natural resources we use and the waste we produce.

Environment, health and safety management

Verizon's **Environmental, Health and Safety (EHS) Policy** describes our commitment to protecting the environment and the health and safety of the V Team, our customers and the communities where we operate.

Verizon's Environment, Health and Safety department is responsible for our EHS management system, which provides a framework for identifying, controlling and reducing the health and safety risks associated with our operations and reinforcing environmental stewardship. We develop and manage environmental compliance programs to promote safe practices across our operations, providing guidance and training for the proper handling of major equipment, batteries, hazardous materials and high-risk activities. Besides performing regular management system assessments, we also conduct internal and third-party annual compliance audits and inspections at facilities worldwide. These assessments aim to identify site-specific issues and to educate and empower employees to take corrective actions. Our EHS efforts are directed and sustained by experienced professionals who support our global operations and facilities.

Our Incident Management Standard delineates responsibilities for reporting, documenting and investigating work-related incidents and developing and implementing corrective actions that reduce the likelihood of recurrence. We maintain a 24-hour hotline and an online portal to facilitate prompt and compliant incident reporting.

Verizon's EHS department maintains International Organization for Standardization (ISO) 14001 (environmental) and ISO 45001 (occupational health and safety) certifications for our EHS management system. Certification shows that our processes meet international best practices, drive continual improvement and create business value.

Responsibly managing natural resources

Water conservation

We implement water conservation measures throughout our operations. Most of our water withdrawal comes from municipal sources and the large majority of our water withdrawal occurs outside of areas of high water risk.[2] We do not withdraw any groundwater and do not currently store any water as a part of our operations.

Verizon consumes the most water at our technical facilities, which require a controlled, cool environment for network equipment. We manage water consumption in these facilities through regular maintenance and upgrades to cooling towers and other water-cooled systems. Where possible, we are also replacing traditional water-cooled equipment, which relies on municipal water supplies, with efficient closed-loop and refrigerant-based systems. We continually monitor our water withdrawal for fluctuations that help us to identify potential leaks.

Our ongoing implementation of energy efficiency measures in our technical buildings also helps to reduce water consumption. We are further conserving water as we consolidate leased and owned buildings and adjust our HVAC systems in our administrative offices to reflect our adoption of a hybrid work environment. We reduced our water withdrawal by 7% from 2019 to 2024.

External assurance. We obtain independent limited assurance of our annual water withdrawal results at our administrative offices, retail stores, data centers, central offices, equipment, garage work centers, warehouses and motor vehicle maintenance centers. Sites that do not routinely use water (e.g., network cabinets and huts, microwave equipment, towers and antennas) are excluded from the results. For details, including our full calculation methodology, read the **Independent Accountants' Review Report**.

Paper policy

Verizon is committed to the sustainable sourcing and use of paper. At least 50% of the paper we source annually will include at least 10% recovered fiber content and/or at least 10% post-consumer waste (PCW) content. This excludes billing segments that are not able to be printed on recycled content paper because of machinery issues. See our **Paper Sourcing and Use Policy** for more information.

Nature

To better understand Verizon's nature-related impacts and dependencies, we conducted a pilot LEAP assessment in 2024 in line with the recommendations of the Task Force on Nature-related Financial Disclosures.

Responsibly managing waste

Our EHS and Circular Supply Chain teams work internally across the company and externally with partners and suppliers to reduce, reuse and responsibly recycle materials. We recycled or reused over 92 million pounds of materials, including e-waste, in 2024.

E-waste: reducing, reusing and recycling

Verizon defines electronic waste, or e-waste, as electronic products and component parts that are at the end of their useful life and/or have been returned by customers. E-waste generated by our business operations includes cell phones, chargers, set-top boxes, network equipment, batteries and associated plastic components. In 2024, Verizon reused or recycled over 49 million pounds of e-waste, including 1.4 million pounds of plastic and 2.2 million pounds of lead-acid batteries.

We strive to divert as much e-waste as possible from landfills by reusing or responsibly recycling materials. To the extent practicable, we reuse electronic products and parts internally. When internal reuse is not possible, we market these materials for reuse through approved partners or work with suppliers to responsibly recycle them. Verizon's Circular Supply Chain team partners with Corporate Sourcing to incorporate terms into our supplier contracts for the responsible end-of-life management of our products.

Many of Verizon's recycling practices exceed regulatory mandates. We engage e-waste suppliers that manage our waste in accordance with high industry standards for environmental stewardship such as R2 and e-Stewards. Our practice is to require lead-acid batteries from our U.S. operations to be sent to Verizon-approved recycling facilities in the U.S. or Canada and to require our suppliers to provide certificates of recycling for the batteries. We regularly audit facilities, including battery smelters, that manage Verizon's hazardous or regulated waste.

Community recycling rallies. To enable our communities to safely recycle e-waste, Verizon sponsors free recycling events open to our employees and the public. We aim to collect and recycle 10 million pounds of e-waste from our communities by 2026. Since 2009, we have collected over 9.2 million pounds of community e-waste for recycling.

Operational and sourcing circularity

We are committed to reducing waste and resource use by reusing, repairing and recycling the materials and products in the goods we offer.

Device trade-in. Verizon's **device trade-in program** supports our circular economy approach to extending the lifespan of mobile devices and accessories. We strive to reuse, resell or recycle all mobile phones – from any brand or carrier, in any condition – that are returned to Verizon. Our processes are designed to keep the mobile phones and related accessories received through our product take-back program out of landfills. The program enables both Verizon and non-Verizon consumers to return qualifying, pre-owned devices in exchange for a Verizon credit or gift card. We repair, repurpose and resell these devices before pursuing responsible recycling at the end of their useful life. We refurbish and redistribute our home internet devices for 4G and 5G fixed wireless access and Fios service to customers. Consumers can also return obsolete devices for responsible recycling.

Teardown lab. Verizon maintains a teardown lab in which a team of engineers and cost modeling experts systematically deconstructs network equipment and devices to assess the efficacy and efficiency of their design. The lab's core objective is to offer insights on design optimization to enhance product sustainability from production to disposal.

Plastic reuse. Teams across the company work to develop new uses for the plastic harvested from old Verizon products. For example, plastic from routers and set-top boxes has been given new life as road signs, park benches and office chairs.

Supplier expectations. Our Supplier Code of Conduct includes key waste-related provisions, including the expectation that suppliers strive to reduce, eliminate or prevent waste of all types by conserving materials and modifying their production or maintenance or facility processes. Suppliers are also expected to reduce the volume and toxicity of products throughout their lifecycle. We have modified our supply chain requirements for all customer-premise products to state that product packaging should be designed to eliminate or minimize the use of single-use plastics and non-recyclable materials and that products should be designed to use post-consumer recycled content to the greatest extent possible.

Reducing plastic and other waste

We are working to reduce the environmental impact of plastics in our products and product packaging, as well as in our day-to-day business operations. Our reduction efforts include:

- Incorporating PCW, recycled plastic resin and ocean-bound plastics in customer-premise equipment, such as routers, set-top boxes and remote controls
- Eliminating single-use plastic packaging from our reverse logistics operations (i.e., product take-back). Products impacted by this change include home routers, optical network terminals and set-top boxes
- Using responsibly sourced packaging materials for Verizon-branded screen protectors
- Eliminating single-use plastics from our cafeteria and kitchen facilities at our corporate headquarters

Verizon’s emissions profile

While Verizon has voluntarily disclosed the GHG emissions associated with our operational energy consumption (scopes 1 and 2) since 2004, 2019 was the first year for which we reported our full value chain (scope 3) emissions.

Scope 1

All direct sources of emissions owned or controlled by Verizon, with the main categories being fuel to power our fleet, heat our buildings and power our backup generators.

Scope 2

Indirect emissions from energy purchased by Verizon. The largest category is electricity to power our networks and data centers, with a small amount of steam and heat purchased to heat our buildings.

Scope 3

Indirect emissions associated with Verizon’s upstream and downstream value chain. The largest categories are those related to purchased goods and services, capital goods, fuel- and energy-related activities (not included in scopes 1 or 2) and use of sold products.

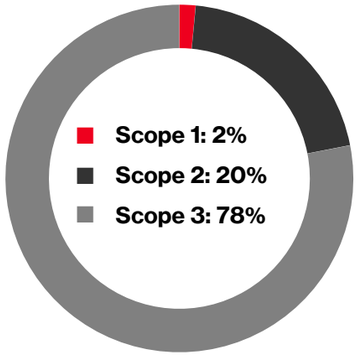
External assurance

We obtain independent limited assurance of our scopes 1, 2 and 3 GHG emissions annually. See the **Independent Accountants’ Review Reports** for more information.

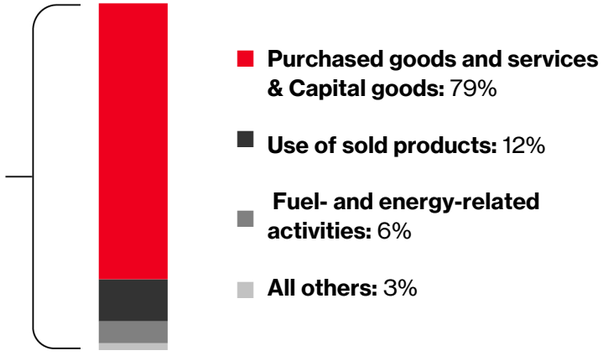
2024 GHG emissions breakdown[3]

GHG emissions Metric tons (MT) CO_2e	2019[4]	2023[4]	2024[4]	% Reduction 2019 vs. 2024
Scope 1	358,753	269,333	265,859	26%
Scope 2 (location-based)	4,006,874	3,511,076	3,596,917	10%
Scope 2 (market-based)	4,006,874	2,195,515	1,458,535	64%
Total scopes 1 & 2 (location-based)	4,365,627	3,780,409	3,862,776	12%
Total scopes 1 & 2 (market-based)	4,365,627	2,464,848	1,724,394	61%
Scope 3	18,979,748	15,124,184	13,743,238	28%

Total emissions (location-based)



Total scope 3 emissions



SASB Standards index

Activity metrics

SASB code	Metric	2022	2023	2024
TC-TL-000.A	**Number of wireless retail connections**	143,253,000	144,751,000	146,075,000
	Wireless retail connections are retail customer device postpaid and prepaid connections as of the end of the period. Retail connections under an account may include those from smartphones and basic phones (collectively, phones), postpaid and prepaid fixed-wireless access (FWA), as well as tablets and other internet devices, wearables and retail IoT devices.			
TC-TL-000.C	**Number of broadband connections**	8,936,000	10,717,000	12,327,000
	Total broadband connections are the total number of connections to the internet using Fios internet services, Digital Subscriber Line and postpaid, prepaid and IoT FWA as of the end of the period.			
TC-TL-000.D	**Network traffic in petabytes**[4]	134,202	156,385	215,799

Accounting metrics

Environmental footprint of operations

SASB code	Metric	2022	2023	2024
TC-TL-130a.1 T	**Total energy consumed in gigajoules (Gj)**[4]	41,167,721	39,759,403	41,487,063
	Percentage grid electricity[4]	88.9%	88.7%	89.5%
	Percentage renewable energy[4]	11.3%	30.6%	49.8%
	Total energy consumed is calculated based on emissions sources included in scopes 1 and 2 GHG emissions, namely natural gas, gasoline, diesel, jet fuel, propane, kerosene, compressed natural gas, B02, B05, B11, B20, E85, methanol, ethanol, electricity, steam and chilled water. **Percentage grid electricity** is calculated as total electricity consumed as purchased from the grid (and reported for scope 2 GHG emissions) divided by total energy consumed. **Percentage renewable energy** is calculated as total renewable electricity generated on-site or purchased in the form of energy attribute certificates divided by total energy consumed. For information on our emissions profile and progress towards our emissions reduction and renewable energy sourcing targets, see our Emissions Reporting **website**.			

Data privacy

SASB code	Metric	2022	2023	2024
TC-TL-220a.1	**Description of policies and practices relating to targeted advertising and customer privacy**			
	See **Data privacy** for a discussion of Verizon's corporate policies and operating procedures governing how we collect, use, retain and protect data.			
TC-TL-220a.2	**Percentage of customers whose information is used for secondary purposes**	100	100	100
	The reported metric is 100% because, as described in the Verizon Privacy Policy, Verizon uses customer data to improve our products and services, which is one of the ways that the SASB Standard defines "secondary purposes" for purposes of this metric.			
TC-TL-220a.3	**Total amount of significant monetary losses as a result of legal proceedings associated with privacy**	Not significant	Not significant	Not significant
	For purposes of reporting this metric, we have established a significance threshold that is lower than the materiality threshold for reporting legal proceedings in our SEC reports and will report any loss of $100 million or more, individually or in the aggregate.			
TC-TL-220a.4	**Number of U.S. law enforcement requests for customer information; number of customer selectors whose information was requested; percentage resulting in disclosure**			
	Verizon issues semiannual Transparency Reports that present the number of demands received from law enforcement in the U.S. and other countries where we did business during the reporting period. See our latest **Transparency Reports** for more information.			

Data security

SASB code	Metric	2022	2023	2024
TC-TL-230a.1	**Number of data breaches** **Percentage that are personal data breaches** **Number of customers affected**	Not available	Not available	Not available
	Except as required by law, Verizon does not report this information.			
TC-TL-230a.2	**Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards**			
	For information about our approach to managing data security risks, see **Cybersecurity**.			

Product end-of-life management

SASB code	Metric	2022	2023	2024
TC-TL-440a.1	**Materials recovered through take-back programs in pounds**	43,428,528	46,970,629	49,091,924
	Verizon defines e-waste as electronic products and component parts that are at the end of their useful life and/or have been returned by customers. E-waste generated by our business operations includes cell phones, chargers, set-top boxes, network equipment, batteries and associated plastic components. For more information on our e-waste recycling and device trade-in programs, see **E-waste: reducing, reusing and recycling**.			

Competitive behavior and open internet

SASB code	Metric	2022	2023	2024
TC-TL-520a.1	**Total amount of significant monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations**	Not significant	Not significant	Not significant
	For purposes of reporting this metric, we have established a significance threshold that is lower than the materiality threshold for reporting legal proceedings in our SEC reports and will report any loss of $100 million or more, individually or in the aggregate. For information on Verizon's global antitrust program, see **Antitrust compliance**.			
TC-TL-520a.2	**Average actual sustained download speed in Megabits per second (Mbps) of (a) owned and commercially-associated content and (b) non-associated content**	Not available	Not available	Not available
	Verizon does not measure download speeds on the bases specified in the standard (i.e., owned and commercially associated content versus non-associated content). We are committed to an **open internet** and have been at the forefront of innovation in the broadband ecosystem, advocating consistent policies aimed at creating a robust, level and dynamic playing field for all participants in the internet environment. For information on the expected and actual performance of our networks and our network management practices, see **Network performance**.			
TC-TL-520a.3	Description of risks and opportunities associated with net neutrality, paid peering, zero rating and related practices			
	See Verizon's SEC reports for our disclosures relating to the risks and opportunities associated with laws and regulations addressing net neutrality. Verizon's **Interconnection Policy for Internet Networks** establishes separate requirements for each of our three regional internet networks, with the requirements scaled for each network.			

Managing systemic risks from technology disruptions

SASB code	Metric	2022	2023	2024
TC-TL-550a.1	**System average interruption duration, system average interruption frequency and customer average interruption duration**	Not available	Not available	Not available
	Verizon does not currently calculate and report metrics relating to the frequency and duration of system disruptions in the manner specified in the standard.			
TC-TL-550a.2	**Discussion of systems to provide unimpeded service during service interruptions**			
	Verizon is an industry leader in operating resilient and reliable networks that support the needs of our customers. Our networks in the U.S. include various design elements, technologies and business processes that work together to enhance the reliability of our services. **Designed with dual path and equipment redundancy.** Verizon's network design includes redundancy on critical paths and for critical network components to mitigate the impact of network events on customers. We use forward-looking risk assessments to plan and maintain our fiber backhaul configuration for critical network sites. Such sites may contain traffic aggregation points, data centers or other technical facilities and typically have fiber backhaul deployed in a resilient ring or hub configuration, as well as dual diverse entrance facilities supporting our core infrastructure. Verizon has also implemented a "meshed" core network architecture, which enables network equipment to switch traffic almost instantly across multiple available transmission paths between two endpoints. When available, this enables the network to self-recover promptly from outages to physical facilities (e.g., a fiber cut). **Use of battery and generator technology.** To minimize the impact of power disruptions at critical sites, we deploy reserve power in the form of batteries and/or generators. Our switching facilities are equipped with battery backup power and generators. Macro sites have battery backup power as well, and the majority are equipped with generators. In addition, we have a fleet of portable backup generators that can be deployed as needed. **Reliability-focused business processes.** To minimize the likelihood of congestion on our networks, Verizon proactively manages and augments network capacity based on defined thresholds associated with the expected voice, video, application and data traffic patterns across our network. To help ensure appropriate network diversity and redundancy, we perform several internal audits per year. Our engineering standards for strategic directional platforms require high availability equipment with auto-failover capabilities to protect critical services. Requirements for diversity and redundancy for critical paths and network sites are reviewed and addressed as part of network planning, engineering and operations activity. **Overlapping spectrum and coverage areas.** Verizon designs its wireless network to provide for overlapping spectrum and coverage areas in many cases. If a particular cell site goes offline, devices may switch to a different site and maintain connectivity. Different spectrum bands deployed on our 4G and 5G networks can provide customers with additional options for connectivity and capacity if certain bands or nodes experience an increase in usage. Most customer devices have the option to move seamlessly between our 4G and 5G networks and available Wi-Fi networks to provide our customers with a high degree of reliability. For more information on how we manage business continuity risk and the measures we have undertaken to make our networks more resilient, see **Network resilience** and our **latest TCFD Report**.			

Endnotes

1	Verizon was not required to file a Conflict Minerals Report in 2024 for the period from January 1, 2023, to December 31, 2023, because we did not manufacture or contract to manufacture products subject to reporting.
2	Based on the World Resources Institute's Aqueduct data set.
3	In 2023, Verizon made adjustments in the calculation of the 2019 scope 3 baseline to reflect the following subsequent developments: a) the acquisition of TracFone Wireless, Inc. in November 2021, b) the application of the environmentally extended input-output (EEIO) emissions factors developed by The Carbon Trust to relevant categories and c) the calculation of well-to-tank emissions to relevant categories in alignment with the 2023 calculation methodology. These updates resulted in an increase of ~12% in the scope 3 base-year emissions from 16,954,198 MT CO_2e to 18,979,748 MT CO_2e. The impact of the acquisition of TracFone Wireless, Inc. on Verizon's base-year scopes 1 and 2 emissions was determined to be de minimis and therefore the 2019 scopes 1 and 2 base year values have not been updated. Reported 2021 and 2022 results exclude TracFone results. We further note that, in accordance with the accounting methodology described in the relevant **Independent Accountants' Review Reports**, market-based scope 2 emissions account for our use of energy attribute certificates, the majority of which were obtained through REPAs. In certain instances, we swapped RECs generated by the REPA projects (project RECs) for an equal number of other RECs (non-project RECs) or accepted non-project RECs in lieu of project RECs pursuant to the REPAs.
4	This data has been independently assured. See the **Independent Accountants' Review Reports** for more information.