



2025 SASB Index

The table below references the SASB Standard for the Telecommunications industry, as defined by SASB’s Sustainable Industry Classification System.

Topic	SASB code	Requested metric	2025 response
Environmental footprint of operations	TC-TL-130a.1	(1) Total energy consumed	27,990,710 GJ Total energy consumed is calculated based on emissions sources included in Scope 1 and 2 GHG emissions. For a full list of fuel sources, please see GRI 302-1. For more information, please refer to our Independent Assurance Statement on our Corporate Responsibility Reporting Hub.
	TC-TL-130a.1	(2) Percentage grid electricity	97.2% 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.
	TC-TL-130a.1	(3) Percentage renewable	97.2% Percentage renewable electricity is calculated as total renewable electricity generated on-site or purchased in the form of renewable energy credits divided by total energy consumed.

SASB content index

Topic	SASB code	Requested metric	2025 response
Data privacy	TC-TL-220a.1	Description of policies and practices relating to targeted advertising and customer privacy	The T-Mobile Privacy Center houses our Privacy Notices describing our privacy practices for consumers, education articles, and our Privacy Dashboard where consumers can exercise privacy choices. Consumers can find the choices they have over the use of their personal data and descriptions of the data we collect, how it is used, when it is shared, how we retain and protect it, and other privacy safeguards. The T-Mobile Privacy Center gives consumers easy access to information concerning targeted advertising and their choices. This includes the choices consumers have over the use of their personal data for relevant advertising and data analytics and reporting. Please see the T-Mobile Privacy Notice for how the company collects, uses, shares, retains, and protects personal data. T-Mobile has policies and practices in place for data handling and to govern the data lifecycle, including the use of Privacy by Design principles and processes to evaluate new collection, uses, and disclosure of personal data using Privacy Impact Assessments. T-Mobile further has policies and practices in place to maintain the security of data through review by its Cybersecurity team. T-Mobile also conducts an extensive data inventory of its systems. T-Mobile doesn't knowingly collect data from or about children under the age of 18 without the permission of their parent or guardian. When we do collect that data, we might do it directly, as when signing up for a service. We might also collect data automatically if a child uses the products or services we offer. Please see our Children's Privacy Notice for more information.
	TC-TL-220a.2	Number of customers whose information is used for secondary purposes	The number of customers whose information is used for secondary purposes varies by product, and is dynamic over time, as consumers may opt out of many of these uses. In our Privacy Notice , we publicly disclose information on how we use personal data and the choices we offer with respect to those uses. We publish the number of requests we have received to opt-out of certain data uses and the number of requests we have received from customers to access or delete their personal data for the prior year.
	TC-TL-220a.3	Total amount of monetary losses as a result of legal proceedings associated with customer privacy	For purposes of reporting this metric, we'll report on regulatory fines or legal settlements for matters that have a material impact on our operations, or which we'd otherwise disclose to investors pursuant to SEC guidance. For the 2025 fiscal year ending on December 31, 2025, we did not have any material monetary loss as the result of litigation or regulatory investigations concerning our processing of consumer data that was not previously disclosed to investors pursuant to the SEC guidance.
	TC-TL-220a.4	(1) Number of law enforcement requests for customer information	T-Mobile discloses the number of law enforcement requests for customer information and the number of requests that were rejected, received no response, or received a written explanation of why T-Mobile was unable to respond in whole or in part. For the latest annual figures, please visit our Corporate Responsibility Reporting Hub to view the most current annual Transparency Report. The 2025 Transparency Report is scheduled to be published in the summer of 2026. T-Mobile releases customer records to law enforcement personnel only when legally compelled to do so. The Legal and Emergency Response team relies on a variety of Federal and State statutes and regulations when determining appropriate compliance. The Legal and Emergency Response Specialists are trained to analyze legal demands and make a determination regarding appropriate compliance.
	TC-TL-220a.4	(2) number of customers whose information was requested	T-Mobile does not measure the number of individual customers; as noted above we track government requests, which may cover more than one customer.
	TC-TL-220a.4	(3) percentage resulting in disclosure	T-Mobile discloses the number of law enforcement requests for customer information and the number of requests that were rejected, received no response, or received a written explanation of why T-Mobile was unable to respond in whole or in part. For the latest annual figures, please visit our Corporate Responsibility Reporting Hub to view the most current annual Transparency Report. The 2025 Transparency Report is scheduled to be published in the summer of 2026.

SASB content index

Topic	SASB code	Requested metric	2025 response
Data security	TC-TL-230a.1	(1) Number of data breaches	T-Mobile does not report these figures publicly, in part as the definition of “data breach” varies across laws and contract terms. We do provide public notice for those incidents where such notice is required by law. In unusual cases, we may provide additional information about an incident and our response.
	TC-TL-230a.1	(2) percentage that are personal data breaches	
	TC-TL-230a.1	3) number of customers affected	
	TC-TL-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	T-Mobile maintains a comprehensive cybersecurity program that aligns with leading industry frameworks and regulatory standards, including National Institute of Standards and Technology (NIST) 800-53, International Organization for Standardization (ISO) 27001, Payment Card Industry Data Security Standard (PCI DSS), and Cybersecurity Maturity Model Certification (CMMC). Vulnerability management is supported by nightly perimeter scans, bug bounty intake, and telemetry from cloud and containerized environments. Vulnerabilities are prioritized and remediated according to risk-based service level agreements (SLAs), with critical issues addressed within 15 days and exceptions managed through formal risk acceptance processes. All risks are tracked and regularly reviewed by Cyber Risk Management. T-Mobile’s Threat Intelligence team leverages the MITRE ATT&CK framework to monitor global adversary behavior. Threat trends including phishing, credential abuse, third-party software exploitation, and the growing use of AI-generated content and zero-day vulnerabilities. Third-party risk is managed through the Third-Party Risk Management (TPRM) program and the Unified Controls Program (UCP), with compliance enforced through vendor assessments, required attestations, and certifications aligned to NIST and ISO standards.
Product end-of-life management	TC-TL-440a.1	(1) Materials recovered through take back programs	T-Mobile is committed to responsibly disposing of customer devices and extending their product life. Through our Device Reuse and Recycling program, customers can trade in an eligible device for a credit toward a new one or they can bring in unused devices to our retail collection sites. T-Mobile Home Internet routers are also returned through this program and refurbished or recycled. Devices currently included in this program include phones, smartwatches, tablets, hotspots, routers, and IoT items. Our Device Reuse and Recycling program complies with federal and state laws and gives consumers a way to properly and safely recycle these items. T-Mobile requires suppliers and partners that repair and recycle these devices to be certified to the industry leading R2 standard, which provides a common set of processes, safety measures and documentation requirements. R2 is rigorously and independently audited, emphasizing quality, safety, and transparency, including any devices exported for refurbishment and recycling.
	TC-TL-440a.1	Percentage of recovered materials that were (2) reused	In 2025, we processed approximately 12.9 million devices through our Device Reuse and Recycling program. Approximately 77% were reused or resold to approved vendors for reuse, approximately 1% was responsibly recycled by certified third-party facilities, and approximately 22% remained in inventory as of 12/31/25 and are intended to be reused or recycled in 2026.
	TC-TL-440a.1	Percentage of recovered materials that were (3) recycled	
	TC-TL-440a.1	Percentage of recovered materials that were (4) landfilled	
Competitive behavior & open internet	TC-TL-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations	For the fiscal year 2025, T-Mobile had no material losses related to litigation or to non-appealable regulatory decisions involving anti-competitive behavior.



SASB content index

TC-TL-520a.2	Average actual sustained download speed of (1) owned and commercially-associated content and (2) non- associated content	T-Mobile believes everyone should have access to all the internet has to offer. T-Mobile's broadband internet access services do not directly or indirectly favor some traffic over other traffic either in exchange for consideration from a third party or to benefit an affiliated entity. For information on T-Mobile network performance characteristics (including download speeds), customer options, and network management practices, see our Open Internet page .
TC-TL-520a.3	Description of risks and opportunities associated with net neutrality, paid peering, zero rating, and related practices	Please see T-Mobile's SEC reports for our disclosures relating to the risks and opportunities associated with laws and regulations addressing net neutrality. Information regarding network practices for T-Mobile's broadband internet access services is also available on our Open Internet page .



SASB content index

Topic	SASB code	Requested metric	2025 response
Managing systematic risks from technology disruptions	TC-TL-550a.1	(1) System average interruption duration	T-Mobile does not currently disclose the system average interruption duration.
	TC-TL-550a.1	(2) System average interruption frequency	T-Mobile does not currently disclose the system average interruption frequency.
	TC-TL-550a.1	(3) Customer average interruption duration	T-Mobile does not currently disclose the customer average interruption duration.
	TC-TL-550a.2	Discussion of systems to provide unimpeded service during service interruptions	At T-Mobile, we recognize that reliable communications and connectivity are essential during critical events, including natural disasters, emergencies, and other disruptive incidents. Building operational and network resilience remains foundational to how we serve our customers and support the communities in which we operate. We are committed to safeguarding the interests of our customers, employees, and stakeholders by preparing for, responding to, and recovering from potential business disruptions. T-Mobile maintains an enterprise-wide Business Continuity Program designed to proactively reduce risk to operations and minimize impacts to customers and services. Enterprise teams across Business Continuity, Disaster Recovery, Network Availability, Emergency Management, and Customer Support work in a coordinated manner to strengthen preparedness and response capabilities. Dedicated, certified Business Continuity professionals partner with all lines of business to help ensure that all-hazards plans, processes, and protocols remain current, comprehensive, and effective. Crisis and incident management teams are established, trained, and exercised regularly to support timely decision-making, coordinated response actions, and effective execution of continuity strategies during incidents. These efforts are supported by active executive sponsorship, governance, and oversight, reinforcing accountability and continuous improvement across the organization.
Number of wireless subscribers	TC-TL-000.A	Quantitative	T-Mobile reported 142,388,000 wireless customers at the end of 2025. Wireless Subscribers: A customer is generally defined as a SIM number with a unique T-Mobile identifier, which is associated with an account that generates revenue. We provide wireless communications services to a variety of customers needing connectivity, but focus primarily on two categories of customers: • Postpaid customers generally are qualified to pay after receiving wireless communications services utilizing phones, High Speed Internet modems, mobile internet devices (including tablets and hotspots), wearables, DIGITS and other connected devices (including SyncUP and Internet of Things). We serve consumers as well as business customers, who are provided with services under the T-Mobile for Business brand. • Prepaid customers generally pay for wireless communications services in advance. We serve prepaid customers under the T-Mobile, Metro by T-Mobile, Mint Mobile and Ultra Mobile brands.
Number of wireline subscribers	TC-TL-000.B	Quantitative	T-Mobile does not have customers who contract with us for fixed line phone services as outlined by the standard.
Number of broadband subscribers	TC-TL-000.C	Quantitative	T-Mobile reported 9,447,000 total broadband customers, including 5G broadband and fiber customers at the end of 2025.
Network traffic	TC-TL-000.D	Quantitative	T-Mobile does not currently report this information.