

2021 Sustainability Accounting Standards Board Index

This is LiveVox's first year of reporting using the [Sustainability Accounting Standards Board \(SASB\) Standards for the Software & IT Services industry](#). The table below discloses information and data for the reporting period January 1, 2021, to December 31, 2021.

Topic	SASB Code	Metric	2021 Response
Environmental Footprint of Hardware Infrastructure	TC-SI-130a.1	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	<p>(1) 11,224 gigajoules, (2) 100% grid electricity, (3) 12% renewable.¹</p> <p>¹ Our San Francisco headquarters is a CleanPowerSF customer. Percentage of energy from renewable sources is determined using the difference between California's power mix and CleanPowerSF's "Green" power mix.</p> <p>We have 670 global employees and are headquartered in San Francisco, with offices in Atlanta metro; Columbus; Denver; St. Louis metro; Medellin, Colombia; and Bangalore, India. In 2021, a majority of our employees worked remotely from home.</p> <p>Our San Francisco office building is LEED (Leadership in Energy and Environmental Design) Platinum certified, and our Medellin and Atlanta office locations are LEED Gold certified. Verified by the Green Business Certification Inc., LEED-certified buildings save money, improve efficiency, lower carbon emissions, and create healthier places for people. They are a critical part of addressing climate change, enhancing resilience, and supporting more equitable communities.</p>
	TC-SI-130a.2	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	(1) 129,000 m ³ , 0.6% from regions with High or Extremely High Baseline Water Stress. (2) Based on our total annual water use, total water consumed is not a material issue.
	TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	<p>We do not own or operate any data centers. In 2021, we leased space from a private colocation center in New York City. By year-end, we had fully transitioned to a virtual public cloud environment with a presence in geo-diverse regional environments across North America via Amazon Web Services (AWS). We expect to maintain our lease in New York City through Q1 2022 as we decommission that site.</p> <p>Through their scale, AWS data centers can achieve higher resource utilization and energy efficiency than is possible for the typical on-premises data center. In addition, AWS has multiple initiatives underway to use water more efficiently and use less potable (drinking) water to cool its data centers. AWS assesses both</p>

			<p>the water use and the energy use of each potential cooling solution to select the most efficient method.</p> <p>From an architecture perspective, we focus on running our platforms as leanly as possible, using component rightsizing, containerization, and auto-scaling, which helps us reduce our electricity consumption.</p> <p>The Nominating and Corporate Governance Committee of our Board of Directors, in conjunction with our Environmental, Social, and Governance (ESG) Subcommittee, oversees the company’s ESG strategy, policies, and practices in order to manage risk, lay a foundation for sustainable growth, and effectively communicate ESG initiatives to stakeholders. This committee must periodically review and evaluate emergent ESG-related trends and issues in connection with the company’s business activities and make recommendations to the Board regarding those trends and issues.</p>
<p>Data Privacy & Freedom of Expression</p>	<p>TC-SI-220a.1</p>	<p>Description of policies and practices relating to behavioral advertising and user privacy</p>	<p>Website User Privacy</p> <p>We are committed to ensuring that user privacy is protected. We may collect certain information from users who visit our websites. This information falls into two categories: (1) personal information that users voluntarily supply when filling out forms on our websites, as well as partner sites, and (2) tracking information collected as users navigate our sites.</p> <p>Our Web Privacy Policy governs how LiveVox uses and protects any data collected through our websites. To that end, we will not collect, use, or disclose personal information other than in compliance with this policy. Our Web Privacy Policy only applies to personal information obtained by LiveVox and not information collected from user interactions with third parties.</p> <p>We do not sell user personal information to third parties. We will share user personal information with third parties only in the ways that are described in our Web Privacy Policy. We may use third-party service providers for demand generation and sales support, along with career, network, security, email, and hosting services. Suppliers, partners, and service providers are required by contract to keep confidential the information received on our behalf and may not use it for any purpose other than to carry out the services they are performing for us.</p>

			<p>Customer Data</p> <p>Our customers determine what data elements and volume they bring into the LiveVox platform in order to run their campaigns, and they retain ownership of this data while in LiveVox custody. LiveVox does not use it for any purpose other than to fulfill its obligations under the agreement it has with each customer. LiveVox does not disclose this customer data to any third parties without the customer's written consent.</p> <p>As part of standard and customary service delivery, LiveVox collects and stores certain information provided by customers. Customers have discretion as to the nature of the information provided and its use in their campaigns. LiveVox deploys the customer-provided information to launch calling campaigns and to enable customers to access the results of such campaigns. LiveVox also, as a matter of course, stores its customers' call recordings on a rolling basis for the prior 15 days of calls; a longer storage period is available upon request. LiveVox records agent calls beginning when a call is bridged to an agent until the call ends. Automated messages are not recorded.</p> <p>Customer data pertaining to the LiveVox platform and the customers' use of the platform is stored only within designated storage systems and file systems within the platform.</p> <p>Data Retention & Disposal</p> <p>We have developed and implemented a comprehensive Data Retention and Disposal Policy and program. Policy directives are fully enforced to ensure that the Data Retention and Disposal Policy is executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other resources deemed critical by the organization.</p> <p>Our Data Retention and Disposal Policy governs the data storage period for customer-provided information. Data is retained in accordance with prevailing standards and industry best practices (e.g., PCI DSS, HIPAA, and FISMA), as well as in accordance with customer-specified retention schedules on record.</p>
--	--	--	--

		<p>Once the maximum retention period has been reached for specified data, the data is removed. The purge process executes by automated processes and schedules to perform rolling deletions of content as its defined retention periods lapse. Methods for disposal include OS filesystem deletion and cryptographic erase (deletion of encryption keys) as per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88: Guidelines for Media Sanitization.</p> <p>Where applicable, when production hardware has reached the end of useful life, data is deleted and storage media is sanitized following NIST guidelines, such as SP 800-88. We deploy a variety of methods, including a secure wipe program in accordance with industry-accepted standards for secure deletion and/or an authorized physical destruction method of storage media by the third party ensuring documented chain of custody.</p> <p>Only authorized personnel may administrate data retention periods. These activities are considered highly sensitive in nature, and they must be precipitated by a compelling business or operational requirement.</p>
TC-SI-220a.2	Number of users whose information is used for secondary purposes	We had no users whose information was used for secondary purposes.
TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	We had no monetary losses as a result of legal proceedings associated with user privacy.
TC-SI-220a.4	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	<p>We received a total of 55 subpoenas from law enforcement in 2021 for information relating to customer phone numbers. We responded to 100% of these law enforcement requests.</p> <p>Under certain circumstances, personal information may be subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders, or when we believe in good faith that disclosure is necessary to protect our rights, protect user safety or the safety of others, investigate fraud, or respond to a government request or to any other third party with user prior consent to do so. If we are ever legally compelled to disclose user personal information to a third party, we will notify the user with the contact information we have unless doing so would violate the law or a court order. Additional information can be found in our Web Privacy Policy.</p>

	TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	There are no countries where our core products or services are subject to government-required monitoring, blocking, content filtering, or censoring.
Data Security	TC-SI-230a.1	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	(1) We are not aware of any data breaches, (2) n/a, (3) n/a.
	TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	<p>We take the security of our data and each client’s information seriously. We have implemented reasonable precautions to protect against unauthorized access to our systems and to prevent data from being disclosed to unauthorized parties. We follow generally accepted standards to protect the personal information submitted to us, both during transmission and once we receive it. In addition, in accordance with PCI DSS requirements, LiveVox has established a formal policy and supporting procedures regarding cardholder data retention and disposal.</p> <p>Our approach to security is embedded across every aspect of our organization. From our dedicated security team and continuous process improvements to ongoing technology developments and certifications, protecting customer data and operations is core to our business.</p> <p>We utilize strict controls over customer data across every facet of our platform and organization. This includes:</p> <ul style="list-style-type: none"> • Network security • Application security • Data security • System security • Physical security • Code review and software development life cycle <p>We employ an experienced team of cloud security experts who continue to improve our security posture. They handle a variety of factors impacting cloud security, including:</p> <ul style="list-style-type: none"> • Encryption • Identity and access management

- Firewalls
- Cloud server management
- Security policy standardization and adherence
- Business and disaster recovery plans
- User and employee education
- Client audit fulfillment

We maintain compliance with industry standards and best practices and conduct ongoing assessments to continually upgrade our security infrastructure and posture. Some of the standards with which we comply are defined by the industry itself, government, and various regulations. Others are derived from ongoing audits on the part of our customer base, which represents a broad range of industries with concerns in areas as varied as payment, finance, federal, healthcare, and other sensitive data areas. Additionally, some standards have available certifications, while others are based more on having certain policies, procedures, or safeguards in place, albeit without a formal certification process.

Our comprehensive security policies and procedures are designed to support compliance with a variety of data protection standards, laws, and regulations and are also reviewed by third-party auditors. Examples of such standards include:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- American Institute of CPAs (AICPA) System and Organization Controls for Service Organizations (SOC 2)

In addition, these policies and processes provide alignment, where applicable, with the NIST Special Publication (SP) 800 series in general, with SP 800-53 r4 as the primary compliance guide.

For example, we encrypt all customer data rather than encrypting only specific data elements, leveraging AES (Advanced Encryption Standard) and 256-bit encryption where applicable. We maintain current versions of Transport Layer Security (TLS) following PCI DSS and NIST SP 800-53 r4 requirements. We invest heavily in securing data across the numerous points of a call transaction, employing multiple approaches to encryption both at rest and in transit.

			<p>We review our security policies and procedures once annually (at minimum) and whenever changes in the threat environment take place or are communicated to LiveVox, and we revise them accordingly. Reviews are conducted by security operations personnel and directors and stem from coordination with various organizational entities. The Information Security and Compliance Committee approves revisions, with the inclusion of Legal Counsel and the Senior Vice President of Technical Operations, and represents the organization’s commitment to these controls, processes, and standards. In addition, the Cybersecurity Committee of our Board of Directors provides oversight of the company’s policies, plans, and programs relating to cybersecurity and data protection risks associated with our products, services, and business operations. The committee meets quarterly and provides regular reports to the Board about its activities and decisions.</p> <p>Compliance with our security policies and processes is mandatory for all LiveVox personnel. Employees and contractors must be well informed of their responsibilities as information owners, managers, users, and service providers. All employees are required to:</p> <ul style="list-style-type: none"> • Read and acknowledge understanding of – at hire and periodically thereafter – the policies contained in our Employee Security and Compliance Handbook. • Complete the company’s training program as required throughout the year. Department-specific and role-specific training via on-the-job training, formal instruction, or computer-based training may be required in addition to what is required companywide. Additional training and materials may be offered to instill the importance of appropriate information handling and to explain the implications of this policy. <p>Violations are subject to disciplinary action by company management up to and including termination of employment.</p>
Recruiting & Managing a Global, Diverse &	TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and (2) located offshore	(1) 3% of employees in the U.S. and 3% of employees in Colombia are foreign nationals. (2) 36.8% of employees are located offshore (outside of the U.S.) – 16% in Colombia and 20.8% in India.

Skilled Workforce			<p>Creating tomorrow’s technology requires the ability to leverage cutting-edge software tools, a global workforce, freedom to explore, and support to succeed. LiveVox innovators across India, Colombia, and the U.S. are empowered with a team structure that drives individual leadership and leverages the latest software capabilities.</p> <p>Our talent recruitment and hiring efforts are targeted at developing and retaining highly capable teams in each of our global office locations. Any potential risks from recruiting a global workforce are addressed through a dedicated team of talent acquisition specialists. When needed, we involve our immigration attorney to ensure compliance with local, regional, and national employment laws, regulations, and policies.</p>																																												
	TC-SI-330a.2	Employee engagement as a percentage	<p>Defined as the average of employee ratings of agreement or strong agreement with positive engagement statements, our employee engagement is 88%, which is determined via our annual employee survey.</p> <p>We also monitor employee engagement through employee retention and internal mobility, as well as participation in Employee Affinity Groups and wellness activities, such as our global community outreach program.</p>																																												
	TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	<p>Gender Representation of Global Employees (%)</p> <table border="1" data-bbox="1014 922 1892 1062"> <thead> <tr> <th></th> <th>Female</th> <th>Male</th> <th>N/A*</th> </tr> </thead> <tbody> <tr> <td>Management</td> <td>23.26%</td> <td>76.74%</td> <td>0.00%</td> </tr> <tr> <td>Technical Staff</td> <td>20.07%</td> <td>71.28%</td> <td>8.65%</td> </tr> <tr> <td>All Other Employees</td> <td>34.78%</td> <td>58.89%</td> <td>6.32%</td> </tr> </tbody> </table> <p>* N/A = not available or not disclosed</p> <p>Racial/Ethnic Group Representation of U.S. Employees (%)</p> <table border="1" data-bbox="1014 1159 1892 1422"> <thead> <tr> <th></th> <th>Asian</th> <th>Black or African American</th> <th>Hispanic or Latino</th> <th>White</th> <th>Other^</th> <th>N/A*</th> </tr> </thead> <tbody> <tr> <td>Management</td> <td>14.02%</td> <td>1.87%</td> <td>5.61%</td> <td>75.70%</td> <td>2.80%</td> <td>0.00%</td> </tr> <tr> <td>Technical Staff</td> <td>26.67%</td> <td>5.71%</td> <td>3.81%</td> <td>58.10%</td> <td>5.71%</td> <td>0.00%</td> </tr> <tr> <td>All Other Employees</td> <td>6.16%</td> <td>8.53%</td> <td>5.69%</td> <td>75.83%</td> <td>2.37%</td> <td>1.42%</td> </tr> </tbody> </table>		Female	Male	N/A*	Management	23.26%	76.74%	0.00%	Technical Staff	20.07%	71.28%	8.65%	All Other Employees	34.78%	58.89%	6.32%		Asian	Black or African American	Hispanic or Latino	White	Other^	N/A*	Management	14.02%	1.87%	5.61%	75.70%	2.80%	0.00%	Technical Staff	26.67%	5.71%	3.81%	58.10%	5.71%	0.00%	All Other Employees	6.16%	8.53%	5.69%	75.83%	2.37%	1.42%
	Female	Male	N/A*																																												
Management	23.26%	76.74%	0.00%																																												
Technical Staff	20.07%	71.28%	8.65%																																												
All Other Employees	34.78%	58.89%	6.32%																																												
	Asian	Black or African American	Hispanic or Latino	White	Other^	N/A*																																									
Management	14.02%	1.87%	5.61%	75.70%	2.80%	0.00%																																									
Technical Staff	26.67%	5.71%	3.81%	58.10%	5.71%	0.00%																																									
All Other Employees	6.16%	8.53%	5.69%	75.83%	2.37%	1.42%																																									

			<p data-bbox="1024 250 1808 310">^ Other includes the following classifications: Native American or Alaska Native, Native Hawaiian or Pacific Islander, and Two or More Races</p> <p data-bbox="1024 315 1430 342">* N/A = not available or not disclosed</p> <p data-bbox="1010 383 1881 602">Diversity is vital for our ability to grow and innovate in such a fast-changing environment. We strive to build teams where employees can bring new ideas and perspectives to bear, promoting creativity and driving effective business solutions. We make a concerted effort to develop a diverse candidate pipeline and offer a diverse slate of candidates for all vacant positions. As part of this effort, we survey hiring managers post-hire to elicit feedback on the diversity of the candidate pool.</p> <p data-bbox="1010 643 1892 862">We actively recognize and celebrate diversity at LiveVox—in our heritage, history, experiences, abilities, personal identification, and perspectives. For example, we celebrate and educate our employees about various cultures and capabilities through our annual diversity, equity, and inclusion calendar, which highlights diverse events, celebrations, awareness, and festivities each month. We also offer formal training and development on diversity and inclusion, as well as harassment and discrimination prevention, to all employees.</p> <p data-bbox="1010 902 1881 1089">Our EAGs (Employee Affinity Groups) are an integral component of LiveVox’s commitment to help drive change in diversity and inclusion and allow us to capitalize on the extraordinary resources of our employees. EAGs are employee led, self-directed, voluntary groups that offer opportunities to network internally, attract a diverse employee base, enable the inclusion of ideas and solutions, and create opportunities for mentoring and career development.</p>
Intellectual Property Protection & Competitive Behavior	TC-SI-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations	We had no monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations.
Managing Systemic Risks From	TC-SI-550a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Currently, this information is not available for external publication; however, we do use it internally for remediation initiatives, better risk assessment, and fine-tuning existing product reliability safeguards.

Technology Disruptions	TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	<p>We strive to stay ahead of problems and to catch developing ones before they affect customer operations. LiveVox platform environments are built to minimize risks and disruptions of operations and include capabilities to deliver and better manage high availability, reliability, business continuity, and disaster recovery.</p> <p>The LiveVox platform architecture inherently supports high availability, leveraging highly resilient and redundant pooled services and application components. We've designed reliable and seamless failover into every level of our systems, with periodic testing, change control, and data center resilience to help deal with any event and recover quickly.</p> <p>We address business continuity and disaster recovery separately:</p> <ul style="list-style-type: none"> • Business continuity consists of technologies, configurations, and contractual arrangements applied across our platform, with a focus on resilience (i.e., ability to withstand stress) and continuation of services in the event of failures. • Disaster recovery is a customer-specific set of procedures to respond to force majeure events, developed in collaboration with customers and based on customer-specific requirements. <p>Our comprehensive approach to business continuity and disaster recovery classifies different categories of potential outage causes:</p> <ul style="list-style-type: none"> • Carrier, customer, internal, and vendor hardware and software failure and/or bugs • Human error, including carrier, customer, and internal personnel • Force majeure events, such as weather and terrorism <p>LiveVox cloud mitigation is designed with measures in place to address these potential outage causes, including:</p> <ul style="list-style-type: none"> • Resilient data center, agent, and carrier interconnect architectures that build significant business continuity into the LiveVox platform • 24/7 quality assurance processes • Agile continuous system integration and testing, as well as extensive staff training • Phased and dynamic deployment to production, which results in both rapid and stable deliveries
-------------------------------	--------------	---	--

			<ul style="list-style-type: none">• Change control process that improves traceability and reliability across the entire LiveVox platform• Geographic data center failover• Customer service level agreements (SLAs) <p>We operate in virtual public cloud environments, with presence in geo-diverse regional environments across North America through AWS. AWS chooses its data center locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity. Each AWS Region has multiple, isolated locations, known as Availability Zones. Because we operate multiple regional environments in the United States, we also support requirements for further geo-diversity than can be met within a region and availability zones. Portal instances between these environments and regions are not synchronized, as the environments are separate and distinct by design. Current SLAs can be further enhanced by adding intra-region availability to ensure high availability in the event of data center failure within an Availability Zone.</p> <p>Given the SaaS nature of our business and the development and release cycles, life cycle management of environments is on a continuous cadence. These factors drive constant monitoring and an ongoing approach to assessing risk. Standing weekly touch points across business and technical operations translate to a practical operational feedback loop.</p>
--	--	--	--