TECHNOLOGY & COMMUNICATIONS SECTOR

SOFTWARE & IT SERVICES

Sustainability Accounting Standard

Sustainable Industry Classification System® (SICS®) TC-SI

Prepared by the
Sustainability Accounting Standards Board

October 2018

INDUSTRY STANDARD | VERSION 2018-10

SUSTAINABILITY DISCLOSURE TOPICS & ACCOUNTING METRICS

Table 1. Sustainability Disclosure Topics & Accounting Metrics

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-SI-130a.1
	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Quantitative	Thousand cubic meters (m³), Percentage (%)	TC-SI-130a.2
	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	n/a	TC-SI-130a.3
Data Privacy & Freedom of Expression	Description of policies and practices relating to behavioral advertising and user privacy	Discussion and Analysis	n/a	TC-SI-220a.1
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-SI-220a.2
	Total amount of monetary losses as a result of legal proceedings associated with user privacy[2]	Quantitative	Reporting currency	TC-SI-220a.3
	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-SI-220a.4
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring[3]	Discussion and Analysis	n/a	TC-SI-220a.5
Data Security	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected[4]	Quantitative	Number, Percentage (%)	TC-SI-230a.1
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-SI-230a.2
Recruiting & Managing a Global, Diverse & Skilled Workforce	Percentage of employees that are (1) foreign nationals and (2) located offshore[5]	Quantitative	Percentage (%)	TC-SI-330a.1
	Employee engagement as a percentage[6]	Quantitative	Percentage (%)	TC-SI-330a.2
	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees[7]	Quantitative	Percentage (%)	TC-SI-330a.3

[2] Note to **TC-SI-220a.3** – The entity shall briefly describe the nature, context, and any corrective actions taken as a result of the monetary losses.
[3] Note to **TC-SI-220a.5** – Disclosure shall include a description of the extent of the impact in each case and, where relevant, a discussion of the entity's policies and practices related to freedom of expression.
[4] Note to **TC-SI-230a.1** – Disclosure shall include a description of corrective actions implemented in response to data breaches.
[5] Note to **TC-SI-330a.1** – Disclosure shall include a description of potential risks of recruiting foreign nationals and/or offshore employees, and management approach to addressing these risks.
[6] Note to **TC-SI-330a.2** – Disclosure shall include a description of methodology employed.

Data Privacy & Freedom of Expression

Topic Summary

As software and IT services companies increasingly deliver products and services over the Internet and through mobile devices, they must carefully manage two separate and often conflicting priorities. On the one hand, companies use customer data to innovate and provide customers with new products and services and to generate revenues. On the other hand, there are privacy concerns associated with companies having access to a wide range of customer data, such as personal, demographic, content, and behavioral data. This dynamic is leading to increased regulatory scrutiny in many countries around the world. The delivery of cloud-based software and IT services also raises concerns about potential access to user data by governments that may use it to limit the freedoms of citizens. Effective management in this area is important to reduce regulatory and reputational risks that can lead to decreased revenues, lower market share, and regulatory actions involving potential fines and other legal costs.

Accounting Metrics

TC-SI-220a.1. Description of policies and practices relating to behavioral advertising and user privacy

1 The entity shall describe the nature, scope, and implementation of its policies and practices related to user privacy, with a specific focus on how it addresses the collection, usage, and retention of user information.

1.1 User information includes information that pertains to a user's attributes or actions, including but not limited to, account statements, transaction records, records of communications, content of communications, demographic data, behavioral data, location data, and/or personally identifiable information (PII).

1.2 Demographic data are defined as the quantifiable statistics that identify and distinguish a given population. Examples of demographic data include gender, age, race/ethnicity, knowledge of languages, disabilities, mobility, home ownership, and employment status.

1.3 Behavioral data are defined as the product of tracking, measuring, and recording individual behaviors, such as online browsing patterns, buying habits, brand preferences, and product usage patterns.

1.4 Location data are defined as data describing the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that would enable identifying and tracking an individual's physical location.

1.5 PII is defined as any information about an individual that is maintained by an entity, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment

information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

2 The entity shall describe the information "lifecycle" (i.e., collection, usage, retention, processing, disclosure, and destruction of information) and how information-handling practices at each stage may affect individuals' privacy.

2.1 With respect to data collection, it may be relevant for the entity to discuss which data or types of data are collected without the consent of an individual, which require opt-in consent, and which require opt-out action from the individual.

2.2 With respect to usage of data, it may be relevant for the entity to discuss which data or types of data are used by the entity internally, and under which circumstances the entity shares, sells, rents, or otherwise distributes data or information to third parties.

2.3 With respect to retention, it may be relevant for the entity to discuss which data or types of data it retains, the length of time of retention, and practices used to ensure that data is stored securely.

3 The entity shall discuss the degree to which its policies and practices address similar issues as those outlined in the U.S. Office of Management and Budget's (OMB) "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22)," including use of Privacy Impact Assessments (PIAs).

3.1 A PIA is an analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information in order to mitigate potential privacy risks.

3.2 As outlined by OMB M-03-22, PIAs must analyze and describe: (a) what information is to be collected, (b) why the information is being collected, (c) the intended use of the information, (d) with whom the information will be shared, (e) what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), including how individuals can grant consent, and (f) how the information will be secured, among other government-specific requirements.

4 The entity shall discuss how its policies and practices related to privacy of user information address children's privacy, which at a minimum includes the provisions of the U.S. Children's Online Privacy Protection Act (COPPA).

5 The scope of disclosure includes both first- and third-party advertising.

6 With respect to behavioral advertising, the entity may describe how it addresses the following principles, described by the cross-industry Self-Regulatory Principles for Online Behavioral Advertising:

6.1 Education: participation in educational efforts for consumers about behavioral online advertising

6.2 Transparency: clearly disclosing information about data collection and data use practices

6.3 Consumer control: allowing users to choose whether data is collected or transferred to non-affiliates

6.4 Data security: providing basic security provisions and having clear policies relating to retention of user information

6.5 Material changes: obtaining consent before applying changes to policies that are less restrictive than existing ones

6.6 Sensitive data: abiding by COPPA, and handling user data such as financial information, Social Security numbers, and medical information

6.7 Accountability: participation in self-regulatory organizations such as the Direct Marketing Association

TC-SI-220a.2. Number of users whose information is used for secondary purposes

1 The entity shall disclose the number of unique users whose information is used for secondary purposes.

1.1 User information includes information that pertains to a user's attributes or actions, including but not limited to, account statements, transaction records, records of communications, content of communications, demographic data, behavioral data, location data, and/or personally identifiable information (PII).

1.1.1 Demographic data are defined as the quantifiable statistics that identify and distinguish a given population. Examples of demographic data include gender, age, race/ethnicity, knowledge of languages, disabilities, mobility, home ownership, and employment status.

1.1.2 Behavioral data are defined as the product of tracking, measuring, and recording individual behaviors such as online browsing patterns, buying habits, brand preferences, and product usage patterns.

1.1.3 Location data are defined as data describing the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that would enable identifying and tracking an individual's physical location.

1.1.4 PII is defined as any information about an individual that is maintained by an entity, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

1.2 Secondary purpose is defined as the intentional use of data by the entity (i.e., not a breach of security) that is outside the primary purpose for which the data was collected. Examples of secondary purposes include, but are not limited to, selling targeted ads, improving the entity's products or service offerings, and transferring data or information to a third party through sale, rental, or sharing.

1.3 User accounts that the entity cannot verify as belonging to the same individual shall be disclosed separately.

2 The scope of disclosure shall include the users whose information is used by the entity itself for secondary purposes as well as the users whose information is provided to affiliates or non-affiliates to use for secondary purposes.

2.1 Affiliate is defined as an entity that directly or indirectly controls, is controlled by, or is under common control with the entity.

2.2 Non-affiliates are all third parties other than the entity and its affiliates.

TC-SI-220a.3. Total amount of monetary losses as a result of legal proceedings associated with user privacy

1 The entity shall disclose the total amount of monetary losses it incurred during the reporting period as a result of legal proceedings associated with incidents relating to user privacy.

2 The legal proceedings shall include any adjudicative proceeding in which the entity was involved, whether before a court, a regulator, an arbitrator, or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement or verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (e.g., civil judgments or settlements), regulatory proceedings (e.g., penalties, disgorgement, or restitution), and criminal actions (e.g., criminal judgment, penalties, or restitution) brought by any entity (e.g., governmental, business, or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defense.

5 The scope of disclosure shall include, but is not limited to, legal proceedings associated with the enforcement of relevant industry regulations, such as:

5.1 California Consumer Privacy Act

5.2 EU Directive 2002/58/EC (ePrivacy Directive)

5.3 EU-U.S. Privacy Shield

5.4 EU's General Data Protection Regulation (GDPR) (EU) 2016/679

5.5 Japan's Act on the Protection of Personal Information

5.6 U.S. Children's Online Privacy Protection Act

5.7 U.S. Federal Trade Commission Privacy Act

6 The scope of disclosure shall include, but is not limited to, legal proceedings associated with the enforcement of relevant industry regulations promulgated by regional, national, state, and local regulatory authorities, such as:

6.1 European Data Protection Supervisor

6.2 Japan's Personal Information Protection Commission

6.3 U.S. Federal Trade Commission

Note to **TC-SI-220a.3**

1 The entity shall briefly describe the nature (e.g., judgment or order issued after trial, settlement, guilty plea, deferred prosecution agreement, non-prosecution agreement) and context (e.g., unauthorized monitoring, sharing of data, children's privacy) of all monetary losses as a result of legal proceedings.

2 The entity shall describe any corrective actions it has implemented as a result of the legal proceedings. This may include, but is not limited to, specific changes in operations, management, processes, products, business partners, training, or technology.

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

1 The entity shall disclose (1) the total number of unique requests for user information, including user content and non-content data, from government or law enforcement agencies.

1.1 Content data includes user-generated information such as email text or recorded phone conversation.

1.2 Non-content data includes information such as an email address, a person's name, country of residence, or gender, or system-generated data such as IP addresses and traffic data.

1.3 Both content and non-content data can include personally identifiable information (PII).

1.3.1 PII is defined as any information about an individual that is maintained by an entity, including (a) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (b) any other information that is linked or linkable to an individual, such as medical, educational, financial,

and employment information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

2 The entity shall disclose (2) the total number of unique users whose information was requested by government or law enforcement agencies.

2.1 The number of records requested shall be calculated as the sum of unique users whose user information was requested across all requests for information from government or law enforcement agencies received during the reporting period.

2.1.1 If the entity is not able to verify that two records (i.e., user information) belong to the same user, the entity shall consider this two users.

3 The entity shall disclose (3) the percentage of government and law enforcement requests that resulted in disclosure to the requesting party.

3.1 The percentage shall be calculated as the number of unique requests that resulted in disclosure to the requesting party divided by the total number of unique requests received.

3.2 The scope of requests that resulted in disclosure shall include requests that resulted in full or partial compliance with the disclosure request within the reporting period.

3.3 The scope of the requests that resulted in disclosure shall include disclosure of aggregated, de-identified, and anonymized data, which is intended to prevent the recipient from reconfiguring the data to identify an individual's actions or identity.

3.3.1 The entity may discuss whether these characteristics apply to a portion of its data releases if this discussion would provide necessary context for interpretation of the entity disclosure.

4 The entity may additionally break down its disclosure by region or country.

5 The entity may describe its policy for determining whether to comply with a request for user data, including under what conditions it will release user data, what requirements must be met in the request, and the level of management approval required.

6 The entity may describe its policy for notifying users about such requests, including the timing of notification.

TC-SI-220a.5. List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring

1 The entity shall disclose a list of the countries where its products and services are monitored, blocked, or content is filtered or censored due to governmental, judicial, or law enforcement requests or requirements, where:

1.1 Monitoring occurs when a government authority or law enforcement agency has routine access to content or non-content data of specific users or of all users of a particular product or service.

1.2 Blocking occurs when the entity is prohibited by law or government authority from providing some or all of the entity's products or services in a country.

1.3 Content filtering or censoring occurs when a government authority alters access to, or display of, content of a product or service either directly by overriding service provision, or indirectly by requiring that a company remove certain content. Examples include content that is considered politically or culturally sensitive.

2 The scope of this disclosure includes company operations that have been discontinued, or were never offered, in a region due to government activity related to monitoring, blocking, content filtering, or censoring.

Note to **TC-SI-220a.5**

1 The entity shall describe the extent of monitoring, blocking, content filtering, or censorship across its product or service lines, including the specific products affected, nature and duration of impact, and percent of customers affected.

2 The entity may discuss implications of blocking or censorship, such as affecting ability to grow market share, or increased costs to comply with these restrictions.

3 For products and services that have been modified in a manner material to their functionality, the entity shall identify the product or service affected and discuss the nature of the modification, indicating whether modification was undertaken to avoid monitoring or blocking, or to enable monitoring or blocking. The entity shall describe how the modified product or service differs from the product or service offering in its home country or other significant markets.

4 Where relevant, the entity shall discuss its policies and practices related to freedom of expression, including how they influence its decision making when operating in countries that may request or require some form of monitoring, blocking, content filtering, or censoring of the entity's content.

Data Security

Topic Summary

Software & IT services companies are targets of growing data security threats from cyber attacks and social engineering, which puts their own data and their customers' data at risk. Inadequate prevention, detection, and remediation of data security threats can influence customer acquisition and retention and result in decreased market share and lower demand for the company's products. In addition to reputational damage and customer turnover, data breaches can also result in increased expenses, commonly associated with remediation efforts such as identity protection offerings and employee training on data protection. Meanwhile, new and emerging data security standards and regulations are likely to affect the operating expenses of companies through increased costs of compliance. Additionally, companies in this industry are well-positioned to uncover revenue opportunities by providing secure software and services to meet the demand for ensuring data is kept secure.

Accounting Metrics

TC-SI-230a.1. (1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected

1 The entity shall calculate and disclose (1) the total number of data breaches identified during the reporting period.

1.1 Data breach is defined as the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. This definition is derived from the U.S. National Initiative for Cybersecurity Careers and Studies (NICCS) glossary.

1.2 The scope of disclosure is limited to data breaches that resulted in a deviation from the entity's expected outcomes for confidentiality and/or integrity.

2 The entity shall disclose (2) the percentage of data breaches in which personally identifiable information (PII) was subject to the data breach.

2.1 PII is defined as any information about an individual that is maintained by an entity, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

2.2 The scope of disclosure shall include incidents in which encrypted data were acquired with an encryption key that was also acquired, as well as if there is a reasonable belief that encrypted data could be readily converted to plaintext.

2.2.1 Encryption is defined as the process of transforming plaintext into ciphertext. This definition is derived from the NICCS glossary.

2.3 The scope of disclosure is limited to breaches in which users were notified of the breach, either as required by law or voluntarily by the entity.

3 The entity shall disclose (3) the total number of unique users who were affected by data breaches, which includes all those whose personal data was compromised in a data breach.

3.1 Accounts that the entity cannot verify as belonging to the same user shall be disclosed separately.

4 The entity may delay disclosure if a law enforcement agency has determined that notification impedes a criminal investigation or until the law enforcement agency determines that such notification does not compromise the investigation.

Note to **TC-SI-230a.1**

1 The entity shall describe the corrective actions taken in response to data breaches, such as changes in operations, management, processes, products, business partners, training, or technology.

1.1 The U.S. SEC's Commission Statement and Guidance on Public Company Cybersecurity Disclosures may provide further guidance on disclosures on the corrective actions taken in response to data breaches.

2 All disclosure shall be sufficient such that it is specific to the risks the entity faces, but disclosure itself will not compromise the entity's ability to maintain data privacy and security.

3 The entity may disclose its policy for disclosing data breaches to affected users in a timely manner.

TC-SI-230a.2. Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards

1 The entity shall describe its approach to identifying vulnerabilities in its information systems that pose a data security risk.

1.1 Vulnerability is defined as a weakness in an information system, system security procedures, internal controls, and/or implementation that could be exploited.

1.2 Data security risk is defined as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or nations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

2 The entity shall describe its approach to addressing data security risks and vulnerabilities it has identified, including, but not limited to, operational procedures, management processes, structure of products, selection of business partners, employee training, and use of technology.

3 The entity shall describe its use of third-party cybersecurity risk management standards.

3.1 Third-party cybersecurity risk management standards are defined as standards, frameworks, and/or guidance developed by a third-party with the explicit purpose of aiding companies in identifying cybersecurity threats, and/or preventing, responding to, and/or remediating cybersecurity incidents.

3.2 Examples of third-party cybersecurity risk management standards include, but are not limited to:

3.2.1 The American Institute of Certified Public Accountants' (AICPA) Service Organization Controls (SOC) for Cybersecurity

3.2.2 ISACA's COBIT 5

3.2.3 ISO/IEC 27000-series

3.2.4 National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*

3.3 Disclosure shall include, but is not limited to:

3.3.1 Identification of the specific cybersecurity risk management standard(s) that have been implemented or are otherwise in use

3.3.2 Description of the extent of its use of cybersecurity risk management standard(s), such as by applicable operations, business unit, geography, product, or information system

3.3.3 The role of cybersecurity risk management standards in the entity's overall approach to identifying vulnerabilities in its information systems and addressing data security risks and vulnerabilities

3.3.4 If the third-party verification of the use of cybersecurity risk management standards is conducted, including independent examinations or audits

3.3.5 Ongoing activities and initiatives related to increasing the use of cybersecurity risk management standards, even if such standards are not currently in use

4 The entity may discuss trends it has observed in type, frequency, and origination of attacks to its data security and information systems.

5 The U.S. SEC's Commission Statement and Guidance on Public Company Cybersecurity Disclosures may provide further guidance on disclosures on the entity's approach to addressing data security risks and vulnerabilities.

6 All disclosure shall be sufficient such that it is specific to the risks the entity faces but disclosure itself would not compromise the entity's ability to maintain data privacy and security.

SUSTAINABILITY ACCOUNTING STANDARDS BOARD
1045 Sansome Street, Suite 450
San Francisco, CA 94111
415.830.9220
info@sasb.org

sasb.org