SASB DISCLOSURES 2024

SASB STANDARDS
Now part of IFRS Foundation

For FY24, we are pleased to continue reporting in line with the Sustainability Accounting Standards Board ("SASB") Sustainability Accounting Standard for Professional & Commercial Services, which enables us to share sustainability data in a consistent and transparent way for the benefit of our stakeholders.

Topic	Accounting metric	Code	Response
Data security	Description of approach to identifying and addressing data security risks	SV-PS-230a.1	**Our approach** We take data security seriously and proactively address any potential risks. Data security is not only a critical aspect of our operations, but also a key part of our sustainability initiatives. We follow a structured approach to assess and treat risks in IT and cyber security. This process involves several key steps to ensure that risks are identified, evaluated, and mitigated effectively. 1. Risk Identification We start by identifying potential risks that could impact our IT and cyber security. This involves: • Asset Inventory: Maintaining a comprehensive inventory of all IT assets, including hardware, software, data, and network components. • Threat Analysis: Identifying potential threats such as cyber-attacks, data breaches, and system failures. • Vulnerability Assessment: Conducting regular assessments to identify vulnerabilities in our systems and processes. 2. Risk Assessment Once risks are identified, we assess their potential impact and likelihood. This involves: • Risk Evaluation: Evaluating the potential impact of each risk on our business operations, data integrity, and reputation. • Likelihood Analysis: Assessing the likelihood of each risk occurring based on historical data and current threat landscape. • Risk Prioritization: Prioritizing risks based on their potential impact and likelihood, focusing on those that pose the greatest threat to our organization. 3. Risk Treatment After assessing the risks, we implement measures to mitigate or eliminate them. This involves: • Risk Mitigation: Implementing controls and safeguards to reduce the likelihood and impact of risks. This includes technical measures such as firewalls, encryption, and access controls, as well as procedural measures such as policies and training. • Risk Transfer: Transferring risks to third parties through insurance or outsourcing certain functions to specialized providers. • Risk Acceptance: Accepting certain risks that are deemed to be within acceptable levels, based on analysis. • Risk Avoidance: Avoiding activities or processes that pose unacceptable risks. 4. Continuous Monitoring and Review We continuously monitor and review our risk management processes to ensure their effectiveness. This involves: • Regular Audits: Conducting regular audits and assessments to evaluate the effectiveness of our risk management measures. • Incident Response: Implementing robust incident response procedures to quickly address and mitigate the impact of security incidents.

Topic	Accounting metric	Code	Response
Data security continued	Description of approach to identifying and addressing data security risks	SV-PS-230a.1	• Continuous Improvement: Continuously improving our risk management processes based on lessons learned from incidents and changes in the threat landscape. **Our goal** Our goal is to protect and secure our clients' data at all times, and to respect their privacy. We use industry standard best practices and technologies to achieve this, such as: • Security Information and Event Management (SIEM) and eXtended Detection and Response (XDR) systems, which help us monitor and detect any security threats in real-time. • Industry-leading security and compliance platforms, which ensure end-to-end data protection. We use encryption, firewalls, and other security measures to secure data both in transit and at rest. • Regular risk assessments and updates, which enable us to stay ahead of the curve and implement new measures as needed. • Data privacy by design, which means that we consider the privacy implications of our data processing activities from the outset and implement appropriate safeguards throughout. • Data privacy by default, which means that we only collect and process the minimum amount of data necessary for our purposes and that we limit the access and retention of data to the extent required. **Our accreditation** We are proud to be Cyber Essentials Plus accredited and GDPR compliant, which shows our commitment to data security and privacy. This accreditation means that we meet high standards in the protection of sensitive information and that our clients can trust us with their data. **Our Achievements** In 2024 Fintel developed The Fintel PLC Cyber Security standard. This is a comprehensive and flexible cyber security standard that provides assurance it has implemented a range of important cyber security, privacy, and data protection measures. It is based on the IASME Cyber Assurance framework and is mapped to important ISO27001 Annex 6 controls.
	Description of policies and practices relating to collection, usage, and retention of customer information	SV-PS-230A.2	One of our core values is data privacy by design, which means that we always prioritise the protection and respect of customer information in all aspects of our business. We adhere to the highest standards of data security and privacy, as demonstrated by our compliance with UK data protection laws, such as the General Data Protection Regulation (GDPR) and the Data Protection Act (2018). Fintel maintains a comprehensive suite of policies relating to data collection, usage and retention, including: • Privacy Information Management Manual • Collecting and Processing Personal Data • Data Protection and Privacy • Privacy Impact Assessment • Rights of the Individual Polic Our Privacy Information Management Manual expands the framework for policies and procedures adopted by the Executive Management Board of Fintel PLC to implement an information security management system (ISMS) that complies with ISO/IEC 27001:2022. It addresses privacy information management in conformance with ISO/IEC 27701:2019. In accordance with our internal processes all data processing activities are subjected to a risk assessment. The conditions and controls for collecting, processing, transfer and disclosure of data are clearly defined, along individual and business responsibilities relating to data processing. The purpose and basis under which data is collected and processed is recorded and we provide the information regarding mechanisms to modify or withdraw consent, object to processing, access, correction, and erasure on our website.

Topic	Accounting metric	Code	Response
Data security continued	Description of policies and practices relating to collection, usage, and retention of customer information	SV-PS-230a.2	By following Privacy by Design and Default frameworks we limit the collection and processing of data, ensuring accuracy and quality, PII minimization, de-identification, and deletion at the end of processing. Fintel PLC is working towards achieving IASME Cyber Assurance Plus certification in 2025, further demonstrating our commitment to the highest standards of data privacy and security.
	(1) Number of data breaches, (2) percentage involving customers' confidential business information (CBI) or personally identifiable information (PII), (3) number of customers affected	SV-PS-230a.3	(1) 0 (2) 0 (3) 0 — As a matter of course, we do not disclose this information unless necessary to do so to meet regulatory compliance. However, we can confirm there have been no material data breaches in the past year.
Workforce Diversity & Engagement	Percentage of gender and racial/ethnic group representation for (1) executive management and (2) all other employees	SV-PS-330a.1	We have a number of policies and programs for fostering equitable employee representation. A summary of these can be found on pages 26-27 and 32-33 of the 2024 annual report and accounts. Throughout 2024 we continued to run a dedicated campaign to better understand levels of diversity amongst our staff, which incrased our disclosure rate across multiple diversity metrics from 27% to 38%. Our goal is to improve this to better understand our workforce and we set a goal to reach a 50% disclosure rate.
	(1) Voluntary and (2) involuntary turnover rate for employees	SV-PS-330a.2	(1) 9.2% (2) 3.7% — The voluntary turnover rate has been calculated as the total number of employee-initiated voluntary separations (e.g. resignation and retirement) during the reporting period, divided by the total number of unique workers employed during the reporting period. The involuntary turnover rate has been calculated as the total number of entity-initiated separations (e.g. dismissal, downsizing, redundancy and non-renewal of contract) during the reporting period, divided by the number of unique workers employed during the reporting period.
	Employee engagement as a percentage	SV-PS-330a.3	81% — Aggregated participation rate is based on data gathered via our employee engagement tool, Peakon.
Professional Integrity	Description of approach to ensuring professional integrity	SV-PS-510a.1	We have multiple policies in place to ensure appropriate conduct, including (but not limited to): Code of Ethics, Whistleblowing, Bribery and Corruption, Gifts and Hospitality, Modern Slavery and Discrimination and Harassment. Nominated senior individuals within the company are responsible for looking after these.
	Total amount of monetary losses as a result of legal proceedings associated with professional integrity	SV-PS-510a.2	£0

Gender representation

	Female	Male
(1)	29%	71%
(2)	55%	45%

Racial/ethnic group representation

	White	Prefer not to say	Ethnic minorities	Not disclosed
(1)	44%	0%	5%	51%
(2)	31%	0%	4%	65%

Activity metric	Code	Response
Number of employees by: (1) full-time and part-time, (2) temporary, and (3) contract	SV-PS-000.A	(1) 96% (2) 1% (3) 3% — As of 31 December 2024 we had 656 employees. This number does not include any external contractors. Contract workers metric (3) includes zero hour contracts.
Employee hours worked, percentage billable	SV-PS-000.B	Fintel does not track employee hours.

Fintel plc
Fintel House
St. Andrew's Road
Huddersfield
West Yorkshire
HD1 6NA
T: 01484 439 100