Now a Part of S&P Global

Data Security at S&P Global **Switzerland SA ("SAM")** for Corporate Sustainability Assessment (CSA)

This document describes a set of administrative, technical and physical controls which are in place in order to protect SAM internal and our customers' non-public personal information, including information and documentation submitted to SAM as part of its annual Corporate Sustainability Assessment. These controls are intended to:

1. ensure the confidentiality, integrity, and availability of data
2. define, develop, and document mechanisms that support SAM goals and objectives
3. allow SAM to satisfy its legal and ethical responsibilities regarding its IT resources (i.e. applications and servers)

Geographical resiliency of SAM applications
All SAM core applications are hosted in a corporate Virtual Private Network hosted at AWS Ireland in two geographically separated datacenters providing a full redundant infrastructure.

Account Control Process
Once a year SAM makes sure that the access rights for each application and shared resource (e.g. shared mailboxes, access to CSA data, network folders) is reviewed and approved by the respective Business Owner. Access to SAM's proprietary software (SIMS3) for collecting and evaluating sustainability information provided through the Corporate Sustainability Assessment is approved by the Business Owner, ensuring that existing and new employees do not gain access to information to which they should not have access.

Cyber Security and Vulnerability Assessment
SAM executes regular Vulnerability Assessments on the Corporate Sustainability Assessment website, which range from network scans till static source code analysis to ensure that the website is securely managed.

Security Awareness Program
At least once a year, all SAM employees are required to participate in mandatory E-Learning modules, an online platform which include topics related to Cyber Security, Business Continuity Management and phishing/social engineering.

Change Management
Change Control is the process that management uses to identify, document and authorize changes to SAM's IT environment. It minimizes the likelihood of disruptions, unauthorized alterations and errors. Information Security officers are involved in the review of architectural designs and changes made to the production environment.

Network Security
In addition to Intrusion Detection and Firewalls system, traffic towards SAM applications is monitored to prevent denial of service attacks, malicious code or other traffic that threatens systems within the network or that violate SAM information security policies. All SAM applications publicly exposed to the internet are only accessible via Secured protocols (e.g. FTPS, HTTPS).

Backup Policies
SAM stores data, including the historical information provided in its production level databases. Regular backups are encrypted and stored at secure locations within the corporate network of S&P Global.

S&P Global Switzerland SA has acquired the ESG Ratings and Benchmarking business from RobecoSAM AG, which includes the SAM Corporate Sustainability Assessment. To understand how SAM and S&P Global collect and process personal information, please see the S&P Global Privacy Policy.