S&P Global

Data Security at S&P Global for Corporate Sustainability Assessment (CSA)

This document describes a set of administrative, technical, and physical controls which are in place in order to protect S&P Global Inc.'s (including its related, affiliated and/or subsidiary companies, hereinafter referred to as "S&P Global") internal and our customers' non-public personal information, including information and documentation submitted to S&P Global 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 S&P Global ESG Research's goals and objectives
3. allow S&P Global to satisfy its legal and ethical responsibilities regarding its IT resources (i.e., applications and servers)

All core applications related to the CSA are deployed in a corporate Virtual Private Network hosted at AWS Ireland (primary) and AWS Germany (secondary) in two geographically separated datacenters providing a fully redundant infrastructure.

Account Control Process

Once a year S&P Global 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 S&P Global'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

S&P Global executes regular Vulnerability Assessments on the Corporate Sustainability Assessment website, which range from network scans to static source code analysis to ensure that the website is securely managed.

Vulnerability assessments are executed as part of monthly/quarterly release activities, and penetration tests are coordinated with an external party on an annual schedule. Vulnerabilities are taken care of and remediated based on actual findings and severity.

S&P Global

Security Awareness Program

At least once a year, all S&P Global 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

A corporate-wide Change Control process is in place to identify, document, and authorize changes to S&P Global's IT environment. It minimizes the likelihood of disruptions, unauthorized alterations, and errors. Information Security officers are involved in the review of architectural designs before such changes are made to the production environment.

Network Security

In addition to Intrusion Detection and Firewalls system, traffic towards S&P Global applications is monitored to prevent denial of service attacks, malicious code or other traffic that threatens systems within the network or that violate S&P Global information security policies. The CSA website is exposed to the internet via secure protocol (HTTPS). Data stored within or uploaded to the CSA website is also encrypted at rest.

Backup Policies

S&P Global 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.

Privacy Protection

To understand how S&P Global collects and processes personal information, please see the S&P Global Privacy Policy.