Data Security at RobecoSAM

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

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

Geographical resiliency of RobecoSAM applications

All RobecoSAM core applications are hosted by third party provider in two geographically separated datacenters providing a full redundant infrastructure.

Account Control Process

Once a year RobecoSAM 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 RobecoSAM' 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

The RobecoSAM Security Officer is member of the Cyber Security Circle, a meeting which is scheduled on a quarterly basis, where all Security Officers in the Robeco Group analyze a number of topics related to Cyber Security and where possible measures of improvements are discussed.

In terms of Vulnerability Assessments, a third party contractor runs a so-called 24/7 SWAT (Secure Web Application Tactics) analysis on the Corporate Sustainability Assessment website, which is an accurate vulnerability management solution for the web applications.

Furthermore, RobecoSAM runs once a year a penetration test on all RobecoSAM servers directly exposed to the internet, its results are discussed in the regular security meetings and, if needed, brought to the attention of Management Board.

Security Awareness Program

At least once a year, all RobecoSAM 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 RobecoSAM IT environment. It minimizes the likelihood of disruptions, unauthorized alterations and errors. Once a week, the Security Officer of RobecoSAM participates in the Change Advisory Board meeting (CAB), where all adjustments to operating systems, applications and network elements of all RobecoSAM servers are discussed and approved/rejected.

Network Security

In addition to Intrusion Detection and Firewalls system, a dedicated Security Operation Center (SOC) monitors traffic towards RobecoSAM applications, prevents denial of service attacks, malicious code or other traffic that threatens systems within the network or that violates RobecoSAM information security policies. All RobecoSAM applications publicly exposed to the internet are only accessible via Secured protocols (e.g. FTPS, HTTPS).

Backup Policies

RobecoSAM stores data, including the historical information provided in its production level databases.
In line with RobecoSAM's backup policy, all production and non-production servers are backed up by 3rd party providers and stored in safe locations by them.
The backup schedule and retention period of production environments is as follows:

1. Daily backup kept for 30 days
2. Weekly backup kept for 37 days
3. Both Daily and Weekly backup for production servers stored offline additionally for 30 days

Disaster Recovery Tests (DRT)

On an annual basis, RobecoSAM performs a DRT covering all RobecoSAM servers hosted in the 3rd party provider's datacenters. The test must confirm that in case of an issue on the primary datacenter, all of RobecoSAM's business critical applications are failed over and tested in the secondary location, and afterwards switched back (and sounded again) to the primary.

RobecoSAM AG, April 2018