SWARCO

Cloud Solutions

Security Program Overview V2.0

The Better Way. Every Day.

Preface

SWARCO is obliged to protect the security of customer data. By providing end-to-end security, the data is saved in a scalable and highly available environment. We at SWARCO know that only secure systems can create trust.

Transparent security policies enable to establish an understanding of how data is secured. Thus, SWARCO can convey to its customers a strong sense of security. Thanks to strict operative controls, the customers know that their data is always in good hands at SWARCO. There are continuous quality controls with comprehensive security checks for processing and monitoring of sensitive data. In addition, a multi-layered system composed of detailed controls protects companies from legal liability as a result of improper use and/or access.

This document presents the security processes which SWARCO Cloud Services implements in customer environments. An information security management system (ISMS), which is ISO/IEC 27001 certified, is operated to achieve the security objectives.

Table of Contents

1 Introduction

1.1 Hazard classification

By means of the security guidelines of SWARCO, the following hazards are meant to be minimised:

- O1: Vulnerabilities of the architecture and data centre
- O2: Failure of the service platform
- O3: Violation of data protection and data loss
- O4: Failure/reduction of performance (software and hardware)
- O5: Change process risks and human error
- O6: Control processes for implementing security measures

1.2 Hazard minimization

This document describes the countermeasure applied by SWARCO Cloud Services to minimise the global risks mentioned above.

Risk	Measures
Vulnerabilities of the architecture and data centre	Facilities Management
Failure of the service platform	Disaster Recovery Change management Incident Response
Violation of data protection and data loss	Data Backup Incident Response Authentication management
Failure/reduction of performance (software and hardware)	Incident Response Capacity Management
Operational safety - Change process risks and human error	Change Management
Facility Management	CMDB Management Change Management Deployment of Products & Services

1.3 Continual improvement process

As part of integrating the ITIL guidelines into the Change Management Processes, SWARCO implements a continual improvement process of the components belonging to the global security structure. For this reason, SWARCO reserves its right to adjust contents and quality of the elements described in the present document, if applicable.

2 Security principles

2.1 Overview

The Cloud Information Security Programme established by SWARCO consists of numerous guidelines on the governance of technology, people and processes within the organisation. The top management levels establish principles and competences of the organisations. SWARCO Cloud Service uses processes based on ITIL for incident and change management processes in its operating activities. In doing so, SWARCO optimises planning, performance and monitoring of operation.

Guideline	Purpose
Authentication Management	Authentication Management guarantees a secure authentication when accessing SWARCO Cloud Services systems and related infrastructure.
Incident Management	Incident Management determines the way in which SWARCO has to respond to Security Incidents and/or reported vulnerabilities. This includes internal and, if necessary, external investigation, limitation of damage, obligation to notify (as far as applicable), changes in security control and documentation.
Change Management	The purpose of this guideline lies in ensuring the safe operation of SWARCO's infrastructure (IS) also in the case of necessary changes. Changes require good planning, monitoring, tests and validation in order to be value-enhancing as well as to counteract possible impairments.
Data Backup	Serves SWARCO Cloud Services as orientation in establishing data backup and recovery plans for customers who use SWARCO Cloud Services. Backup solutions are a central element of the flexible, scalable and permanently available security system of the SWARCO Cloud Services.

2.2 Guidelines updates

In addition to the Cloud Policies, SWARCO also follows extensive internal guidelines and processes for which there is supporting documentation in each case. The internal requirements established by SWARCO provide for the revision of the guidelines at least once a year and/or in case of important changes.

2.3 Competencies & responsibilities

Security principles such as separation of tasks and the principle of least privilege are part of each guideline and each process. The Change Management Process followed by SWARCO is based on the ITIL guidelines, separates units with security tasks from general administrative tasks, keeps documentation and/or approval of changes or access requests and is supported by the problem-solving expertise of an IT Service Management Solution.

Security competencies and responsibilities are managed separately from general system and network administration functions. Auditing functions are assumed by an external group within SWARCO which is responsible for the careful examination and analysis of the event logs. Risk and Vulnerability Management are administrated and maintained by the group mentioned above.

3 Operational safety

3.1 Change Management

Systems at SWARCO are subject to an extensive process for changes including patch and configuration administration. Change Requests are processed in a standardised procedure. This is to ensure that all changes are released and registered. Events which could have a high impact are discussed and evaluated by a Change and Review Board (CRB) as well as by a Change Advisory Board (CAB) in order to exclude impairments of confidentiality, integrity or availability of a system due to an implemented change. The Change Management Process employed by SWARCO is based on the ITIL guidelines for Incident Management.

3.2 Configuration Management / System base

Within the centralised solution which is applied within the framework of the Cloud Services, SWARCO maintains exact and relevant system guidlines for hardware and software which are subject to a review each year. A comprehensive system list allows SWARCO Cloud Services to efficiently manage adjustments to customer environments. There are adjustments within the framework of the Change Management Process.

3.3 Access Management

By means of the built-in abilities of an ITSM solution, SWARCO Cloud Services provides for the unimpeded flow of data having regard to the necessary approvals of the supervisors of the requesters, the respective management team as well as the SWARCO Security Office. The access is checked every year and is changed with each change in personnel.

3.4 Training & security awareness

All SWARCO employees as well as contractors/suppliers commissioned by SWARCO who have access to the customer systems have to undergo security training and a course on security awareness before they are granted access. For this, an annual refresher is necessary. If this refresher is not attended, the access is blocked. The access is initially determined during the recruitment process prior to assignment. Upon definition of a certain position within the organisation, the recruiting manager as well as HR determine the requirements regarding access level, security responsibilities and control which are necessary for the respective position. The Security Representative checks the access each year.

3.5 Incident Management

In order to be able to quickly react to security or data protection incidents, SWARCO Cloud Services has established a Privacy and Security Incident Response Team (PSIRT). The PSIRT processes all reports concerning data protection and security incidents and/or vulnerabilities. All information on a respective incident are gathered and fully documented after employment of the procedures.

3.6 Endpoint Management

All SWARCO employees as well as contractors/suppliers commissioned by SWARCO who have access to sensitive customer data are subject to the strict compliance with the security guidelines regarding the workplace computer security.

4 Physical security

When evaluating the Private and/or Public Cloud environments, SWARCO ensures that the IaaS provider follows relevant security rules regarding the physical access control and tracking. SWARCO can get those regulations confirmed by on-site controls, audits by third parties as well as certifications such as ISO27001, ISO9001 and SSAE16/SOC1.
Although these security rules may vary from provider to provider, the minimum specifications described below represent the requirements SWARCO Cloud Services demands from the providers.

4.1 Facilities

Data centres which store, receive or transmit sensitive customer data, are picked strategically to prevent high-risk events such as natural disasters, including risks of force majeure.

4.2 Physical access

SWARCO is obliged to implement processes and guidelines to protect all facilities and installations against physical access, sabotage or theft. The SWARCO guidelines regulate a limited and controlled access to facilities with information systems. This includes the access control of employees according to their function. This also includes visitor control.

4.3 Intruder detection system

By means of the implemented systems monitoring every access, the access to facilities containing sensitive customer data is allowed for authorised personnel only. If possible, the access is authorised by a multi-factor access control.
The data centres are furthermore protected by additional security systems to prevent unauthorised access such as:

- Surveillance cameras, CCTV (Closed-Circuit Television)
- …

4.4 Environmental Controls

Measurements are continuously made where computer systems and storage devices are housed in order to guarantee optimal conditions for computers regarding temperature and humidity. In order to minimise the risks of unfavourable climatic conditions, critical systems such as HVAC are used redundantly. The following controls were implemented to protect against fire and/or flooding, power outage and other environmental conditions which can lead to a failure of the services:

- Central alert system with direct communication with the emergency services
- Fire detection systems
- Fire extinguishing systems
- UPS
- Redundant construction of critical system components for the case of failover

Although a defense in depth concept is no guarantee that failure is excluded, the following regulations will ensure that availability is guaranteed at a reasonable degree. If business needs require further measures concerning availability, SWARCO Cloud Services can guarantee its ability to provide DR services.

4.5 Network communication

The facilities are designed in such way that they prevent impairments of the network concerning the integrity of data processing. In this regard, resistant technologies such as glass fibre or shielded cabling can be used. This can help in the elimination or reduction of impairments due to electrical noise, electromagnetic or other interference.
Critical network components are available in multiple form and are monitored and protected by security solutions such as firewall, host/network based IDS and anti malware solutions. All connections which are used to manage the systems are secured by private communication channels such as VPNs.

5 Logical security

5.1 System authentication

Every user receives his own password which is restricted to personal use. Service accounts are restricted to employees who need the access due to their role in the company. The accounts are checked at regular intervals in order to exclude unauthorised access.

In the framework of managing the account life cycle for all users, periodic checks are carried out. The process of providing the accounts is equally assumed by Human Resources and Cloud Services. Account requests are processed, checked and completed by means of a SWARCO Access Management solution. Every account request is documented in detail. In this regard, the account type and the resources for which access is granted are recorded.

5.2 Netzwork control

Access to the SWARCO system is restricted to users within the SWARCO network. After logging into the SWARCO network, the access is verified by a first authentication barrier. Furthermore, only devices approved by SWARCO are admitted to the SWARCO Cloud.

Only secure protocols are used for authentication vis-à-vis the information systems. Moreover, remote sessions time out at previously defined time intervals in order to guarantee that only authorised users access the systems. Remote sessions are encrypted to protect the confidentiality of the communication traffic.