SWARCO

CYBERSECURITY POLICY

FOR INTERNAL AND EXTERNAL USERS

The Better Way. Every Day. swarco

CONTENT

Introduction

The SWARCO Cybersecurity Policy for Internal and External Users is designed to provide you with information and guidance regarding different aspects of cybersecurity related to the interaction with SWARCO IT systems.

The information contained in this Policy applies to all SWARCO employees including vendors, consultants and agents operating on behalf of SWARCO and it is approved by the SWARCO Executive Board.

You are responsible for reading and complying with the provisions of this Policy.

Group IT will verify compliance to this Policy through various methods, including but not limited to, security tool reports, internal and external audits.

Any exception to any part of this Policy must be approved by Group IT. Group IT is responsible to include Group Legal Department and/or Group Compliance Officer for approval, if necessary.
The content of this Policy is considered binding in all its parts, unless expressly stated otherwise.

For purposes of this Policy, the definitions as stated in the glossary at the end of the document apply.

1 Roles and Responsibilities

1.1 SWARCO Group IT

SWARCO Group IT, the Information Technology department of SWARCO AG, is responsible for the basic strategic orientation of cybersecurity and IT systems within the SWARCO Group. Moreover, it is responsible for the creation and maintenance of the SWARCO Cybersecurity Governance. The SWARCO Cybersecurity Governance is the establishment of cybersecurity rules and standards, and its continuous monitoring of their proper implementation.
All tasks regarding new acquisitions, maintenance of software and hardware, network support, etc. must be coordinated with SWARCO Group IT.

1.2 Local SWARCO ITO

Each company has to define a person who is its designated Information Technology Officer (ITO). An ITO is the central contact person for SWARCO Group IT when interacting with different entities of the SWARCO Group.
The Managing Director (MD) of each company is responsible to hand over the SWARCO Cybersecurity Governance Policies and to ensure that they are implemented in their respective company.
The ITO shall serve as first contact person for all IT issues within its company as well as for the local partner companies.
The ITO shall ensure that necessary employee awareness regarding proper handling of PCs, mobile devices and data is created within the company in alignment with local management.
Employees are required to know who the person responsible within their company is. An up-to-date overview of all ITOs can be found at:
https://swarco.sharepoint.com/:x:/s/sbswattens/EUOtYYNCvn1LqzGZiafjdLgBlfTcizuWJW6tmrTJBjnX2A?e=Z9krQS

If your company is not listed in the overview, or some information needs to be updated, please send an e-mail to support@swarco.com to receive further information.

1.3 SWARCO Employees

Each employee must know and comply with his/her specific duties and responsibilities in the context of cybersecurity as defined in this document.

1.4 External partner companies and outsourcing

1.4.1 General principles

The topic of outsourcing (i.e. the outsourcing of work and business processes to external service providers, this can mean the use and operation of hardware and software as well as services) plays an important role because of the organizational form of the SWARCO Group.
In the case where local management outsources or decides to choose an external company for the maintenance of all or parts of its IT infrastructure (PCs, servers and network), their requirements shall be listed by the local IT team in coordination with SWARCO Group IT.
The uninterrupted operation of the IT systems has the highest priority. Any activities which interfere with this operation, especially during business hours, must be agreed upon with the respective department.

1.4.2 Responsibility of External Partners

Local management shall inform contracting partners and their employees about their duties regarding the cybersecurity requirements of the SWARCO Group.
If activities are directly linked to IT systems of the SWARCO Group (e.g. payroll accounting, SAP support, maintenance of the IT infrastructure, repair of IT hardware), these contracting

partners are obliged, to treat the information obtained as confidential (conclusion of a non-disclosure agreement). This Policy has to be disclosed to the respective partner companies in order to align to the current SWARCO cybersecurity standards. This should also be reflected in the respective contract. If personal data is processed, a contract regarding data processing might be necessary. In case of questions, please involve your internal data protection coordinator, or Group Legal, or your Data Protection Officer (DPO).

2 Internet and Email

The use of Internet and Electronic mail (email) is widely used within the SWARCO Group as the primary communication channel and method. Misuse of Internet and email can post many legal, privacy and security risks; thus, it is important to understand the appropriate use of electronic communication.

2.1 Scope and Purpose

2.1.1 This chapter applies to all SWARCO employees and to all external consultants.

2.1.2 The purpose of this chapter is to ensure proper use of the SWARCO Internet and email system and make users aware of what SWARCO deems as acceptable and unacceptable use of its email system. These are the minimum requirements for use of email within SWARCO.

2.1.3 Changes to configuration templates shall be coordinated, controlled and approved.

2.2 Internet

2.2.1 Access to the Internet is provided to the user for the purpose of supporting business activities necessary to carry out job functions.

2.2.2 All users must follow the SWARCO Code of Conduct (CoC) regarding of Internet usage. Please share this document with external partners. You may find this document on the SWARCO intranet website **https://swarco.sharepoint.com** under Documents > SWARCO Group Policies > Code of Conduct

2.2.3 Connections to the Internet are regulated by pre-configured security rules that filter traffic which might generate a risk for SWARCO. These rules include:

- Non-standard connections, connections that typically are not created by the user when, for example, he/she is browsing the Internet or sending email messages, are blocked by default.
- Preventing systems and applications from using Internet applications, which are considered as high security risk to the SWARCO Group. (i.e. applications that can be used by malwares, evade security devices, or known to contain vulnerabilities)
- Preventing systems and applications to connect to well-known Internet systems used to perform illegal activities.

  Preventing the user from accessing websites that, for example, provide or display content which intends harm to users or their computer systems or that contain instructions and information for how to commit illegal activities or exploit user computer security vulnerabilities.

2.2.4 The configuration of the Internet security rules may be changed according to the SWARCO business needs, at any time, and without notice.

2.2.5 Exceptions to these security rules may be requested, for business purposes, to the local ITO. The local ITO has to involve SWARCO Group IT, which will evaluate the possible exception and grant it or not.

2.3 Email

2.3.1 SWARCO email accounts must be used for SWARCO business-related purposes only; personal communication is not permitted.

2.3.2 All emails will be kept (retained) according to the applicable compliance and law regulations and can be used as SWARCO legal records, where required by the law.

2.3.3 All email communication must be in line with the SWARCO Code of Conduct (CoC).

2.3.4 For the sake of clarification, the SWARCO email system must not be used for the creation or distribution of any disruptive or offensive messages. These include offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or racial or ethnic origin or other inappropriate content such as pornography. Employees who receive any emails with such inappropriate or offensive content from any SWARCO employee shall report the matter to their supervisor immediately.

2.3.5 It is not allowed to alter electronic communications to hide one's identity or to impersonate another individual: this is considered misrepresentation and/or forgery. All email or any other form of electronic communication must contain the sender's real name and/or e-mail address. Exceptions do only apply if a user is authorized to send emails from a group address (e.g. info@swarco.com, group@swarco.com, etc.)

2.3.6 Use of SWARCO resources, including email, for anyone's personal or political gain is prohibited. This includes promoting personal services.

2.3.7 Users must not use third-party email and storage systems such as Google, Yahoo, GMX, etc. to conduct SWARCO business, to create or record any binding transactions or to store or retain email on behalf of SWARCO.

2.3.8 Sending chain letters or joke emails from a SWARCO email account is prohibited.

2.3.9 The use of SWARCO email accounts for registration of non-business-related online services or newsletters is prohibited.

2.4 Accounts and mailboxes

2.4.1 Only SWARCO employees are entitled to have an email address with SWARCO Group authorized domains, such as **@swarco.com**, **@swarco.de**, **@mccain-inc.com**, with the following format:

firstname.lastname@swarco.com

2.4.2 If needed, consultants and external personnel can have a SWARCO Group authorized domain email address with the following format:

ext.firstname.lastname@swarco.com

2.4.3 All mailboxes must be linked to a physical person, thus the creation of mailboxes for other purposes is prohibited.

2.4.4 Mailboxes such as info@swarco.com, office@swarco.com etc. must be created as shared mailboxes.

2.4.5 Shared mailboxes must be owned by at least two SWARCO employees.

2.5 Automatic and manual email forwarding

2.5.1 Users are prohibited from automatically forwarding SWARCO email to a third-party email system. Individual messages which are forwarded by the user must not contain SWARCO confidential information.

2.5.2 When necessary, emails can be automatically forwarded to external companies. In this case a Data Transfer Agreement must be in place between SWARCO and the company receiving the emails.

2.6 Using the email system

2.6.1 It is not allowed to use any other applications to access the email system except the SWARCO managed applications approved by Group IT and their web interfaces. These applications are normally installed in the user's computer, by default and a list can be found in this link: **https://swarco.sharepoint.com/sites/GIT/SitePages/Git-software.aspx**

2.6.2 Exceptions to this rule may be granted by the local management. However, Group IT cannot guarantee the functionality, neither can Group IT support these exceptions.

2.6.3 The standard email client (i.e. Microsoft Outlook), part of the SWARCO managed applications, uses predefined and approved protocols to communicate with the email system. The use of other protocols, such as IMAP or POP3, is prohibited.

2.6.4 The standard email client, sends and receives emails in a secure way: the communication with the email server is encrypted. Sending emails is only allowed using encrypted channels (i.e. SMTP over TLS).

2.7 Privacy and control

2.7.1 SWARCO employees shall be aware that SWARCO may access their emails and the email system only if, and as far as, allowed by applicable laws including data protection and privacy regulations.

2.7.2 In particular, SWARCO may, but is not obliged to, monitor messages without prior notice in the following scenarios:

- As per official request by legal and compliance authorities
- The user email account is suspected to be compromised
- During a security incident investigation

2.7.3 Incoming messages may be deleted by Group IT from the user mailbox, after their delivery, if a security threat is subsequently found.

2.8 Archiving

2.8.1 All incoming and outgoing email messages processed by the SWARCO email systems are automatically archived.

2.8.2 Archived email messages cannot be manually deleted by any user or administrator in the archive system.

2.9 Internal or external user contract termination

2.9.1 If an employee leaves the company, or the contract of an external consultant is terminated, Group IT or the local IT personnel has to be informed by local management. The respective accounts will then be disabled.

2.9.2 After an employee leaves the company, new email messages can be forwarded to the user's direct manager for 15 days. After this time period any incoming email message will be bounced back, and the sender will be automatically informed by the email system with a "user not existent" error.

2.9.3 The user mailbox must be saved for a period of maximum 30 days, from the date of termination. After this time the mailbox will be deleted from the email system. As mentioned in chapter 2.7 the emails will still be available in the archive system.

3 Password Protection

Passwords are an important aspect of security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources.

3.1 Scope and Purpose

3.1.1 All personnel, including SWARCO employees, contractors and vendors with access to SWARCO systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.1.2 The purpose of this chapter is to establish a standard for creation of strong passwords and the protection of these passwords.

3.2 Password Creation

3.2.1 All passwords must conform to chapter 4 (SWARCO Password Construction) of this document.

3.2.2 Users must use separate, unique passwords for each of their work-related accounts.

3.2.3 Users must not use any work-related passwords for their own, personal accounts.

3.2.4 User accounts that have administrative or system-level privileges, must have a unique password (different from all other accounts held by that user) to access non user-level privileges, unless other mitigating controls exist, such as security controls built into the operating system or authentication services.

3.2.5 Multi-factor authentication is required for any privileged accounts, where it can be enabled. This is normally carried out by Group IT, in SWARCO Group systems, or by the local IT personnel.

3.2.6 Devices must not be configured allowing logins without a password. Exceptions may be granted for specialized devices such as kiosks (computers that are configured to perform very limited functionalities) which use extremely restricted accounts.

3.2.7 All default passwords must be modified at installation to one that complies with this document.

3.2.8 Any pre-assigned passwords must be changed immediately upon initial access to any account.

3.2.9 The use of privileged accounts must be limited only to system administration activities.

3.2.10 Account and password management functions must be restricted to authorized personnel.

3.3 Password Change

3.3.1 Passwords must be changed whenever a system or account is suspected of being compromised, and the incident must be reported to it.security@swarco.com

3.3.2 Password change procedures must authenticate the user prior to changing the password. Acceptable forms of authentication include answering a series of specific

questions whose answers would not be known except by the user and/or trusted personnel, or showing one, or more, forms of photo ID, etc.

3.3.3 Password expiration mechanisms must be implemented for administrative accounts and shared accounts. This process must take into consideration a time period not lower than 180 days and any changes in the organizational structure (i.e. an administrator leaving the company)

3.3.4 Password audits or guessing may be performed on a periodic or random basis by SWARCO Group IT or its delegates. If a password is guessed during one of these scans, the user will be required to change it to be compliant with chapter 4 of this document.

3.3.5 For shared or service accounts, where the password is managed within a specified team, the password must be changed annually or when a member leaves the team. An individual employee must be designated to maintain the password and ensure that only authorized persons have access to the password.

3.4 Password Protection

3.4.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive and confidential.

3.4.2 Passwords must be stored in “password managers” programs authorized by Group IT.

3.4.3 It is not allowed to use the “Remember Password” feature of applications, such as web browsers.

3.4.4 Any user suspecting that his/her password may have been compromised must report the incident to **it.security@swarco.com** and change all passwords of all accounts.

3.4.5 Passwords must never be sent or stored in clear text.

3.4.6 Temporary passwords must be changed after the first login and these may be sent in clear text.

3.5 Multi-Factor Authentication

3.5.1 Multi-Factor Authentication must be used by all SWARCO Group authorized domains, such as **@swarco.com**, **@swarcod.de**, **@mccain-inc.com**, where applicable. For global systems, managed by Group IT, this feature is enabled by default, if possible.

3.5.2 Multi-Factor Authentication must be used whenever possible.

4 Password Construction

Passwords are a critical component of security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network.

4.1 Scope and Purpose

All personnel, including SWARCO employees, contractors and vendors with access to SWARCO systems, are responsible for taking the appropriate steps, as outlined below, to construct their passwords.
The purpose of this chapter is to provide best practices for the creation of strong passwords.

4.2 Strong passwords

Strong passwords are long, the more characters you have the stronger the password. Password must not be made of less than 8 characters. We recommend a minimum of 14 characters in users' passwords. Passwords must contain numbers, special characters and a change between capital and small letters. Systems may technically force users to comply with these requirements.

4.3 Passphrases

We highly encourage the use of passphrases, passwords made up of multiple words. Examples include:

- It's time for vacation 2020!
- Block-curious-sunny-leaves1
- Summer2020:here-I-come!

You can follow these steps for a secure, unique and noticeable password.

- Choose a passphrase: personal quote, chorus, slogan, motto etc. like "Billie Jean is not my lover."
- Use specific letters from the passphrase. "Billie Jean is not my lover." becomes "BiJeinml."
- An application code makes the password unique. For example, for Windows "BiJewininml."
- Add numbers and special characters like "BiJe$win#inml1"

Passphrases are both easy to remember and type, yet they meet the strength requirements.

4.4 Weak passwords

Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are similar to "Welcome123" "Password123" "Changeme123"

Weak passwords must be avoided at all costs!

4.5 Password Managers

In addition, every work account must have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of a “password manager” software that is authorized and provided by Group IT, if necessary.

4.6 Multi-Factor Authentication and passwords

As mentioned in chapter 3.5, it is required to enable Multi-Factor Authentication, whenever possible and supported, independently from the complexity of the chosen password.

5 Cloud Storage

Cloud storage is an essential tool to store documents effectively and securely. Therefore, SWARCO selected a cloud storage solution for its company data. The selection of the cloud storage technology took into consideration several aspects from a technical and legal point of view.

5.1 Scope and Purpose

All personnel, including SWARCO employees, contractors and vendors with access to SWARCO systems, are responsible to store SWARCO data only into the authorized technology. For more information, visit the following link: **https://swarco.sharepoint.com/sites/GIT/SitePages/Git-software.aspx**

The purpose of this chapter is to define current clear rules on how to use the cloud storage technology approved by SWARCO Group IT.

5.2 Requirements

- A Data Transfer Agreement (DTA) must be in place before any data is transferred to a cloud storage service. The approved cloud storage technology is already covered by a DTA.
- Cloud storage accounts must be protected with strong passwords (according to chapter 4 of this Policy).
- Multi-Factor Authentication must be provided by the cloud storage service to protect unauthorized access to SWARCO data. The approved cloud storage technology already meets this requirement.
- Only cloud storage services authorized by Group IT must be used to store SWARCO data. Any violation must be reported immediately to **it.security@swarco.com**

5.3 Data Security

5.3.1 SWARCO data must be transferred to and from the cloud storage service using a secure way (i.e. an encrypted channel). The provided technology and relative clients (i.e. Microsoft OneDrive), already cover this requirement.

5.3.2 It is strictly forbidden to transfer SWARCO data to a cloud service in cleartext (i.e. not using an encrypted channel or protocol, such as HTTPS or SFTP, while copying files). Exception to this rule are SWARCO public documents, such as SWARCO marketing material, etc. The selected cloud storage technology already meets this requirement.

5.4 Cloud storage service use

5.4.1 The use of the cloud storage service is limited to the storing of SWARCO data only.

5.4.2 The use of the approved cloud storage service for personal use is not allowed.

5.4.3 It is strictly forbidden to store any illegal or copyrighted material into the SWARCO authorized cloud storage service.

5.5 Data synchronization

5.5.1 The use of SWARCO accounts for data synchronization is only allowed from the cloud storage service to any SWARCO managed device.

5.5.2 Synchronize SWARCO data onto devices is only allowed when their storage memory is encrypted. Local management makes sure that users devices meet this requirement.

5.6 Data sharing

5.6.1 SWARCO data may only be shared with SWARCO employees or any other entities authorized to access this data (i.e. consultants, external providers, etc.). For more information contact your direct manager.

5.6.2 SWARCO data shared with unauthorized entities must be reported immediately to the it.security@swarco.com

5.6.3 It is strictly forbidden to create “public links” for SWARCO data, links accessible by anyone. SWARCO documentation created with the purpose to be public, such as marketing material, may be excepted from this rule.

5.7 Backup

5.7.1 SWARCO data stored in the approved cloud storage service is automatically and periodically saved by the approved backup system.

5.7.2 Users do not have access to the approved backup system. For more information contact your direct manager.

6 Remote Access

Remote access is the access of SWARCO systems and resources from outside of the SWARCO locations.

6.1 Scope and Purpose

All personnel, including SWARCO employees, contractors and vendors with access to SWARCO systems, are responsible to ensure that their remote access connection is treated as important as the on-site connection in the SWARCO office.
When accessing the SWARCO network from a personal computer, users are responsible for preventing access to any SWARCO systems by other persons. Performing illegal activities through the SWARCO network by any user is prohibited.
For further information and definitions, see chapter 8 (Acceptable Use) of this document.

The purpose of this chapter is to define rules and requirements for connecting to the SWARCO network from any system. These rules and requirements are designed to minimize the potential risk from damages which may result from unauthorized use of SWARCO resources. Damages include the loss of SWARCO data, intellectual property, damage to public image, damage to critical SWARCO internal systems, and fines or other financial liabilities as a result of those losses.

6.2 Requirements

6.2.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks - VPNs) and strong passphrases. For further information see chapters 3 and 4 of this document.

6.2.2 Users shall protect their account login and password from anyone.

6.2.3 Remote access must be approved in advance by the respective manager.

6.2.4 All systems connected to SWARCO internal networks via remote access technologies must use the most up-to-date anti-virus software and latest patches, this includes personal computers. SWARCO managed devices already meet this requirement.

6.2.5 Personal equipment used to connect to SWARCO networks must meet the requirements of SWARCO managed equipment for remote access. For more information please contact the local ITO.

7 Remote Access Tools

Remote desktop software, also known as remote access tools, provide a way for computer users and support personnel alike to share screens, access work computer systems from home, and vice versa. Examples of such software include, VNC (Virtual Network Computing) and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a risk to unauthorized access to the SWARCO network that can be used for theft or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools must be used on SWARCO systems.

7.1 Scope and Purpose

All personnel, including SWARCO employees, contractors and vendors with access to SWARCO systems, are responsible to ensure the use of approved tools for remote access.

This chapter defines the requirements for remote access tools used at SWARCO.

7.2 Requirements

7.2.1 SWARCO provides mechanisms to collaborate between internal users, with external partners, and from non-SWARCO systems. The SWARCO Approved Software list can be obtained from the **https://swarco.sharepoint.com/sites/GIT/SitePages/Git-software.aspx** web page. This web page contains, among other things, the list of approved software that can be safely installed and used without prior authorization.

7.2.2 All remote access tools must be approved by Group IT except the ones defined in the SWARCO Approved Software list.

8 Acceptable Use

8.1 Scope and Purpose

All personnel, including SWARCO employees, contractors and vendors with access to SWARCO systems, have to be compliant with the content of this chapter.
Customer systems and their related applications are out of scope.

This chapter defines what is considered “Acceptable” when using or accessing SWARCO resources.

8.2 General Use and Ownership

8.2.1 SWARCO data stored on electronic and computing devices whether owned or leased by SWARCO, the employee or a third party, remains the sole property of SWARCO.

8.2.2 Users must promptly report the theft, loss or unauthorized disclosure of SWARCO data, or any other security incident (such as if a user loses his/her company mobile phone or laptop, or if an email containing SWARCO data is sent to a wrong person). If personal identifiable information is involved, also the rules of your local Data Breach Policy have to be followed.

8.2.3 Users are only allowed to access or share SWARCO data to the extent they are authorized and it is necessary to fulfill the assigned job duties.

8.2.4 In the case of a security incident or for specific network maintenance purposes, authorized individuals within SWARCO may monitor equipment, systems and network traffic at any time.

8.2.5 SWARCO reserves the right to audit networks and systems on a periodic basis to ensure compliance with this document.

8.2.6 All portable devices (i.e. USB sticks) containing SWARCO data must use an approved method of encryption to protect SWARCO data at rest. For more information please contact the local ITO.

8.2.7 Users are expressly forbidden from storing SWARCO data on devices that are not approved by SWARCO or from applications not managed by SWARCO.

8.3 Security and Proprietary Information

8.3.1 Providing access to SWARCO data or resources to another individual, either deliberately or through failure to secure its access, is prohibited.

8.3.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. Users must lock the screen or log off when devices are unattended.

8.3.3 All postings from a SWARCO email address to newsgroups must comply with the CoC and Social Media Policy. You may find these documents on the SWARCO intranet website https://swarco.sharepoint.com under Documents > SWARCO Group Policies

8.3.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain harmful content.

8.3.5 All devices containing SWARCO data must employ full disk encryption with an approved encryption software. No SWARCO data must exist on any device in unencrypted format. Typically, this is addressed by IT personnel. For more information please contact the local ITO.

8.4 Unacceptable Use

The following activities are, in general, prohibited. For specific employees there may be exceptions from these restrictions during the course of their legitimate job responsibilities (e.g., system administration personnel may have to disable a system network access if that system is disrupting production services).
Under no circumstances is an employee of SWARCO authorized to engage in any activity that is illegal under local, state, federal or international law while using SWARCO-owned resources.
SWARCO reserves any and all rights to take any legal actions for any consequences resulting from unacceptable use.
The list below is by no means exhaustive. It attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

8.4.1 The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SWARCO.

8.4.2 Installation of any copyrighted software for which SWARCO or the end user does not have an active license is strictly prohibited.

8.4.3 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

8.4.4 Creating security breaches or disruptions of network communication.

8.4.5 Security scanning (i.e. port scans or vulnerability scans) unless prior notification and authorization from SWARCO Group IT.

8.4.6 To bypass or go around any user authentication or security of any system, network or account.

8.4.7 Introducing purposefully vulnerable systems (such as honeypots, honeynets, or similar technology) on the SWARCO network.

8.4.8 Interfering with or denying service to any user other than the employee's system (for example, denial of service attack).

8.4.9 Using any program/script/command with the intent to interfere with other employees or SWARCO systems.

9 Endpoint Security

9.1 Scope and Purpose

All SWARCO employees are responsible to be compliant with this chapter.

The purpose of this chapter is to regulate protection of the SWARCO systems when accessed by “Endpoint” equipment, such as desktop computers, laptops, tablets, mobile devices or similar.
The objective is to reduce the risk of security breaches that could result from the connection and use of Endpoint devices. This chapter seeks to limit security threats by:

- Ensuring employees are aware of the requirements and restrictions around Endpoint devices.
- Enabling protective measures and controls to manage Endpoint security and software compliance risks.

9.2 Endpoint Encryption

All Endpoints locally storing SWARCO data must be encrypted as described in the chapters before.

9.3 Endpoint Software

9.3.1 Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical and advisable to do so.

9.3.2 Endpoint OS and application software must be updated according to the following deadlines:

- Critical security patches are applied within 1 week from their release.
- Important security patches are applied within 8 weeks from their release.
- Endpoint systems must be restarted following a security patch installation, if an update requires to do.

9.3.3 Automatic updates shall be turned off on all Endpoint devices.

9.3.4 OS that reach end of support life are (i.e. Windows 7, old Android phones, etc.), are not permitted to connect to any SWARCO production system or network. If a special exemption is required, the manager responsible for the system must present a formal report documenting the system function, location, business software and responsible person to SWARCO Group IT. The local SWARCO entity will be in charge to the secure configuration and the implementation of this system.

9.3.5 Departments who choose to operate and manage their own specific software on Endpoint devices accept responsibility for the associated licensing, installation, updates, and security as it relates this software, in accordance with this document.

9.4 Endpoint devices management

9.4.1 Endpoint device management software shall be installed, as required, on any Endpoint connected to the SWARCO network.

9.4.2 Group IT will audit managed Endpoint devices and has the ability to:

- Install OS updates
- Install software updates
- Address software vulnerabilities or licensing issues
- Remove unlicensed or unauthorized software

9.4.3 The removing or disabling of Endpoint device management software without prior approval of SWARCO Group IT is prohibited.

9.5 Administrative Access

In accordance with the principle of least privilege, unnecessary administrative access on SWARCO owned Endpoint devices will be restricted.

9.6 Authentication

9.6.1 Endpoint devices containing SWARCO data must be secured via a password or a PIN according to the chapters 3 and 4 of this document.

9.6.2 For the scope of this chapter, Multi-Factor Authentication is currently not required to login into Endpoint devices such as Personal Computers or Mobile Devices.

9.7 Antivirus Software & Firewalls

9.7.1 All Endpoint devices capable of running an antivirus software program are required to do so before being connected to any SWARCO internal network or system. Additionally, any antivirus software must be running with the latest virus definitions to accurately detect the latest viruses and malware and be set to automatically update when newer definitions become available. Typically, this is the case for SWARCO Endpoints. For more information please contact the local ITO.

9.7.2 Disabling or removing of Antivirus software or disabling of Antivirus software definition updates on Endpoints is prohibited.

9.7.3 All Endpoint devices capable of running local Firewall software are required to do so to protect the device from external threats. Typically, this is the case for SWARCO Endpoints. For more information please contact the local ITO.

9.8 Personal devices

9.8.1 The security of personal devices (those not purchased or owned by SWARCO) that are authorized to connect to the SWARCO network remains in the responsibility of the owner and must comply with this document.

9.8.2 Personal devices that need to access and store SWARCO data must be managed by IT Personnel for all the relevant SWARCO managed applications.

9.8.3 The use of personal devices by SWARCO employees to conduct SWARCO business from non-managed SWARCO applications is forbidden.

10 Glossary

- **Administrator**

  A special role assigned to users which allows to change system or global settings of a computer or service.

- **Archiving**

  The act of automatically copying an email while it arrives to the email system and saving it in a specific system which will preserve it in an unchangeable (immutable) state.

- **Automatic email forwarding**

- A special mailbox rule that automatically copies and sends any incoming email to a different email address.

- **Cybersecurity**

  Cybersecurity is the protection of networks and computer systems from damage to their software or the data they process, as well as from interruption or misuse of the services and functions offered.

- **Data synchronization**

  The process of establishing consistency among data from a source to a target data storage and vice versa and the continuous harmonization of the data over time

- **Data Transfer Agreement**

  Agreement established between companies that governs the transfer of one or more personal data sets from the owner to a third party.

- **Exploitation**

  Taking advantage of a weakness or vulnerability in a system or process with the aim to disrupt, compromise, or breach any system or business-related service.

- **External partner**

  Any company which has a business relationship with SWARCO for supporting or maintaining its infrastructure or business-related functions.

- **Firewall software**

  Software used to block and regulate network access to and from a specific system.

- **Mailbox**

  A well-defined memory area in an email system where emails, appointments and other related data is saved.

- **Multi-Factor Authentication**

  An authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.

- **Permission levels**

  The authorization that a user has on a system while interacting with it. This can be granted by external mechanisms such as group memberships or programs such as the Linux “sudo” command. Examples of these permission levels are user-level, system-level, administrative-level.

- **Personal identifiable information**

  Any piece of information that relates to any identified or identifiable living individual.

- **Private encryption keys**

  A bit of code used in algorithms for text encryption and decryption.

- **Privileged account**

  A user account that has higher than normal authorization levels on a system.

- **Security incident**

  Any event generated by internal or external threats, aimed to disrupt, compromise, or breach any system or business-related service.

- **Security patches**

  A software update which includes code inserted into an existing program to remove any previously present security issues.

- **Security threat**

  Anything that can be or be used to disrupt, compromise, or breach any system or business-related service.

- **Service account**

  An account configured in a system typically to perform operations where human interaction is not needed.

- **Shared account**

  An account used by multiple users which share the same authentication login information.

- **SWARCO data**

  Any digital data and digital information collected, generated, received, owned or processed by or on behalf of SWARCO in connection with the operation of SWARCO Business.

- **SWARCO managed device**

  Any device which configuration and life cycle is managed by SWARCO.

11 Policy versions

Current Version	Published on	Supersedes	Approved by	Notes