SWARCO

# CYBERSECURITY POLICY

## FOR IT PERSONNEL AND DEVELOPERS

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 Acceptable Encryption

## 2.1 Scope and Purpose

2.1.1 This chapter applies to all SWARCO IT personnel and developers.

2.1.2 The purpose of this chapter is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

## 2.2 Algorithm Requirements

2.2.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the NIST publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

2.2.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

2.2.3 Signature Algorithms

| Algorithm | Key Length (min) | Additional Comment |
|---|---|---|
| ECDSA | P-256 | Consider RFC6090 to avoid patent infringement. |
| RSA | 2048 | Must use a secure padding scheme. PKCS#7padding scheme is recommended.<br>Message hashing is required. |
| LDWM | SHA256 | Refer to LDWM Hash-based Signatures Draft |

## 2.3 Hash Function Requirements

In general, SWARCO adheres to the NIST Policy on Hash Functions.

## 2.4 Key Agreement and Authentication

2.4.1 Key exchanges must use one of the following cryptographic protocols:

- Diffie-Hellman
- IKE
- Elliptic Curve Diffie-Hellman (ECDH)

2.4.2 Endpoints must be authenticated prior to the exchange or derivation of session keys.

2.4.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

2.4.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

2.4.5 All production servers and applications using SSL or TLS must have the certificates signed by a known trusted provider.

## 2.5 Key Generation

2.5.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

2.5.2 Key generation must be seeded from an industry standard random number generator (RNG).

# 3 Portable Devices Encryption

Portable devices such as laptops, smartphones and tables offer a great flexibility and improved productivity for employees. However, they can also create added risk and potential targets for data loss. As such, appropriate and state of the art standards and encryption technology should be used when possible.

## 3.1 Scope and Purpose

3.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

3.1.2 This chapter describes the information security requirements for encrypting data at rest on SWARCO portable devices.

## 3.2 General

3.2.1 All portable devices containing stored data owned by SWARCO must use an approved method of encryption to protect data at rest.

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

## 3.3 Laptops

3.3.1 Laptops must employ full disk encryption with an approved encryption software. No SWARCO data may exist on a laptop unencrypted.

## 3.4 Smartphones and Tablets

3.4.1 Any SWARCO data stored on a smartphone or tablet must be saved to an encrypted file system using SWARCO approved software.

3.4.2 SWARCO shall also employ remote wipe technology to remotely disable and delete any data stored on a SWARCO smartphone or tablet which is reported lost or stolen.

## 3.5 Encryption Keys

3.5.1 All encryption keys and passwords or passphrases must meet the complexity requirements described in the SWARCO Password Creation and Protection rules of the Cybersecurity Policy for Internal and External Users.

3.5.2 SWARCO data must be stored in any storage system or service in an encrypted form while at rest.

3.5.3 Private encryption keys may be managed by the cloud storage service.

3.5.4 In the case where private encryption keys are locally managed a strong secure key management program must be in place.

## 3.6 Loss or Theft

3.6.1 The loss or theft of any portable device containing SWARCO data must be reported immediately to the local ITO.

# 4 End User Encryption Key Protection

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

## 4.1 Scope and Purpose

4.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

4.1.2 This chapter outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

4.1.3 All encryption keys covered by this chapter must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

## 4.2 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in SWARCO Acceptable Encryption chapter of this document.

If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and that each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

## 4.3 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

## 4.4 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with the company PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local ITO or Group IT for secure storage.

The Group IT Security Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with the SWARCO Password Protection and Construction rules.

## 4.5 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

## 4.6 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

## 4.7 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in Portable Devices Encryption chapter of this document, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

## 4.8 Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in the SWARCO Password Protection and Construction rules.

## 4.9 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this document must be reported immediately to Group IT. Group IT personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

# 5 Audit

## 5.1 Scope and Purpose

5.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

5.1.2 This chapter is aimed to all systems owned or operated by Group IT or any other local SWARCO IT entity. It also covers any systems present on SWARCO premises, but which may not be owned or operated by SWARCO.

5.1.3 SWARCO hereby provides its consent to allow Group IT to access its systems to the extent necessary to allow Group IT, or any Group IT approved company, to perform scheduled and ad hoc audits of all systems at SWARCO.

5.1.4 The purpose of this chapter is to ensure all system deployed at SWARCO are configured according to the SWARCO Cybersecurity Policys or the relative cybersecurity standards. Systems deployed at SWARCO shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted in particular to:

- Ensure integrity, confidentiality and availability of information and resources and ensuring the resilience of the processing systems
- Ensure conformance to SWARCO security rules

## 5.2 Specific Concerns

Systems in use for SWARCO support critical business functions and store company sensitive information. Improper configuration of systems could lead to the loss of confidentiality, availability or integrity.

## 5.3 Requirements

5.3.1 All relevant logs shall be sent to a central log review system.

5.3.2 All “sudo” / administration actions must be logged.

5.3.3 Use a patch deployment system.

5.3.4 Host security agent such as antivirus shall be installed and updated.

5.3.5 Network scan to verify only required network ports and network shares are in use.

5.3.6 Verify administrative group membership.

5.3.7 Conduct baselines when systems are deployed and upon significant system changes

5.3.8 Changes to configuration templates shall be coordinated control and approved.

## 5.4 Responsibility

Group IT, any other local SWARCO IT entity, or any Group IT approved company, shall conduct audits of all systems owned or operated by SWARCO. Systems and applications owners are encouraged to also perform this work as needed.

## 5.5 Relevant Findings

All relevant findings discovered as a result of the audit shall be listed in the SWARCO tracking system to ensure prompt resolution or appropriate mitigating controls. The procedure for the audits is currently under definition.

## 5.6 Ownership of Audit Report

All results and findings generated by Group IT, or any Group IT approved company, must be provided to appropriate SWARCO responsible person within one week of project completion. This report will become the property of SWARCO and be considered company confidential.

# 6 Remote Access Tools Requirements

## 6.1 Scope and Purpose

6.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

6.1.2 The purpose of this chapter is to list all the requirements used for selecting remote access products.

## 6.2 Requirements

6.2.1 All remote access tools or systems that allow communication to SWARCO resources from the Internet or external partner systems must require Multi-Factor Authentication, where applicable. Examples include authentication tokens and smart cards that require an additional PIN or password.

6.2.2 Remote access tools must support strong, end-to-end encryption of the remote access communication channels. Please contact your local SWARCO ITO for more information.

6.2.3 All SWARCO antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

# 7 Compromised Account Procedure

Compromised accounts can generate a great security risk for SWARCO due to the impact that these have in the overall infrastructure. Once an account is compromised, the threat actor can, in fact, operate on behalf of the user, with all its authorization and have access to its data.
This means that this situation can also lead to a data breach of company or personal identifiable information.
For these reasons it is imperative that the security of these accounts is restored in a very short amount of time.

## 7.1 Scope and Purpose

7.1.1 The scope of this chapter applies to all SWARCO IT personnel.

7.1.2 The purpose of this chapter is to have a clear and pre-approved process to be executed when a SWARCO account has been identified as compromised.

## 7.2 MFA enabled

7.2.1 If the account has MFA enabled reset and send the password following the SWARCO Password Protection rules.

7.2.2 Initiate the sessions reset to kill all open sessions.

## 7.3 MFA not enabled

7.3.1 Reset and send the password following the SWARCO Password Protection rules.

7.3.2 Initiate the sessions reset to kill all open sessions.

7.3.3 Send the Endpoint Protection document, delivered during the rollout of MFA, explaining the user that, for security reasons, MFA will be enabled in his/her account.

7.3.4 Check if the user has a company mobile phone

7.3.5 If the user has a company mobile phone enabled MFA with the standard procedure.

7.3.6 If the user doesn't have a company mobile phone enable MFA and set it to call a provided telephone number.

## 7.4 MDM or MAM enabled

7.4.1 Check with the user if he used its SWARCO credentials to login into some websites or from non-company managed devices.

## 7.5 MDM or MAM not enabled

7.5.1 Send the Endpoint Protection document, delivered during the rollout of MDM/MAM, explaining the user that, for security reasons, MDM or MAM will be rolled out on his/her devices, if not already done in point 7.2.3

7.5.2 Check if the user has a backup of his data

7.5.3 Enroll the user's devices into MDM or MAM

## 7.6 Post-procedure tasks

7.6.1 Trace all emails sent within a week from the time the account was reported as compromised.

7.6.2 If any auto forwarding rules are present, check if the rules are legitimate otherwise delete them.

7.6.3 Check and track all the suspicious OneDrive for Business activities.

7.6.4 In case of suspected or confirmed data breach, follow the SWARCO Data Breach Policy.

## 7.7 Timing

7.7.1 This procedure must be executed within one (1) business day from the date the account was reported or discovered as compromised.

7.7.2 If the procedure cannot be executed within the specified time, the account must be disabled until the procedure is completed.

# 8 Router and Switch Security

## 8.1 Scope and Purpose

8.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

8.1.2 This chapter describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of SWARCO.

## 8.2 Device Access and authentication

8.2.1 No local user accounts should be configured on routers and switches. Routers and switches must use TACACS+ for all user authentication.

8.2.2 Fallback local users can be configured for emergency purposes when the connection to TACACS+ is not available. These users must never be used for normal operations and their password must be changed every 180 days.

8.2.3 The *enable* password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

8.2.4 Management access to network devices directly from the Internet or an insecure network is forbidden. In emergency situations the access can be temporary allowed.

8.2.5 Router console and modem access must be restricted by additional security controls such as:

- Network Access Control Lists
- User roles
- Multi-Factor Authentication, where applicable

8.2.6 Telnet may never be used across any network to manage a network device, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

8.2.7 Use corporate standardized SNMP community strings. Default strings, such as "public" or "private" must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

8.2.8 Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

8.2.9 Each device must have the following statement presented for all forms of login whether remote or local:

*"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged in accordance with the applicable data protection law and violations of this policy may result in disciplinary action and may be reported to law*

*enforcement. Please be aware that all commands will be logged. Use of this system shall constitute consent to monitoring."*

8.2.10 Each device must be included in the corporate enterprise management system with a designated point of contact.

## 8.3 Services configuration

8.3.1 The following services or features must be disabled:

- IP directed broadcasts
- Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
- TCP small services
- UDP small services
- All source routing and switching
- All web services running on the router or switch
- CDP and other discovery protocols on Internet connected interfaces
- Telnet, FTP, and HTTP services
- Auto-configuration

8.3.2 The following services should be disabled unless a business justification is provided:

- CDP and other discovery protocols
- Dynamic trunking
- Scripting environments, such as the TCL shell

8.3.3 The following services must be configured:

- Password-encryption
- NTP configured to a corporate standard source

## 8.4 Routing protocols and traffic management

8.4.1 All routing updates shall be done using secure routing updates.

8.4.2 Access control lists for transiting the device are to be added as business needs arise.

8.4.3 Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

## 8.5 The following device configuration settings may be required:

- IP access list accounting
- Device logging

# 9 Wireless Communication

## 9.1 Scope and Purpose

9.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

9.1.2 This chapter specifies the conditions that wireless infrastructure devices must satisfy to connect to SWARCO network. Only those wireless infrastructure devices that meet the standards specified in this chapter or are granted an exception by the Group IT Security team are approved for connectivity to a SWARCO network.

## 9.2 General Requirements

9.2.1 All wireless infrastructure devices that reside at a SWARCO site and connect to a SWARCO network, or provide access to information classified as SWARCO confidential, or above must:

9.2.1.1 Abide by the standards specified in the Wireless Communication Standard.

9.2.1.2 Be installed, supported, and maintained by the approved support team.

9.2.1.3 Use SWARCO approved authentication protocols and infrastructure.

9.2.1.4 Use SWARCO approved encryption protocols.

9.2.1.5 Maintain a hardware address (MAC address) that can be registered and tracked.

9.2.1.6 Not interfere with wireless access deployments maintained by other support organizations.

## 9.3 Lab and Isolated Wireless Device Requirements

9.3.1 All lab wireless infrastructure devices that provide access to SWARCO confidential or above, must adhere to section 9.2 above. Lab and isolated wireless devices that do not provide general network connectivity to the SWARCO network must:

- Be isolated from the corporate network (that is, it must not provide any corporate connectivity).
- Not interfere with wireless access deployments maintained by other support organizations.

# 10 Wireless Security Standard

## 10.1 Scope and Purpose

10.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

10.1.2 This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a SWARCO network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Group IT are approved for connectivity to a SWARCO network.

10.1.3 Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by Group IT or a Group IT approved support organization. Lab/development network devices must comply with the Lab/development Security chapter.

## 10.2 Standard

10.2.1 General Requirements

All wireless infrastructure devices that connect to a SWARCO network must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

10.2.2 Lab and Isolated Wireless Device Requirements

- Lab/development device Service Set Identifier (SSID) must be different from SWARCO production device SSID.
- Broadcast of lab/development device SSID should be disabled.

# 11 Lab and Development Environments

## 11.1 Scope and Purpose

11.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

11.1.2 This chapter establishes the cybersecurity requirements to help manage and safeguard lab/development resources and SWARCO networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

## 11.2 General Requirements

11.2.1 Organizations owning lab and development environments are responsible for assigning lab/developer managers, a point of contact (POC), and a back-up POC for each environment. Environments owners must maintain up to date POC information with Group IT. Environments managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

11.2.2 Lab/developer managers are responsible for the security of their environments and the impact on the corporate production network and any other networks.

11.2.3 Lab/developer managers are responsible for adherence to this chapter and associated processes. Where policies and procedures are undefined Lab/Dev managers must do their best to safeguard SWARCO from security vulnerabilities.

11.2.4 Lab/developer managers are responsible for the environment’s compliance with the SWARCO Cybersecurity Governance.

11.2.5 The Lab/developer, manager is responsible for controlling environments access. Access to any given system will only be granted by the lab/developer manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

11.2.6 All user passwords must comply with SWARCO's Password specifications.

11.2.7 Individual user accounts on any lab or development device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, Windows, etc.) must be changed quarterly (once every 3 months).

11.2.8 PC-based computers must have SWARCO's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up to date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab/developer Managers

are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

11.2.9 Any activities with the intention to create and/or distribute malicious programs into SWARCO's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use specifications.

11.2.10 No lab or developer environment shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a Group IT.

11.2.11 Immediate access to equipment and system logs must be granted to members of Group IT team upon request, in accordance with the Audit chapter of this document.

11.2.12 The Group IT Security Team will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

## 11.3 Internal Lab and Development environments Security Requirements

11.3.1 Group IT must maintain a firewall device between the corporate production network and all lab equipment.

11.3.2 Group IT reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

11.3.3 Group IT should record all lab networks, which are routed within SWARCO networks, along with current contact information for that lab.

11.3.4 Any environment that wants to add an external connection must provide a diagram and documentation to Group IT with business justification, the equipment, and the IP address space information. Group IT will review for security concerns and must approve before such connections are implemented.

11.3.5 All traffic between the corporate production and the lab/development networks must go through a Group IT maintained firewall. Lab/development network devices (including wireless) must not cross-connect the lab and production networks.

11.3.6 Group IT may require security improvements as needed.

11.3.7 Lab and development users/devices are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-SWARCO networks. These activities must be restricted within the lab or development environment.

11.3.8 Traffic between production networks and other networks, as well as traffic between separate networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Lab/development environments must

not advertise network services that may compromise production network services or put lab confidential information at risk.

11.3.9 Group IT reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

11.3.10 Lab/development owned gateway devices are required to comply with all SWARCO product security advisories and must authenticate against the SWARCO authentication systems.

11.3.11 Enable/root/admin passwords for all lab/development devices must be different from all other equipment passwords in the environment. Passwords must be in accordance with SWARCO's Password specifications.

11.3.12 Enable/root/admin passwords will only be provided to those who are authorized to administer the network/systems.

11.3.13 In environments where non-SWARCO personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no SWARCO confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by Group IT.

11.3.14 Lab/development networks with external connections are prohibited from connecting to the corporate production network or other internal networks through a direct connection, wireless connection, or other computing equipment.

## 11.4 DMZ Lab/Dev Environments Security Requirements

11.4.1 New DMZ lab/development environments require a business justification and a management approval from the business unit. Changes to the connectivity or purpose of an existing DMZ must be reviewed and approved by Group IT.

11.4.2 DMZ lab/development environments must be in a physically separate room, cage, or secured lockable rack with limited access. In addition, the lab/development Manager must maintain a list of who has access to the equipment.

11.4.3 DMZ lab/development POCs must maintain network devices deployed in the lab/development lab up to the network support organization point of demarcation.

11.4.4 DMZ lab/development environments must not connect to corporate internal networks, either directly, logically (for example, IPSEC tunnel), through a wireless connection, or multi-homed machine.

11.4.5 Group IT will maintain the firewall device between the DMZ lab/development environments and the Internet. Firewall devices must be configured based on least privilege access principles and the DMZ Lab/Dev environments business requirements. Original firewall configurations and subsequent changes must be reviewed and approved by Group IT. All traffic between the DMZ lab/development

environments and the Internet must go through the approved firewall. Cross-connections that bypass the firewall device are strictly prohibited.

11.4.6 All routers and switches not used for testing and/or training must conform to the Router and Switch standardization chapter.

11.4.7 Operating systems of all hosts internal to the DMZ lab/development environments running Internet Services must be configured to the secure host installation and configuration.

11.4.8 Remote administration must be performed over secure channels (for example, encrypted network connections using SSH or VPN) or console access independent from the DMZ networks.

11.4.9 DMZ lab/development devices must not be an open proxy to the Internet.

11.4.10 Group IT reserve the right to interrupt lab connections if a security concern exists.

# 12 Server Security

## 12.1 Scope and Purpose

12.1.1 The scope of this chapter applies to all SWARCO IT personnel and developers.

12.1.2 The purpose of this chapter is to establish standards for the base configuration of internal server equipment that is owned and/or operated by SWARCO. Effective implementation of this chapter will minimize unauthorized access to SWARCO proprietary information and technology.

## 12.2 General Requirements

12.2.1 All internal servers deployed at SWARCO must be owned by an operational group that is responsible for system administration.

12.2.2 Approved server configuration guides must be established and maintained by each operational group, based on business needs. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides. The following items must be met:

- Server contact and backup contact
- System location
- Hardware or environment (VMs)
- Operating System version
- Main functions and applications, if applicable
- Used network protocols and ports

12.2.2.1 Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

12.2.2.2 Information in the corporate enterprise management system must be kept up to date.

12.2.2.3 Configuration changes for production servers must follow the appropriate change management procedures

12.2.3 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit chapter.

## 12.3 Configuration Requirements

12.3.1 Operating System configuration should be in accordance with this Cybersecurity Governance.

12.3.2 Operating Systems that reach end of support life are by default not permitted to connect to any SWARCO production system. If a special exemption is required, the team manager must present a formal report documenting the system function, location,

business software and responsible person to Group IT. The local SWARCO entity will be in charge to the secure configuration and the implementation of this system.

12.3.3 Services and applications that will not be used must be disabled where practical.

12.3.4 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

12.3.5 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

12.3.6 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

12.3.7 Always use standard security principles of least required access to perform a function. Do not use root or “Administrator” when a non-privileged account will be sufficient.

12.3.8 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or VPN).

12.3.9 Servers should be physically located in an access-controlled environment.

12.3.10 Servers are specifically prohibited from operating from uncontrolled office areas.

## 12.4 Monitoring

12.4.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental backups will be retained for at least 1 month.
- Weekly full backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

12.4.2 Security-related events will be reported to Group IT, which will review logs and may report incidents to management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts

# 13 Policy versions

| Current Version | Published on | Supersedes | Approved by | Notes |
|---|---|---|---|---|
| | | | | |