SAP GLOBAL SECURITY (SGS)

GLOBAL SECURITY POLICY

Version Number: 1.3
Effective Date: April 6, 2020
Document Classification: INTERNAL | *Approved for distribution to External Parties under NDA or other appropriate confidentiality agreement.*

COVER SHEET

Objective	The objectives of the Policy are to define the high-level requirements for: • Preserving the confidentiality, integrity, and availability of information and assets. • Protecting all assets from threats, whether internal or external, deliberate or accidental, based on an assessment of risks to the organization. • Ensuring that legal, regulatory, operational, and contractual requirements are fulfilled.
Rationale	
Why – the benefits and strategy alignment	The responsibility for security ultimately resides with the SAP Executive Board but cascades to all personnel affiliated with SAP. An appropriate, up-to-date, global security policy defines the company-wide requirements for the protection of SAP's personnel, their work, and the information entrusted to SAP by its customers.
Risk of Non-compliance to SAP	Non-compliance results in an increased risk for SAP of financial impact, reputational loss, legal claims, loss of customers, and/or the prevention of new contracts. Non-compliance in audits (financial audit and/or security audit) may prevent or cause the loss of security certifications and/or attestations which further may cause loss of customers or the prevention of new contracts.
Applicability	
Primary group applicable to	This Policy applies to all businesses within SAP, all SAP employees, all External Parties granted access to SAP Information, and all information and assets owned by or administered by SAP.
Indirectly Affected Areas	None
Confidentiality	Internal
Enforcement	Violations of this Policy may lead to disciplinary sanctions in alignment with applicable labor laws up to and including the termination of employment.
Ownership	
Policy Owner	Chief Security Officer, SAP
Board Area	Office of the Co-CEO
Reviewers	This version 1.3 was reviewed by Daniel Fryer, Head of Security Policy, Standards, and Risk Management, on March 31, 2020 and contains a minor content revision to Version 1.2. Version 1.2 was reviewed by Tim McKnight, SAP Chief Security Officer, on May 30, 2019.
Approved by	This version 1.3 contains a minor content revision to Version 1.2 and was approved by Daniel Fryer, Head of Security Policy, Standards, and Risk Management, on March 31, 2020. Version 1.2 was approved by Tim McKnight, SAP Chief Security Officer, on May 30, 2019.
Document Information	
Master Document URL	This is the officially released version.
Release Date	April 6, 2020.

DOCUMENT IDENTIFICATION

Document Scope	SAP Global
Document Owner	Chief Security Officer, SAP
Review Cycle	Annual
Revision Table	Requests for the full revision table may be sent to SAP_Security_Policy@exchange.sap.corp.
Version Number	1.3
Effective Date	April 6, 2020
Status	Published

TABLE OF CONTENTS

1 INTRODUCTION

SAP is committed to ensuring a secure environment for our people, our information, our assets, and for the information entrusted to us by our customers and partners. We strive to maintain our security posture by leveraging industry standards and applying an informed risk-based approach to implementing a comprehensive and documented set of security controls. In doing so, we will continue to offer the level of security our customers are accustomed to from SAP and reinforce SAP's reputation as a trusted and secure business partner.

2 PURPOSE AND OBJECTIVES

The purpose of the **SAP Global Security Policy** (hereafter known as "this Policy") is to provide governance and structure for an appropriate and effective level of information security within SAP and its businesses. It establishes the strategic goals and objectives that SAP strives to maintain and is aligned with the overall SAP corporate strategy and vision.

The objectives of the Policy are to define the high-level requirements for:

- Preserving the confidentiality, integrity, and availability of information and assets.
- Protecting all assets from threats, whether internal or external, deliberate or accidental, based on an assessment of risks to the organization.
- Ensuring that legal, regulatory, operational, and contractual requirements are fulfilled.

3 SCOPE

This Policy applies to all businesses within SAP, all SAP employees, all External Parties granted access to SAP Information, and all information and assets owned by or administered by SAP.

4 REVIEW, UPDATE, AND MAINTENANCE

This Policy is a living document. It is subject to modification as needed to protect SAP as new threats and vulnerabilities are identified or the risk profile of the organization changes.

This Policy must be reviewed annually or sooner if significant changes occur. The review should include assessing opportunities for improvement to ensure this Policy's continued effectiveness and suitability.

SAP Global Security conducts annual reviews and updates the Policy's content. The content is approved by the members of the SAP Security Steering Committee.

Formatting, editorial, clarification, and minor content revisions are approved by the SAP Chief Security Officer.

5 EXCEPTIONS

SAP allows for exceptions to this Policy in specific circumstances where mitigating controls are implemented to reduce associated risk.

Each request must be submitted in writing via the SAP Global Security Policy mailbox at SAP_Security_Policy@exchange.sap.corp. Included in each request must be a statement detailing the business reasons for the exception, the potential risks, and the proposed measures to mitigate those risks.

Requests for an exception will be evaluated by SAP Global Security, including the appropriate subject matter experts, and the requesting party will be informed of the decision.

6 ENFORCEMENT

Violations of this Policy may lead to disciplinary sanctions in alignment with applicable labor laws

up to and including the termination of employment.

7 SUPPORTING DOCUMENTATION

This Policy is supported by various policies, standards, procedures, and guidelines. The following documents are specifically referenced in this Policy:

- SAP Global Information Classification and Handling Standard
- SAP Global Physical Security Standard
- SAP Global Risk Management Policy
- SAP IT Secure System Operation Standard
- SAP Mobile Device Security Procedure
- SAP Global Data Protection and Privacy Policy
- SAP Supplier Security Standard
- SAP Product Security Standard
- SAP Business Continuity and Operational Resilience Standard
- SAP Information Governance and Records Management Policy
- SAP Code of Business Conduct for Employees
- SAP Social Media Guidelines
- SAP Background Verification Process Guidelines

8 DEFINITIONS

Assets	Something of tangible or intangible value. This includes, but is not limited to, people, information, software, hardware, equipment, procedures, facilities, outsourced services, intellectual property, facilities, and networks.
Asset Owner	Person responsible for effective management of the asset over its lifecycle.
Availability	Ensuring timely and reliable access to and use of information by authorized entities.
Business Unit	Any SAP entity that may require additional security requirements unique to its business operations.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and propriety information.
Data Storage Device	Any device or unit that stores or carries data. This includes, but is not limited to, internal and external hard drives, backup media (such as tapes), removable media (such as flash drive or CD), and data stores in mobile devices.
End User Equipment	Client systems including: • Workstations: Stationary or desktop computers • Laptops: Portable computers • Mobile devices: Cell phones, PDAs, tablets, and other handheld devices
Ephemeral Messaging	Applications or services that cause sent messages or audio, video, and other files to automatically and irretrievably self-delete after a certain time or event (such as recognition by the recipient).
External Party	A third party who is granted access to SAP Information or assets. These third parties may be, but are not limited to, external workers, contractors, consultants, sub processors, customers, suppliers, or partners.
Information	Data with meaning and purpose that can exist in many forms, such as printed, hand-written, spoken, or electronically generated or stored.
Information Security	The combination of processes and controls implemented to protect information from various threats and ensure its confidentiality, integrity, and availability.
Integrity	Guarding against unauthorized modification of systems and information.

Intellectual Property	Patents, copyright, trade secrets, trademarks, and other intellectual and industrial property rights protected by applicable law.
IT System	Technology component. This includes, but is not limited to, end user equipment (workstations, laptops, mobile devices), server systems, network components, software containers, and virtualization infrastructure.
IT System Owner	Person responsible for IT systems operated in the SAP infrastructure.
Mobile Device	Cell phones, PDAs, tablets, and other portable handheld devices running a mobile device operating system that can store and process SAP Information.
Partners	Commercial entity with which SAP has a business alliance.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Principle of Least Privilege	The practice of limiting access to the minimal level that will allow normal functioning and the completion of a task.
Process	The act of accessing, altering, or transmitting information.
Removable Data Storage Device	USB/flash drive, CD, DVD, diskette, or any type of portable physical storage device that can be used to move information from one device to another. Also known as removable media.
Risk	Combination of the probability of an event and its consequences.
SAP Information	Information or data that has financial, competitive, or legal value to SAP or is entrusted to SAP by External Parties, such as customers or partners. This includes information or data that is created in the course of SAP business, stored or processed in SAP systems, created for SAP by others, or requires protection by SAP due to legal, contractual, or regulatory requirements.
SAP Network	The entire network resulting from the connection of multiple local networks via the WAN infrastructure. Within the SAP Network, there are various security zones that correspond to different security and risk levels.
Security Control	Security measure that mitigates risk.
Third Party System	An IT system or technical device owned by or administered by SAP partners, customers, or suppliers. The software installed on this system is not maintained or supplied by SAP IT.
Workstation	Stationary or desktop computer.

9 ORGANIZATION OF INFORMATION SECURITY

9.1 Information Security Roles and Responsibilities

The allocation of security responsibilities must be driven by business needs and aligned with the requirements of this Policy. Management may delegate security tasks to others; however, they remain accountable for the correct performance of the tasks. Conflicting duties and areas of responsibility must be segregated to reduce opportunities for modification or misuse of assets.

9.1.1 Executive Management

Members of executive management are responsible for:

- Ensuring this Policy, its purpose, and its objectives align with the strategic direction of the organization.
- Demonstrating leadership and support for this Policy.

- Showing commitment to preserving, accounting for, and continually improving the organization's security posture.
- Providing sufficient time, resources, and funding for required functions and programs.

9.1.2 Management

Members of management are responsible for:

- Ensuring this Policy and other applicable security policies and standards are implemented and enforced within their areas of responsibility.
- Identifying and addressing security risks per the *SAP Global Risk Management Policy* and applicable risk management standards.
- Providing employees in their area of responsibility with the appropriate levels of facility, system, application, and data access.
- Ensuring the appropriate user accounts are altered or disabled when an employee moves from the manager's area of responsibility or leaves SAP.
- Providing employees in their area of responsibility with all necessary security training at the time of hire and as required thereafter.

9.1.3 Employees

Employees are responsible for doing their part to protect SAP and its customers' and partners' information and assets by preventing unauthorized access and improper use. Employees are also responsible for:

- Understanding the purpose of information security and conforming to all appropriate security policies and standards.
- Properly classifying and handling SAP Information per the *SAP Global Information Classification and Handling Standard* to ensure the security of the Internal and Confidential information that they are processing or storing.
- Reporting security incidents or any issue relating to the protection or abuse of systems without delay pursuant to the incident reporting process.
- Complying with all applicable legislation or regulations that relate to their areas of responsibility.
- Completing the mandatory security awareness training.
- Ensuring they do not participate in activities that may inappropriately alter, change, delete, or use information or IT infrastructure belonging to SAP or its customers and partners.

9.1.4 External Parties

External Parties who are granted access to SAP Information and assets must sign an appropriate agreement to protect the privacy and confidentiality of SAP Information before they are granted access. These agreements include, but are not limited to, a non-disclosure agreement (NDA), Confidentiality and Privacy Statement (CPS), service agreement, or development agreement.

9.1.5 SAP Global Security

SAP Global Security is responsible for the protection of SAP's brand, people, assets, intellectual property, customer data, and information technology from misuse or compromise.

9.1.6 SAP Security Steering Committee

The SAP Security Steering Committee authorizes the contents of this Policy. The committee is comprised of senior leadership and executive board members.

9.2 Segregation of Duties

Adequate segregation of duties must be ensured to reduce the risk of fraud and misuse. Where segregation of duties cannot be applied, mitigating controls must be implemented.

9.3 Contact with Authorities

SAP Global Security must maintain contact with the relevant authorities in the information security area and share relevant information with affected business units and departments.

9.4 Contact with Special Interest Groups

SAP Global Security must maintain contact with suitable interest groups, professional associations, security forums, and other organizations as part of ongoing activities.

9.5 Information Security in Project Management

Information security must be addressed during all phases of project management to ensure that information security risks are identified and addressed. Risk assessments must be conducted during the early stages of projects.

10 RISK MANAGEMENT

Risk management must be embedded within management processes and applied consistently to ensure the proper level of security.

A security review process must be part of any system or application development to ensure that security controls are implemented within all new solutions.

A risk assessment must be conducted periodically to evaluate the potential risks to critical systems that contain Confidential SAP Information.

Further requirements for risk management and the responsibilities for risk management activities are defined in the *SAP Global Risk Management Policy.*

11 HUMAN RESOURCES SECURITY

11.1 Employment

Information security responsibilities must be communicated to all employees in contractual employment agreements.

11.2 Background Checks

All employees must be adequately screened following the *SAP Background Verification Process Guidelines* prior to employment in accordance with applicable legislation, regulations, and business requirements.

11.3 Termination or Change of Employment

Logical and physical access must be revoked or altered in a timely manner when an employee or external worker is terminated, transferred, or departs the company.

11.4 Information Security Awareness and Training

Information security responsibilities must be communicated to all employees and external workers who handle or process SAP Information via regular security awareness activities and training upon hire and annually thereafter.

12 MOBILE DEVICE SECURITY

SAP must manage the risks introduced by the use of mobile devices by implementing adequate controls to protect the SAP Information that is processed or stored.

All SAP owned and personally owned mobile devices that process or store SAP Information must be secured by an SAP IT mobile device management (MDM) solution.

Technical controls must be implemented to control access to SAP Information or data by unauthorized and/or unmanaged applications and software on mobile devices.

Further requirements for mobile devices are defined in the *SAP Mobile Device Security Procedure* and the *Acceptable Use Policy* contained in this document.

13 ASSET MANAGEMENT

SAP has identified and defined ownership and protection responsibilities for all its assets that are relevant in the lifecycle of information. This lifecycle includes the creation, processing, storage, transmission, deletion, and destruction of information.

13.1 Ownership of Assets

Asset owners must be identified and documented when SAP assets are created or acquired. Asset owners are responsible for assets throughout their lifecycle, including inventory, classification, handling, protection, management of access controls, and deletion or disposal.

13.2 Inventory of Assets

All SAP owned assets must be identified and documented in an inventory that is accurate, updated regularly, and reviewed at defined intervals. The inventory must contain each asset's classification level.

13.3 Acceptable Use of Assets

The requirements for the acceptable use of assets are defined in the *Acceptable Use Policy* contained in this document.

13.4 Return of Assets

Management must ensure that assets are recovered upon termination of employment or contract or when they are no longer required for business purposes.

13.5 Classification of Assets

13.5.1 IT System Security Classification

Each IT system must be classified as security-critical or non-security critical according to the criticality of the information stored or processed.

Further requirements for the classification of IT systems are defined in the *SAP IT Secure System Operation Standard.*

13.5.2 Information Classification and Handling

SAP Information must be classified as Confidential, Internal, or Public.

Information owners must classify SAP Information based on its sensitivity, criticality, legal requirements, and value. The information owner ensures that the information asset is appropriately labeled and protected based on its classification to prevent unauthorized access, disclosure, modification, removal, destruction, and improper use.

Access to SAP Information must be based on business requirements using the principle of least privilege. Information users who have been granted access to SAP Information are responsible for handling the information according to its assigned classification level.

Level	Definition
Confidential	Highly sensitive SAP Information that is accessible to only a limited number of specific individuals who have a defined "need to know." Includes information that SAP has a legal, regulatory, and/or contractual obligation to protect and information that qualifies as Personal Data in accordance with the *SAP Global Data Protection and Privacy Policy.*
Internal	Sensitive SAP Information that is accessible to SAP employees and authorized external workers, but all other access must be restricted and controlled.
Public	SAP Information that does not require special protection and may be publicly distributed.

Classification, labeling, and handling requirements are defined in the *SAP Global Information Classification and Handling Standard.*

13.6 Laptops and Workstations

All SAP laptops and workstations must be managed and secured by a central device management solution and have:

- An SAP corporate image.
- Encrypted data storage.
- A solution approved by SAP IT for encrypting data on removable data storage devices.

The requirements for the acceptable use of laptops and workstations are defined in the *Acceptable Use Policy* contained in this document.

13.7 Data Storage Devices

SAP Information stored on data storage devices must be protected from unauthorized disclosure, deterioration, modification, removal, and destruction.

13.7.1 Removable Data Storage Devices

Requirements for the use of removable data storage devices are defined in the *Acceptable Use Policy* contained in this document.

13.7.2 Deletion and Disposal

Data storage devices containing SAP Information must be deleted and disposed of using secure and validated processes that are suitable for the type of device and the sensitivity of the information contained.

The data contained must be suitably protected throughout the entire process. Data must be protected even after the device is no longer in use or if it will be used for a different business purpose. Data retention requirements must be considered.

13.8 Physical Media Transport

Physical media containing SAP Information, such as paper documents, DVDs, or removable media storage devices, must remain secure during transportation.

Data storage devices containing Confidential SAP Information must be encrypted using an internationally recognized procedure that is regarded as secure. Their transport must be documented and traceable. The decryption information must be transmitted using a different communication channel.

14 ACCESS MANAGEMENT

Access granted to SAP IT systems and the SAP Network requires the implementation of access controls that consider legislative and contractual obligations, security risk, and business requirements.

Formal processes must be established to:

- Prevent unauthorized access.
- Detail user access registration and deregistration.
- Detail user access provisioning.
- Restrict and control privileged access rights.
- Establish the intervals for user access rights reviews.
- Ensure removal of access rights upon users' termination of employment, contract, or agreement.
- Restrict and control the use of utility programs that can override system and application controls.
- Restrict access to program source code.
- Control access to systems and applications, where required, by a secure log on procedure.
- Hold all users of SAP systems accountable for safeguarding their authentication information.
- Ensure passwords meet established complexity requirements.
- Manage access for and ensure the secure registration of External Parties.

15 REMOTE ACCESS

SAP IT must define the requirements to manage the risks associated with working outside of SAP locations. Access to the SAP Corporate Network from remote hosts or networks must be restricted and controlled using defined two-factor authorization criteria and encrypted connections.

16 CRYPTOGRAPHY

16.1 Cryptographic Controls

SAP utilizes encryption to protect the confidentiality and integrity of SAP Information.

The use of encryption to protect Confidential SAP Information must follow industry standards and comply with customer contractual obligations and governmental import and export guidelines. All encryption procedures must be internationally recognized and regarded as secure.

16.2 Key Management

Cryptographic keys must be managed and protected throughout their lifecycle including their generation, storage, archival, retrieval, distribution, retirement, and destruction.

Further requirements for cryptography are defined in the *SAP IT Secure System Operation Standard.*

17 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical security measures must be implemented to protect people, maintain the integrity of building facilities and information processing centers, and control the unauthorized outflow of SAP Information and loss of assets.

The protection of human life has priority over all other security measures.

Protection measures provided must be proportional to the identified risks and the classification level and value of the assets and SAP Information.

Further requirements for physical security are defined in the *SAP Global Physical Security Standard* and the *Acceptable Use Policy* contained in this document.

18 OPERATIONS SECURITY

SAP must ensure the secure operation of systems to protect the confidentiality, integrity, and availability of the information it processes.

Formal processes must be established for the following:

- Documenting and maintaining operating procedures
- Change management
- Capacity management
- Separation of production and non-production environments
- Protection from malware
- Backup and recovery
- Logging and monitoring
- Clock synchronization
- Control of operational software
- Vulnerability management
- Systems audit considerations
- Installation of software

19 COMMUNICATIONS SECURITY

19.1 Network Security Management

Controls must be implemented to ensure the security of the SAP Network and the IT systems connected to it and protect information in transit from interception, alteration, and deletion.

Further requirements for network security are defined in the *SAP IT Secure System Operation Standard.*

19.2 Information Transfer

SAP must protect the transfer of information to ensure that the communication maintains its confidentiality, integrity, and availability during the entirety of its transmission. All IT systems are to be configured so that they use secure communication in accordance with the protection requirements of the transmitted information.

Further requirements for information transfer are defined in the *SAP IT Secure System Operation Standard* and the *SAP Global Information Classification and Handling Standard.*

19.2.1 Electronic Communication

SAP must implement appropriate controls to protect the SAP Information and data that is transmitted via electronic communication, such as email and messaging applications and software.

All third-party applications and software used to transmit or communicate SAP Information, data, or business-related communication must be authorized by SAP IT. SAP must ensure that data retention, data protection and privacy, and other applicable legal and regulatory requirements are considered as part of the authorization process.

All authorized applications and software used to transmit or communicate SAP Information, data, or business-related communication on a mobile device must be managed by an SAP mobile device management (MDM) solution.

Further requirements for electronic communications at SAP are provided in the *Acceptable Use Policy* contained in this document.

19.2.2 Information Transfer Agreements

The transfer of information between SAP and External Parties must be addressed in appropriate agreements, including any necessary data protection agreements.

Confidential and Internal SAP Information must not be disclosed to External Parties unless a non-disclosure agreement (NDA) or other appropriate confidentiality agreement is in place.

20 SECURE DEVELOPMENT AND ACQUISITION

Security must be integrated into SAP IT systems and applications throughout their development lifecycle. Requirements must be defined and implemented for maintaining the confidentiality, integrity and availability of the information contained during application and system risk assessment, planning, development or acquisition, modification, testing, validation, and response phases.

Further requirements for SAP developed applications are defined in the *SAP Product Security Standard.*

21 SECURITY IN SUPPLIER RELATIONSHIPS

All relevant suppliers, partners, and service providers to SAP are required to implement the security measures defined in contractual agreements when delivering services.

SAP must manage the risks associated with supplier access to the organization's information and assets by:

- Defining the security requirements within supplier agreements.
- Identifying the risks associated with the information and communication technology supply chain.
- Monitoring supplier service delivery.
- Managing changes to supplier services.

Further requirements for External Parties and suppliers are defined in the *SAP Supplier Security Standard* and the *SAP IT Secure System Operation Standard.*

22 SECURITY INCIDENT RESPONSE AND MANAGEMENT

Security incident reporting and management requirements must be defined and implemented to ensure a timely and effective response to security incidents.

These requirements must be documented, maintained, audited, and regularly tested. These requirements must include:

- Incident management responsibilities.
- Procedures for the collection and preservation of evidence.
- Processes for security incident reporting.
- Process flows for preparation, detection, analysis, containment, notification, eradication, and recovery.
- Post-incident activities to identify lessons learned.

Requirements for security incident reporting by employees are defined in the *Acceptable Use Policy* contained in this document.

23 BUSINESS CONTINUITY

SAP must maintain a business continuity management program to adequately ensure the continuation and restoration of business operations in the event of a disruptive incident. Business continuity at SAP encompasses disaster recovery, IT service continuity, process continuity, and crisis management. The program must:

- Identify critical assets.
- Define recovery timeframes.
- Address the requirements for asset protection.
- Maintain information security continuity.

Each business unit, IT service, and critical process must maintain a plan that provides the security requirements for protecting SAP Information and assets during interruptions to business operations. The plans must be documented, maintained, audited, and regularly tested in preparation for unforeseen threats to business operations.

Further requirements for business continuity are defined in the *SAP Business Continuity and Operational Resilience Standard* and *SAP Global Physical Security Standard.*

24 COMPLIANCE WITH SECURITY REQUIREMENTS

SAP must ensure compliance with organizational, regulatory, and contractual security requirements by subjecting its security and controls environment to periodic reviews.

24.1 Legal and Contractual Requirements

Contractual obligations and local and international legislation must be identified, documented, and adhered to in cooperation with the responsible SAP organizational units.

24.1.1 Protection of Records

Records must be protected from loss, destruction, deterioration, falsification, unauthorized access, and unauthorized release in accordance with legislative, regulatory, contractual, and business requirements.

SAP must define requirements for the retention, storage, inventory, handling, and disposal of records and SAP Information.

Further requirements for records protection are defined in the *SAP Information Governance and Records Management Policy.*

24.1.2 Data Protection and Privacy

SAP must ensure the protection and proper handling of the personal data it collects, processes, or uses.

The SAP Data Protection and Privacy Office (DPPO) ensures that SAP adheres to the applicable provisions of data protection and privacy law. Where applicable, local laws may require additional handling requirements.

Each employee is responsible for the secure handling of personal data, which may include customer and/or partner information.

Further requirements for data protection and privacy are defined in the *SAP Global Information Classification and Handling Standard* and the *SAP Global Data Protection and Privacy Policy.*

24.1.3 Intellectual Property

Procedures for the protection of intellectual property rights must be maintained per contractual obligations, local and international legislation, and regulations.

24.2 Information Security Reviews

24.2.1 Independent Review

Security related certifications and/or attestations provided by independent auditing organizations must be maintained.

24.2.2 Compliance with SAP Security Policies and Standards

Internal reviews of security controls must be performed to ensure compliance with SAP policies and standards. Any findings of non-compliance must be evaluated for corrective action.

24.2.3 Technical Review

SAP IT systems and networks must be regularly reviewed for compliance with technical security requirements.

Processes for conducting secure code reviews on SAP developed applications must be defined and adhered to.

Application and/or infrastructure penetration testing must be performed based on the application or infrastructure's sensitivity and criticality classification.

Periodic vulnerability scanning must be performed according to business requirements. Remediation of a vulnerability is based on the vulnerability's risk level and criticality. Applications and systems must be patched based on the criticality of the vulnerability. Critical vulnerabilities must be patched as soon as possible.

Further requirements for SAP developed applications are defined in the *SAP Product Security Standard.*

25 ACCEPTABLE USE POLICY

SAP defines the acceptable behavior and activities with regards to the use of SAP Information and assets. All SAP employees and External Parties who use, process, or otherwise handle SAP Information or assets are required to comply with the following requirements.

25.1 Prohibited Activities

The following activities are prohibited:

- Using any SAP IT systems, SAP Information, customer information, and/or partner information for any unauthorized use.
- Engaging intentionally in activities that could compromise SAP's, its customers', its partners', or its External Parties' security of information, IT systems, or networks.
- Engaging in any activity that is illegal under local, state, federal, or international law while using SAP resources.
- Violating the intellectual property rights of any person or company.
- Unauthorized attempts to change the security configuration of an SAP IT system or to bypass or deactivate the security restrictions to gain access to protected information or areas.
- Using SAP IT systems to download, store, or transfer offensive material. Offensive material includes material that is sexually explicit, abusive, discriminatory, racist, or defamatory.
- Using SAP IT systems to create, download, store, sell, distribute, copy, or exchange illegal, copyright-protected, or non-licensed software, information, music, or other multimedia files.
- Deliberately deleting or destroying SAP Information, communications, or records that are protected by the *SAP Information Governance and Records Management Policy*, the *SAP Global Data Protection and Privacy Policy*, or other legal and regulatory requirements.
- Using applications or software (including ephemeral messaging applications) that are not authorized by SAP IT to communicate on SAP business-related matters.
- Using any kind of tools, applications, devices, or exploits to access SAP Information in an unauthorized manner.

25.2 Personal Use of SAP Equipment

SAP end user equipment and voice communication equipment may be used for incidental personal use. Personal use of this equipment is governed by the same regulations as business use.

All use must adhere to the *SAP Code of Business Conduct for Employees* and the requirements for the handling of SAP Information as stated in the *SAP Global Information Classification and Handling Standard*.

Personal use of central IT systems or servers that are primarily used for the processing, mass storage, and exchange of SAP Information and data is not permitted. Personal files must not be stored on these systems.

Any personal use of SAP equipment must not negatively affect productivity, system availability, or performance.

25.3 Laptops and Workstations

25.3.1 Locking Laptops and Workstations

SAP laptops and workstations must be locked when left unattended (for example, using ⊞ + L to trigger the screen lock function on Windows computers), even if the device is only being stepped away from for a short time. The time-dependent lock of devices must not be deactivated.

25.3.2 Unauthorized Access

Unauthorized users must not be granted access to SAP laptops or workstations.

25.3.3 Security Updates and Patches

Security update distribution (patching) is an automated process. Security and operating system updates must be accepted on any SAP laptop or workstation. In addition, the update must be supported by rebooting the device.

25.3.4 Backup

SAP laptops and workstations must use the backup service provided by SAP IT. SAP Information must not be backed up to personally owned devices.

25.3.5 Software and Application Installation

All software and applications on SAP laptops and workstations must be obtained from an SAP IT software store or otherwise authorized by SAP.

Unauthorized or illegal copies of software on SAP laptops and workstations must be immediately deleted upon email notification from SAP IT.

25.3.6 Personally Owned Workstations and Laptops

Personally owned workstations and laptops must not be used to access and/or process SAP Information unless using external virtual desktop access approved by SAP IT. Personally owned workstations and laptops must not be used to export SAP Information from SAP systems and/or store SAP Information.

The use of personally owned mobile devices, such as smartphones or tablets, for SAP business is addressed elsewhere in this Policy.

25.4 Removable Data Storage Devices

Removable data storage devices may be used for SAP business to temporarily transport or backup information, but only if there are no other options available for this.

Confidential SAP Information stored on removable data storage devices must be encrypted using an SAP IT approved method. The transport must be documented, and the location of the devices must be known at all times. The information required for the decryption must be transmitted to the recipient using a different communication channel than that used for the removable data storage device.

Any removable data storage device used with SAP end user equipment or a personally owned mobile device used for SAP business must be from a known and reliable source.

25.5 Mobile Devices

Further requirements for mobile devices security are provided in the *Mobile Device Hardening Procedure.*

25.5.1 Use of Personally Owned Mobile Devices

Personally owned mobile devices are allowed for SAP business use if they are approved for use in the employee's country and are secured by the SAP IT mobile device management (MDM) solution.

Personally owned mobile devices used for SAP business must not be compromised (by actions such as jail-breaking or rooting).

Before disposing of or selling a personally owned mobile device that has been used for SAP business, all SAP Information must be deleted from the device or the device must otherwise be rendered permanently unusable.

25.5.2 Security Updates and Patches

Security and operating system patches and updates must be installed as soon as they are made available. Similarly, applications must be updated when updates are made available.

25.5.3 Software and Application Installation

Applications on SAP mobile devices or personally owned mobile devices used for SAP business must be obtained from official application store providers (such as Apple or Google Play) or from an SAP IT managed mobile application store.

All third-party applications and software used to transmit or communicate SAP data, information, or business-related communication must be authorized by SAP IT.

Unauthorized or illegal copies of software on SAP mobile devices must be immediately deleted upon email notification from SAP IT.

25.6 Hardware Procurement

SAP hardware must be ordered and obtained using the standard processes of SAP IT and the Global Procurement Office.

25.7 Protection Against Theft

Laptops, removable data storage devices, and mobile devices used for SAP business must not be left unattended in places where they can be easily taken.

The loss or theft of any of the aforementioned equipment must be reported immediately via the SAP Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

25.8 Protection Against Malware

25.8.1 Antivirus Software

Antivirus software must not be deactivated, interfered with, or reconfigured in any way.

Regular full virus scans or the automatic updating of the antivirus software should be allowed to run unhindered whenever possible. If the scan or update must be delayed for any reason, it must be resumed within 48 hours.

Users are responsible for notifying SAP IT Services if the antivirus software is not running or is otherwise interfering with work productivity.

25.8.2 Virus Scan of External Information

The virus protection software provided by SAP IT Services must be used to scan software, information, and media from external sources for viruses before using them.

25.8.3 Suspected Malware Infection

If there is a suspicion that SAP end user equipment or other SAP IT system has been infected with malware, the user must immediately report it via the SAP Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

25.9 Monitoring

Internet access and communications may be logged by IT for diagnostic, security, and billing purposes.

25.10 Travel Requirements

25.10.1 Possession of Devices and Information

SAP Information and equipment used to conduct SAP business, including, but not limited to, paper documents, laptops, mobile devices, and removable data storage devices, must always be kept in one's possession while traveling. The information and devices must not be checked in as luggage. The only exception to this is the existence of an airline or government regulation requiring that laptops be checked in as luggage.

The loss, seizure, or theft of the aforementioned information and devices must be reported immediately via the SAP Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

If customs personnel or other law enforcement officers request to decrypt an SAP laptop, removable data storage device, or mobile device used for SAP business, this incident must be reported immediately as a potential compromise of SAP Information via the SAP Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

25.10.2 Password and Web Browsers

Users are encouraged to clear web browsers after each travel session, including all history, cache, cookies, URLs, and temporary files.

Upon return from overseas travel, users are encouraged to change all passwords and PINs associated with the SAP laptop or mobile device used for SAP business.

25.11 Internet Use

Filters are set to prevent access to certain sites. However, if a user discovers they have connected to a website that contains sexually explicit, racist, or potentially offensive materials, the user must immediately disconnect from the site.

The use of Internet services to transmit, forward, or otherwise make, share, or promulgate information that could be detrimental to the interests or reputation of SAP is prohibited.

The use of any Internet services in any manner that contravene laws or regulations is prohibited.

25.12 Social Media

All use of social media is governed by the *SAP Social Media Guidelines*.

25.13 Communication

Further requirements for the communication of SAP Information are provided in the *SAP Global Information Classification and Handling Standard.*

25.13.1 Voice Communications

Conference bridges must be in an activated state only when in use.

All parties must be notified in advance whenever conversations are being recorded.

25.13.2 Voicemail

The mailbox PIN must be changed:

- When a voice mailbox is being used the first time.
- If there is reason to believe the PIN has been compromised.
- At regular intervals.

It is prohibited to leave Confidential and Internal SAP Information on answering machine or voice mail systems that are not known to be secure.

25.13.3 Faxes

Faxing of any SAP document must be in accordance with the requirements set forth in the *SAP Global Information Classification and Handling Standard*.

25.13.4 Electronic Communication

Each person is accountable for the activities and use of his or her assigned email or messaging account.

Electronic SAP data, information, and business-related communication must only be transmitted or communicated via:

- SAP provided email and messaging systems.
- Third party applications and software that are authorized by SAP IT.
- Customer initiated messaging systems that fulfill contractual obligations.

Further requirements for electronic communication are provided in the *SAP Global Information Classification and Handling Standard.*

Messaging Applications

The retention and deletion settings on any authorized third-party messaging or social media applications used for SAP business must be configured to retain messages in accordance with the *SAP Information Governance and Records Management Policy*, the *SAP Global Data Protection and Privacy Policy*, and other legal and regulatory requirements.

Further requirements for the handling of information in messaging applications are provided in the *SAP Global Information Classification and Handling Standard*.

Email

SAP email messages must not be automatically re-routed or forwarded to external messaging systems.

Caution must be used before opening attachments or hyperlinks from unknown senders.

It is prohibited to open, send, or forward any email attachments suspected of containing viruses or other contents that could result in damage for SAP or SAP's customers or partners.

Virus warning messages must not be forwarded to colleagues. Any concerns about virus messages should be submitted via to the Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

Email must be classified based upon the email's contents and attachments in accordance with the *SAP Global Information Classification and Handling Standard*.

25.13.5 Unacceptable Content

It is prohibited to use SAP email or messaging systems to send or respond to any communication that contains any of the following:

- Content that may be considered offensive, threatening, illegal or harassing, including but not limited to sexual comments or images, racial slurs, or other comments or images that would offend someone based on his or her race, national origin, gender, sexual orientation, religion, political beliefs, disability or other legally protected status.
- SPAM messages, chain mail, or pyramid schemes of any type.

25.14 Passwords

25.14.1 Password Requirements

All passwords or PINs are subject to the minimum requirements defined in the *SAP IT Secure System Operation Standard*.

25.14.2 Recommendations for Strong Passwords

Avoid using dictionary words in any language, slang, dialect, or jargon (even if spelled backwards or adding a digit or special character), such as secret1.

Avoid using personal information (including birthdates, names of family, or pets).

Consider basing passwords on the first letters of a song title, affirmation, or other phrase with numbers and special characters. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or similar.

25.14.3 Password Protection

SAP system passwords, Single Sign On (SSO) user certificates, PINs, or any other password used for SAP IT systems or applications must not be shared with anyone who is not explicitly authorized to access to them.

Passwords or PINs must not be written down on paper or otherwise stored in a readable form. Users are instead required to use a secure password management system.

If a password must be shared for a password-protected document or a demo system, the password must be sent separately from the document and other log-in information. Never include a password with the document or account it unlocks.

Password entry must not be bypassed with auto login, application remembering, embedded scripts, or hard-coded passwords in client software.

PINs and passwords must not be saved on public computers. In addition, browser caches and history must be cleared after disconnecting from computers accessible by others to prevent accidental transmission of passwords, PINs, and other log-in information to unauthorized individuals.

Do not use the same password for SAP accounts and personal accounts.

Passwords and PINs must be changed immediately if there is any reason to suspect that a password or PIN is no longer secure.

If a third-party requests one's password or PIN, the incident must be reported immediately as a security incident and a potential compromise of SAP Information via the incident reporting process.

25.15 Clean Desk and Clear Screen

All employees and External Parties must comply with the handling requirements for SAP Information as described in the *SAP Global Information Classification and Handling Standard*.

25.15.1 Paper Documents

Confidential SAP Information must:

- Be secured (for example, in a locked file cabinet, office, or storage area) when not in use.
- Be shredded or disposed of in a secure storage container if it is not to be used or archived. This includes intermediate work products related to information such as memos or drafts.
- Be generated in a hard-copy format only when necessary to complete normal business operations.

Confidential and Internal SAP information must not be left unattended on desks, tables, or printers.

25.15.2 Screens and Work Areas

SAP laptops and workstations must be locked manually when left unattended (for example, by using ⊞ + L to trigger the screen lock function on Windows computers). The screensaver must

be configured to automatically lock the screen with a maximum of five minutes of inactivity. This time-dependent lock of devices must not be deactivated.

Mobile devices that hold SAP information or that could provide access to another SAP device or IT system must be locked in a secure location, such as a file cabinet, closet, or desk drawer, when not in use.

25.16 Physical Security

All employees, External Parties, and visitors must comply with the following requirements:

- Badges shall be worn and clearly visible while on SAP premises.
- Badge holders must not use their badges to allow access for others.
- Tailgating is prohibited.
- Badge holders are required to use their badges at every card reader whether or not the door or gate is already open as they approach.
- Any lost or stolen badges must be immediately reported to SAP Global Physical Security.
- All visitors must always be escorted by their host while on SAP property and in restricted areas.
- Photography, filming, or recording on SAP property is not permitted without approval from SAP Global Physical Security.
- Movement of bulk items out of buildings requires an approved Equipment Removal Form.
- Combinations, codes, or personal identification numbers used for physical security must be changed every six months.
- Personal items, bags, briefcases, cabinets, and space assigned by SAP are subject to search based on probable cause and in accordance with applicable legislation and regulations.
- Weapons of any kind are prohibited on all SAP property unless such prohibition is contrary to local law.

25.17 Reporting Security Incidents

All actual or suspected security incidents must be immediately reported via the SAP Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

Security incidents include, but are not limited to, the following:

- Unauthorized physical access to a building or secure location, physical threat, imminent danger, or personal safety issues.
- Unauthorized access to electronic systems owned or operated by SAP or unauthorized access to Personally Identifiable Information (PII) stored on such systems.
- Malicious alteration or destruction of data, information, or communications.
- Unauthorized interception or monitoring of communications.
- Any deliberate and unauthorized destruction or damage of IT systems.
- A team or unit has not properly disposed of records containing PII on an individual.
- Equipment such as a workstation, laptop, CD-ROM, or other data storage device containing SAP Information has been lost, misplaced, or stolen.

25.18 Return of Assets

Upon termination or resignation, employees and external workers must return all SAP-owned assets. The manager is accountable for confirming that all assets have been returned. These assets include, but are not limited to, laptops, mobile devices, removable data storage devices, keys, badges, software, SAP Information, documentation, and manuals.