SAP GLOBAL SECURITY (SGS)

GLOBAL SECURITY STANDARD
Information Classification and Handling

Version Number: 2.1
Effective Date: April 6, 2020
Document Classification: INTERNAL

THE BEST RUN SAP®

DOCUMENT IDENTIFICATION

Document Scope	SAP Global
Document Owner	Daniel Fryer Head of Security Policy, Standards, and Risk Management
	Program Management and Communication
Review Cycle	Annual
Revision Table	Requests for the full revision table may be sent to SAP_Security_Policy@exchange.sap.corp.
Version Number	2.1
Effective Date	April 6, 2020
Status	Published

TABLE OF CONTENTS

1 INTRODUCTION

Information, defined as data with meaning and purpose, is an essential SAP asset. We must ensure the confidentiality, integrity, and availability of our information and the information entrusted to us by our customers and partners. Without these protections, SAP Information may be at risk and our organization's financial, competitive, or legal position may be negatively impacted.

SAP Information is 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 Information is classified as **Confidential**, **Internal**, or **Public**. Each classification level has corresponding handling requirements to direct individuals in the application of appropriate safeguards and security controls.

2 PURPOSE

This Standard provides the criteria and requirements for classifying and handling SAP Information based on its sensitivity, the associated level of risk, and the potential impact that may result from its unauthorized or inappropriate access, use, loss, modification, or disclosure.

3 SCOPE

This Standard applies to all business units within SAP, all SAP employees, all External Parties that access or handle SAP Information, and all information and assets owned by or administered by SAP.

The requirements in this Standard extend to all forms of SAP Information, including, but not limited to, paper documents, electronic data stored on systems and media, and information stored or processed in third party cloud applications.

4 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.
Availability	Ensuring timely and reliable access to and use of information by authorized entities.
Authorized External Worker	An External Worker who is engaged through the SAP External Workforce Center and has completed security awareness training, acknowledged relevant global policies, and signed an appropriate confidentiality agreement.
Business Unit	Any SAP entity that may require additional security requirements unique to their business operations.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and propriety information.
Data Storage Device	Any device or unit that stores or carries data. 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.
External Party	A third party who is granted access to SAP Information or assets. These third parties may be external workers, contractors, consultants, sub processors, customers, suppliers, and partners.

Identifiable Natural Person	One who can be identified, directly or indirectly, 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.
Information	Data with meaning and purpose that can exist in many forms, including printed, hand-written, spoken, or electronically generated or stored.
Information Asset	An asset that is associated with the access, processing, use, or storage of information.
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 improper information modification or destruction. Includes ensuring information nonrepudiation and authenticity.
Intellectual Property	Patents, copyright, trade secrets, trademarks, and other intellectual and industrial property rights protected by applicable law.
Need to Know	A legitimate and confirmed business need to access 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.
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.
Security Control	Security measure that mitigates risk.
Third Party Cloud Application	A third-party storage or collaboration application used to conduct SAP business.

5 ROLES AND RESPONSIBILITIES

5.1 Information Owners

Information Owners are typically business leaders or managers with the authority for acquiring, creating, and maintaining information and assets within their assigned area of control.

Information Owners are accountable for:

- Selecting the appropriate classification level for their information.
- Authorizing, reviewing, and revoking access to their information.
- Ensuring the appropriate confidentiality agreement is in place, if applicable.
- Ensuring data retention and archiving is appropriately managed.

Information Owners are also responsible for understanding the sensitivity of their information and whether additional approval (such as legal) is needed before authorizing its release.

5.2 Information Users

Information Users are individuals who are authorized to access, modify, delete, create, or otherwise handle SAP Information or information assets. They may include SAP employees and External Parties.

All Information Users are required to comply with this Standard. Persons to whom the information is forwarded or given are responsible for adhering to the information's protection and handling requirements.

Persons who receive information that they are not authorized to access must inform the relevant Information Owner or sender.

6 INFORMATION CLASSIFICATION

Information must be classified as **Confidential**, **Internal,** or **Public**, and appropriate access controls must be implemented. When combining information of differently sensitivities, the most restrictive classification level of the combined information asset must be applied.

6.1 Confidential Information

CONFIDENTIAL	
Classification Criteria	• **Highly sensitive SAP Information that is accessible to only a limited number of specific individuals who have a defined "need to know."** • Business critical or major damage could occur to SAP's financial, competitive, or legal position if unauthorized disclosure, compromise, or destruction occurs. • The following information is also **Confidential**: ✓ Information that SAP and Information Users have a legal, regulatory, and/or contractual obligation to protect. ✓ Information that qualifies as Personal Data in accordance with the *SAP Global Data Protection and Privacy Policy* and is subject to the additional protection and handling requirements defined in that Policy.
Access Requirements for SAP Employees/ Authorized External Workers	• Access must be restricted and controlled. • Information Owners may grant a limited number of specific SAP employees and/or Authorized External Workers access to the information if the individuals have a defined "Need to Know." • Legal, regulatory, and contractual requirements must be adhered to.
Access Requirements for External Parties	• Access must be restricted and controlled. • Information Owners may grant a limited number of specific External Parties (such as customers or partners) access to the information if the individuals have a defined "Need to Know." A valid non-disclosure agreement (NDA) or appropriate confidentiality agreement must be in place with the individual or their organization. • Legal, regulatory, and contractual requirements must be adhered to.

Guiding Questions	If the answer to any of these questions is "Yes", then the information is **Confidential**. 1. Is the information highly sensitive and must be accessed only by a limited number of specific individuals who have a defined "need to know?" 2. Is there a legal, regulatory, and/or contractual obligation to protect the information? *3.* Does the information contain Personal Data as defined in the *SAP Data Protection and Privacy Policy*? 4. Would unauthorized disclosure, compromise, or destruction of the information have a major impact to SAP in terms of finance, competition, and/or legal position?

6.2 Internal Information

INTERNAL	
Classification Criteria	• **Sensitive SAP Information that is accessible to SAP employees and Authorized External Workers, but all other access must be restricted and controlled.** • Moderate or some damage could occur to SAP's financial, competitive, or legal position if unauthorized disclosure, compromise, or destruction occurs.
Access Requirements for SAP Employees/ Authorized External Workers	• Access is unrestricted when used for SAP business purposes.
Access Requirements for External Parties	• Access must be restricted and controlled. • Information Owners may grant External Parties (such as customers or partners) access to the information. A valid non-disclosure agreement (NDA) or appropriate confidentiality agreement must be in place with the individual or their organization. • Legal, regulatory, and contractual requirements must be adhered to.
Guiding Questions	If the answer to any of these questions is "Yes", then the information is **Internal.** 1. Can SAP employees/Authorized External Workers access the information, but access by other External Parties must be restricted and controlled? 2. Does the information need to be secured from public access, but does not meet the criteria for a Confidential classification? 3. Would unauthorized disclosure, compromise, or destruction of the information have a moderate impact to SAP in terms of finance, competition, and/or legal position?

6.3 Public Information

PUBLIC	
Classification Criteria	• **SAP Information that does not require special protection and may be publicly distributed.** • Insignificant or no damage would occur to SAP's financial, competitive, or legal position if unauthorized disclosure, compromise, or destruction occurs. • Can be disclosed without violating an individual's right to privacy.
Access Requirements for SAP Employees/ Authorized External Workers	• Access is unrestricted.
Access Requirements for External Parties	• Access is unrestricted

6.4 Special Considerations

6.4.1 Email

An email's body content and its attachments determine the email's classification level. For example, an email address in an address field does not alone trigger a **Confidential** classification.

Emails containing **Confidential** information or **Confidential** attachments must be flagged in Outlook as "confidential" regardless of internal or external distribution.

6.4.2 Personal Data

Personal data is defined as:

> *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.*

In other words, Personal Data is any information that is related to an individual. The confidentiality of Personal Data is dependent on the processes in which the data is used. For example, the confidentiality of a letter or email is not based solely upon a name or address in the salutation or heading; it is based upon the total content of the letter or email.

The specific requirements for defining, processing, and Personal Data are provided in the *SAP Global Data Protection and Privacy Policy*.

7 POTENTIAL IMPACT

CLASSIFICATION LEVEL	RISK LEVEL	IMPACT LEVEL	Negative Impact on Confidentiality *Adverse effect of unauthorized disclosure of information*	Negative Impact on Integrity *Adverse effect of unauthorized modification or destruction of information*	Negative Impact on Availability *Adverse effect of disruption to access or use of information or an information system*
Public	Low	Insignificant /Minor	Negligible/None	Negligible/None	Negligible/None
Internal	Medium	Moderate	Some	Some	Some
Confidential	High	Major/ Business Critical	Significant	Significant	Significant

8 EXAMPLES

These information examples provide guidance for determining the classification of information assets. *This is not a comprehensive list of all SAP Information or information assets.* Information Owners must use the classification criteria to assign the appropriate classification levels to the information for which they are responsible.

8.1 Examples of Confidential Information

CONFIDENTIAL	
Information Type	**Examples**
SAP	• General ledgers • Integration process documents • Product design/functional requirements • Data files containing information protected by legislation/regulation • Marketing strategies • Customer terms and conditions • Draft and executed service level agreements • Third party and internal audit reports • Internal risk assessments and results • Vulnerability scan results • Security incident reports or related information • Business continuity and disaster recovery audits, plans, and reports • Non-public strategic information (pending merger, acquisition or divestiture plans) • Non-public financial information such as current or projected earnings, actual or contingent liabilities • Executive meeting notes and/or minutes • Planned management and organizational changes • Non-public information pertaining to corporate litigation • Trade Secrets • Pricing, product, service development information
Payment Card Industry (PCI) Data	• Primary Account Number • Cardholder Name • Expiration Date • Service Code • Full track data (magnetic-stripe data or equivalent) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks
Personal Data ***SAP Data Protection and Privacy Policy requirements apply***	• Name • Physical or Email address • Phone Number • Social Security Number • Individual Taxpayer Identification Number • Date of birth • Driver's license number • Age, sex, marital status or family status • Identifying number, symbol or other assigned to them • Disability • Offenses (including alleged offenses) • Criminal records • Data for uniquely identifying a natural person • Customer/supplier lists • Geo-location information

Sensitive Personal Data ***SAP Data Protection and Privacy Policy requirements apply***	• Race, national or ethnic origin • Religious beliefs or associations • Political opinions • Trade union membership • Genetic data • Medical or health information • Sexual orientation
Human Resources	• Salaries, bonuses, disciplinary actions, investigations or background checks • Information pertaining to incentive programs • Individual employee benefit selections • Executive succession plans • Employee performance reviews • Promotional information/metrics
Customer/ Partner	• Customer/supplier lists • Any information received under the terms of a confidentiality agreement • Data defined as confidential by a customer or partner
User Authentication	User name or ID in combination with: • Passwords • Information used to reset a password or validate a user's identity • Biometric data
Technology	• Non-ABAP® source code • Information pertaining to unmitigated security vulnerabilities • Encryption keys or passphrases • Security system configuration settings or parameters • Internal IP addresses

8.2 Examples of Internal Information

INTERNAL	
Information Type	**Examples**
SAP	• Statements of Work • Status reports • Policies and standards • Project plans
Customer/ Partner	• Presentations or documentation for customers and partners that do not meet the criteria for confidential but must not be made public. (This includes, but is not limited to, customer or partner-facing documentation that is uploaded to portals accessed by S-users). • SAP Notes • Marketing contact status
Human Resources	• Employee directory • Organization charts • Metrics and reporting status for employees/teams in operational processes • Employee training
Operational	• Procedures • Wiki Content

8.3 Examples of Public Information

PUBLIC	
Information Type	**Examples**
Application Documentation	• SAP Application Brochures • SAP Release Notes
Marketing/ Media	• Marketing brochures • Customer disclosure statements • Published interviews with the news media • Published press releases
Technology	• ABAP® Source Code

9 INFORMATION HANDLING

This Standard addresses information handling requirements from an information security perspective. Information handling may also be dictated by certain legal, contractual, or regulatory requirements. In addition to the handling requirements listed below, the following SAP policies must be adhered to:

SAP Business Code of Conduct for Employees
SAP Global Data Protection and Privacy Policy
SAP Communications Policy

The handling requirements that apply to SAP employees also apply to Authorized External Workers.

	Handling Requirement	Confidential	Internal	Public
Email to SAP Employees	Tag in Outlook as "confidential."	X		
	Ensure Information Owner has authorized the recipients' access to the content and attachments.	X		
	Use SAP provided email services only.	X	X	
	Ensure email addresses are not inadvertently selected.	X	X	
	Review content and attachments to ensure appropriateness.	X	X	X
Email to External Parties	Tag in Outlook as "confidential."	X		
	NDA or confidentiality agreement with External Party organization must be in place.	X	X	
	Ensure Information Owner has authorized the recipients' access to the content and attachments.	X	X	
	Use SAP provided email services only.	X	X	
	Ensure email addresses are not inadvertently selected.	X	X	
	Review content and attachments to ensure appropriateness.	X	X	X
Communication/ Messaging Applications	Limit group or channel members to only those individuals with a defined "need to know" the information discussed.	X		
	Limit group or channel External Party members to those who are authorized to access the information discussed.	X	X	
	Use only applications provided or approved by SAP IT or customer initiated messaging systems that fulfill contractual obligations.	X	X	
Shipping/Mail to SAP Employees	Ensure Information Owner has authorized the recipient's access to the information.	X		
	Securely seal the package.	X		
	Deliver directly to the recipient or authorized representative. Use SAP in house mail services only when direct delivery is not possible.	X		
	Use SAP in-house mail services or deliver directly to the recipient or authorized representative.		X	
Shipping/Mail to External Parties	Delivery confirmation is required.	X		
	NDA or confidentiality agreement with External Party organization must be in place.	X	X	
	Ensure Information Owner has authorized the recipient's access to the information.	X	X	
	Package in sealed, secure, tamper-resistant envelopes.	X	X	
Paper/Hard Copies	Print only when necessary.	X		
	Secure when not in use whether inside or outside of an SAP facility.	X		
	Do not leave unattended on desks, tables, or printers.	X	X	
	Secure when not in use while outside of an SAP facility.	X	X	
	Use dedicated containers for secure disposal. When possible, use shredders.	X	X	
Faxing to SAP Employees	Ensure Information Owner has authorized the recipient's access to the information.	X		
	Confirm that the recipient received the document.	X		
	Original documents must not be left unattended on fax machine.	X	X	
	Use a corporate fax cover page that includes the classification level.	X	X	X

	Handling Requirement	Confidential	Internal	Public
Faxing to External Parties	Ensure Information Owner has authorized the recipient's access.	X	X	
	Confirm that the recipient received the document.	X	X	
	NDA or confidentiality agreement with External Party organization must be in place	X	X	
	Original documents must not be left unattended on fax machine.	X	X	
	Use a corporate fax cover page that includes the classification level.	X	X	X
Copying/ Scanning	Scanned documents automatically saved to a network drives must be immediately deleted by the individual responsible for scanning.	X		
	Original documents and copies must not be left unattended on copier.	X	X	
Data Storage	Access to the information must be restricted to authorized individuals with a "Need to Know."	X		
	Storage is only permitted on SAP owned workstation or laptops, SAP owned mobile devices, or personally owned mobile devices managed by an SAP mobile device management solution. SAP Information must not be stored on a personally owned workstation or laptop	X	X	
External Cloud Storage	Access to the information must be restricted to authorized individuals with a "Need to Know."	X		
	Access is only permitted via SAP owned workstations or laptops, SAP owned mobile devices, personally owned laptops or workstations using external virtual desktop access approved by SAP IT, or personally owned mobile devices managed by an SAP mobile device management solution.	X	X	
	Storage is only permitted on solutions approved by SAP IT.	X	X	
Removable Data Storage Devices (Removable Media)	Must be encrypted for physical transport. The decryption information must be transmitted using a different communication channel. The transport must be documented and traceable.	X		
	Customer information is prohibited from being stored on removable data storage devices.	X		
	Secure when not in use whether inside or outside of an SAP facility.	X		
	Secure when not in use while outside of an SAP facility.	X	X	
	Must be sanitized appropriately by overwriting or degaussing prior to disposal.	X	X	
	Must be secured for physical transport.	X	X	
Workstations and Laptops	Access to SAP Information is only permitted via SAP owned workstations or laptops or via personally owned workstations or laptops using external virtual desktop access approved by SAP IT.	X	X	
	Storage of SAP Information is only permitted on SAP owned workstations or laptops. SAP Information must not be stored on a personally owned workstation or laptop.	X	X	
	SAP laptops and workstations must be locked when left unattended (for example, using ⊞ + L to trigger the screen lock function on Windows computers).	X	X	X
Mobile Devices	Access to or storage of SAP Information is only permitted on SAP owned mobile devices or personally owned mobile devices managed by an SAP mobile device management solution.	X	X	
	Devices used for SAP business must not be left unattended.	X	X	
Voice	Ensure that unauthorized persons nearby cannot follow your conversation.	X	X	
	Do not leave information on an answering machine or voice mail system that is not known to be secure.	X	X	

10 INFORMATION LABELING

10.1 Classification Levels

Labeling is the practice of marking information with its classification level so that others know how to properly handle the information.

Information Owners are required to label all **Confidential** and **Internal** information with the appropriate level.

- On paginated documents, label every page of the document regardless of its format (printed, handwritten, or electronic).
- On non-paginated documents (for example, web pages), place the label near the title of the document or at the top of the first page.

When feasible, Information Owners are encouraged to label **Public** information.

10.2 Optional Authorized Recipient Groups

An optional best practice is to append the authorized recipient groups to the **Confidential** or **Internal** label. This practice provides a way for the Information Owner to:

- Specify the authorized recipients for **Confidential** information.
- Grant access to specific External Parties for **Internal** information.

The actual verbiage used to describe the authorized recipient group is at the discretion of the Information Owner; however, proper names (in other words, first names or last names) and Personal Data must not be used.

Some examples of this optional best practice are:

- Confidential: SAP Executive Board Members only
- Confidential: SAP Customer Project XYZ only
- Internal: SAP Employees and External Workers
- Internal: SAP Customers
- Internal: SAP Partners

Additionally, SAP IT offers a solution in Microsoft Office that may be used to identify an authorized recipient group by appending a pre-defined sub-label to a classification level label. (This solution may not be available on all operating systems.)

The handling and access requirements defined in this Standard for each classification level apply regardless of the appended verbiage used. The appended verbiage must only be used to indicate the authorized recipient groups and must not be used to alter, add, or delete other requirements. For example, appended verbiage must not be used to alter the requirement that all External Parties must have an NDA or appropriate confidentiality agreement must in place.

If the Information User wishes to distribute outside of the identified authorized recipient group or if the appended verbiage is unclear, the Information Owner must be contacted for authorization.

11 SECURITY INCIDENT REPORTING

If **Confidential** or **Internal** information of any kind is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of SAP Information assets or systems has taken place or is suspected of taking place, the incident must be reported via the Global Security Incident Management (GSIM) tool on the SAP Corporate Portal.

12 GOVERNMENT CLASSIFIED INFORMATION

Government Classified Information is any information classified according to laws or regulations that requires additional protection of confidentiality, integrity, or availability. It is typically marked with one of several levels of sensitivity, such as **restricted**, **confidential**, **secret,** or **top secret**. Access is restricted by law or regulation to officially authorized people. Unauthorized access or disclosure can incur criminal penalties and loss of reputation for SAP. A formal security clearance is a mandatory prerequisite to view, access, process, or store government classified documents. The clearance process is usually owned by a dedicated government body and executed together with a commissioned SAP Secrecy Officer.

Anyone who encounters Government Classified Information or requests for any related security clearance, (for example, during customer engagements within highly regulated or security sensitive industries such as Defense, Defense Suppliers, Public Sector, or customers providing critical infrastructure customers) must involve the SAP Secrecy immediately. Address an email to: secrecy@sap.com.