Security Recommendations from SAP

SAP’s Standards, Processes, and Guidelines for Protecting Data and Information

Table of Contents

The Best-Run Businesses Run SAP®

Security as a Top Priority at SAP

Sophisticated business software doesn't have to be complicated. At SAP, we believe in keeping it simple, smart, and secure. And it's true: the success of many organizations facing the challenges of the digital transformation today depends to a large extent on flexible business solutions, high-performance industry software, and smoothly functioning information technology. Success also depends on the measures taken to secure those systems on which your businesses rely.

The role of IT is to gather, store, analyze, process, and prepare information from across the entire organization so your employees have the best possible information available at all times to make the best decisions. IT, and enterprise resource planning software in particular, plays a vital role in making your organization more transparent and efficient – so it can realize growth potential and generate real added value.

In a clear trend, companies are networking ever-more intensively – both internally and with their business partners. This, in turn, requires increasingly integrated IT systems. Almost every employee now has access to the Internet at the workplace, while many access their company's applications via mobile devices. At the same time, the key role that IT systems play in the running of an organization also increases the damage that can be done if data falls into the wrong hands or is manipulated.

Maintaining the security of data and information has become extremely important. As with material assets, companies must ensure that necessary safeguards are in place to protect their data and information. Safeguards include monitoring access to buildings and data centers, configuring, maintaining, and updating applications, and agreeing to rules among employees and business partners on the release and confidentiality of data.

Legal frameworks may also change, imposing elaborate and extensive conditions on companies. For example, the German Federal Data Protection Act amended in 2009 stipulates several things: Not only are companies responsible for implementing data protection requirements within their own organizations, but they must also enter into the necessary contractual agreements with all of their vendors. And they must be satisfied that such vendor agreements are being upheld.

As a world market leader in enterprise-class solutions, SAP provides business-critical software solutions to more than 296,000 customers worldwide. We work very closely with our customers by providing long-term software maintenance services, including those for their business-critical software systems. Thus, SAP employees have access to sensitive customer data, such as personnel data or mission-critical information.

In a clear trend, companies are networking ever-more intensively – both internally and with their business partners. This, in turn, requires increasingly integrated IT systems.

For this reason, we often are asked how SAP helps ensure that the software systems, information, and data of our customers are fully protected. Here we answer these questions with a clear overview of the security standards used at SAP, the various measures taken, and the precautions we take to guarantee the security of our customer data.

OBJECTIVES

We set out to explain the existing security standards at SAP and to make our working methods, guidelines, and processes more transparent for customers with regard to security and data protection. We aim to comprehensively answer the many questions you may have surrounding this important topic, not least in order to simplify and streamline the auditing process that new legal requirements impose on many customers.

Our intention is to make the wealth of information on this complex subject as clear and succinct as possible. We welcome your thoughts and feedback. Please send your questions and comments to info@sap.com with the subject header "Service & Support Security."

CONTENT AND STRUCTURE

In this document, we outline the measures and standards that SAP uses to protect information and data. This includes standards used throughout SAP worldwide, as well as specific regulations that apply to SAP organizations involved in the provisioning of service and support. A wide range of information is detailed in the following sections:

- **General Security at SAP:** This section provides information about general measures and standards valid for all departments and business areas within SAP. We also outline how we continuously evaluate and develop these security standards and measures and modify them to meet new challenges. In particular, we focus on requirements for personnel, access to buildings, access to data systems, and requirements for IT security.
- **Security Management at SAP:** We explain how a framework of management systems and methods helps ensure that SAP is always ready to meet new requirements. We explore how we enable our standards and measures to be rigorously executed in practice. This section includes both an outline of our internal guidelines and the underlying organizational structures.
- **Security in the Digital Business Services organization:** Here we discuss the measures employed within SAP organizations especially for the protection of customer information and data.
- **Appendix:** This section contains information to help you better understand the topic of security at SAP, including information on certifications, useful links, and frequently asked questions, where we provide answers to common questions related to employees, facility access, IT security, and other relevant security information.

General Security at SAP

ESTABLISHING HIRING REQUIREMENTS FOR PEOPLE

The data protection concept for SAP employees is broken down into three phases: application and recruitment, ongoing employment, and departure from the company.

Before SAP hires an employee, a rigorous application and recruitment process is conducted, in which the technical qualifications and the character of the applicant are matched against the profile for the position. For roles that involve a high level of responsibility for data and process security, SAP places particular emphasis on determining that applicants have the right character profile. Each employee is made explicitly aware of the data protection guidelines and the SAP security policy in their individual employment contract. Each employee also signs our "Code of Business Conduct," which governs general conduct throughout the organization. We also instruct employees in the internal data protection guidelines and general security provisions.

Immediately following their employment, new employees receive intensive induction training, which covers topics such as security and data protection. SAP provides mandatory refresher courses on a regular basis.

If an employee leaves SAP, all authorizations for accessing information or systems are revoked. If an employee switches to a new organizational unit within SAP, rights and role-based access rights are adjusted in accordance with the new function. Following the end of employment, employees must return to SAP all security-relevant equipment such as PCs, laptops, keys, and encryption cards for remote access. On leaving the company, employees are bound not to discuss any information obtained during their employment with SAP and to treat all such information as confidential.

ACCESSING AND PROTECTING OUR BUILDINGS

The protection of all facilities and buildings is of vital importance to SAP. Therefore, all facilities worldwide are classified according to a global security structure. This structure defines the security levels and the specific security requirements that apply to such facilities.

In general, all buildings are protected by access controls using access control systems that are supported by radio frequency identification, or RFID. Regardless of their security classification, all buildings also are guarded by security personnel or other security measures. These can include measures from specific access profiles, video-monitoring systems, and anti-intruder systems through to biometric access control methods and proximity security systems. We use special security measures such as these latter systems, for example, in certain SAP data centers or for buildings where certain support services are provided. This means that customers in particularly security-sensitive industries can benefit from an extremely high level of protection.

Employees and visitors must always wear their company IDs in a visible location when in the buildings. Guests are registered at the reception desk when they arrive at SAP, collected by an SAP employee, and accompanied throughout the buildings. Noncompany personnel such as guests, visitors, and service providers can be clearly identified by their assigned ID cards.

To enable logon from outside SAP premises and SAP networks, we use a two-factor authentication system valid around the world.

Access rights are granted to all authorized employees individually based on specific requirements.

ACCESSING OUR DATA PROCESSING SYSTEMS

Access to our data processing systems is subject to strict requirements for personnel and is governed by a global authorization system. Authorizations are not assigned automatically; they need to be requested specifically. Authorizations take into account all relevant instances before they are granted.

Once an authorization is assigned, it's valid for noncritical profiles and roles for five years. Critical authorizations have a more restricted term of three years; or if it's an insider critical profile, it's valid for one year. Authorizations are extended using a dedicated approval process. This control mechanism prevents critical authorizations from being extended without being checked.

ENABLING SECURE SYSTEM LOGON

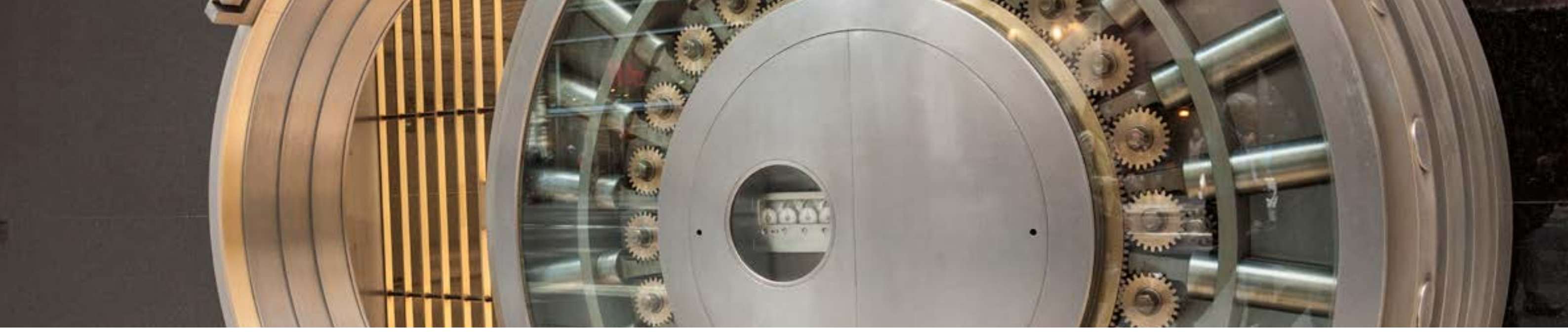
Internally, SAP uses a single sign-on (SSO) system. With SSO, employees are granted access to all systems relevant to them according to their role and the associated authorizations following a single logon in the SSO system using their user ID and password. After a specified number of failed attempts, logon to the IT systems is blocked. If the password is entered incorrectly too many times on smartphones, the data is deleted from the mobile device.

To enable logon from outside SAP premises and SAP networks, we use a two-factor authentication system valid around the world, supported by RSA SecurID cards or a soft token. These allow secure access to internal and external networks, virtual private networks, and wireless LANs, e-mail, Microsoft Windows desktops, Web servers, and other networks. The RSA SecurID card remains the property of SAP. It can be used only by the owner of the card, and it must be returned to SAP following the end of employment with the company.

AUTOMATING USER MANAGEMENT PROCESSES

The user management process concerns all activities related to setting up, assigning, and terminating roles, including associated rights and authorizations. This process is largely automated and is based on our identity management system and the access request management. Comprising data classification, access procedures, and profile administration, user management helps ensure a secure authorization lifecycle in the following ways:

- Regular security solution: When the employee leaves the company, most user data is deleted automatically.
- Special security solution: If user rights need to be blocked immediately for internal or external users, the manager can trigger this separately. User management then blocks user access to all relevant systems. This means SAP can help ensure that users can be blocked immediately and lose all system rights.
- External systems security guidelines: External systems are connected to the SAP company network only in exceptional circumstances and only if this is urgently required for business reasons. All external systems that are connected to SAP are registered accordingly. The external system must never be connected with other non-SAP systems.



REINFORCING IT SECURITY

We have a number of requirements to help ensure security of our technology.

Network Security Management

Our network is divided into multiple network security zones that correspond to different security and risk levels. Our corporate network contains five security zones.

The classification of IT systems in the security zones depends on the operational purpose of the IT systems. The security measures for a zone depend on the access radius, exposure level, and security requirements.

As the most heavily exposed zone, Zone 4 requires the most thorough security measures. Zones 1 through 3 must be protected against Zone 4 by security measures. The potential risks reduce from Zone 4 through to Zone 1, and the confidence level rises from Zone 4 through to Zone 1. The four network security zones and the external Internet zone (Zone 5) are described in the table.

Zone	Description	Examples
5	Public Internet, customer network, and partner network	Amazon Web services, Google, Microsoft, and so on
4	Internet DMZs	SAP® Developer Network (SDN) site, SAP.com, SAP Support Portal destination, and SAP Service Marketplace extranet
3	Fenced (internal) DMZs	Training areas, offshore Windows Terminal Server (WTS), partner WTS
2	Internal default zone (office network)	Office area, development area, core services such as Microsoft Active Directory, domain name system (DNS) server, and others
1	Protected, high-security area	Enterprise resource planning, customer relationship management, business warehouse, human resources, and so on

Encrypting SAP and customer data helps ensure the confidentiality and integrity of the data. As such, we lay down strict requirements for the encryption standards in our IT software systems and servers.

Security Zone Encryption

Encrypting SAP and customer data helps ensure the confidentiality and integrity of the data. As such, we lay down strict requirements for the encryption standards in our IT software systems and servers.

For strong encryption methods and keys, we use at least 128-bit symmetric keys or 2048-bit asymmetric keys, as well as strong and internationally recognized algorithms such as advanced encryption standard (AES), digital signature algorithm (DSA), and SHA-256.

For all IT systems in security zones 1 and 4, strong encryption of communications (such as HTTPS) is mandatory. Additionally, strong encryption is mandatory for all IT systems in security zones 2 and 3 that process confidential data (such as personal data).

For IT systems in security zones 2 and 3 that do not process confidential data, strong encryption is optional.

Hard Disk Encryption

SAP's security policy requires encryption for the storage of all confidential and strictly confidential data. Using the products Pretty Good Privacy (PGP) and Microsoft BitLocker, SAP employs dedicated, internal, sector-based hard disk encryption to protect sensitive data from unauthorized access from outside the SAP network. PGP and Microsoft BitLocker encrypt all saved data and decode this data when it is accessed directly on the hard disk. Encryption and decoding are possible only with the use of a password. Applications that need to access encrypted data cannot automatically read the data. In addition to hard disk encryption, PGP and Microsoft BitLocker install an authentication system that requests user authorization before the operating system starts (preboot authentication).

E-Mail Encryption

SAP uses PGP encryption to securely communicate with external parties who have exchanged PGP keys with SAP. This enables the authentication, integrity, and confidentiality of e-mail communication according to the highest technical standards.

Protection Against Malware

All data in our IT systems is checked for viruses and other malware with antivirus software. We manage our antivirus solution centrally and regularly update it. If a virus is discovered, the solution alerts the server administrators immediately.

ADOPTING REQUIREMENTS FOR CLASSIFYING INFORMATION

All information must be protected against unauthorized access in line with the security requirements of the information. To this end, the owner of the information is obliged to classify the information according to the respective level of confidentiality. All information must be labeled, managed, stored, and disposed of or destroyed according to classification. Employees are responsible for ensuring that this objective is met in accordance with SAP's information classification security standard. Regular training sessions and campaigns remind employees of this obligation.

Access to data and systems belonging to customers and partners is provided on a strict need-to-know basis. Employees may view confidential data only if there is a specific requirement. Data belonging to business partners and customers to which an SAP employee has access during employment must be treated in confidence.

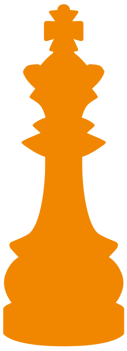
MAINTAINING CONFIDENTIALITY WHILE HANDLING PERSONAL DATA

Personal data at SAP is always processed in compliance with the most applicable regulations and laws. We can collect personal data only for specified, explicit, and legitimate purposes, and we cannot process it in a way incompatible with those purposes.

SAP has technical and organizational measures in place to enable us to fulfill our legal obligations as data controller as well as data processor in processing personal data on behalf of our customers.

As a matter of principle, SAP treats all personal data as confidential. This applies both to the personal data of SAP employees and to the personal data of customers or other third parties that is saved or accessed by SAP.

Employees and contractors with access to personal data either controlled by SAP or by customers are obliged to maintain data privacy and confidentiality. They are required to observe national provisions, legislation, and data protection regulations.



A key element of SAP's security strategy is the introduction of cross-departmental security risk areas. Tailored security measures are defined for each of these security risk areas in collaboration with the responsible organizations.

ENSURING CORPORATE CONTINUITY IN CRISIS SITUATIONS

SAP's corporate continuity framework enables us to respond and adapt rapidly to threats posed against our workforce, business, and reputation. SAP follows an "all-hazard" approach, which incorporates handling of all types of disruptive incident situations and prepares for specific scenarios that are most likely to happen and recur. Within this framework, the loss or absence of normal business processes triggers crisis management and process continuity activities, which are continuously supported by situation monitoring, travel safety, and security. These activities help to prepare and protect SAP's workforce in order to enable continuity in critical decision making.

Crisis management supports decision-making and response coordination from a strategic, tactical, and operational perspective. It also takes into account time constraints and pressures by internal and external stakeholders in the event of a disruptive incident. Crisis management operates on a local, regional, and global level and uses a two-step approach. First, emergency response teams take immediate action in the event of a disaster. Following local rules and regulations, these teams have been trained, for example, to extinguish fires in an early stage, to evacuate offices, and to perform first aid. Second, our crisis management teams are authorized to make necessary operational decisions to mitigate and control the situation. They are equipped with an alert network, required documentation, and crisis rooms.

Our process continuity team helps ensure best business process continuity practices by setting the objective to identify, describe, and prioritize SAP's critical business processes and the resources needed to support them. We view as critical all processes that are crucial for our customers, partners, service providers, employees, and shareholders and that, if disrupted, impact the company's survival. Another main objective is to conduct a business impact analysis to understand the effects of a disruption of these processes. Based on this analysis, we create process continuity plans for both locations and global lines of business. These plans cover impacts such as unavailability of offices, employees, service providers, and infrastructure outages.

SAP verifies the ongoing effectiveness of its corporate continuity framework to ensure that critical activities can be recovered as soon as possible. Top management commitment as well as regular dry runs and reviews help us ensure that plans and procedures are kept up-to-date and effective. With such a framework in place, we can take immediate measures to protect our employees, to maintain and recover our critical business processes in the event of a disruptive incident, as well as to safeguard our reputation.

PROTECTING INFORMATION IN INDIVIDUAL INCIDENTS

SAP has several policies in place to protect data in individual events.

Product Safety

Incidents that relate to an SAP® product trigger a fixed list of defined measures that are performed in several steps. Once an incident has been reported, immediate countermeasures are initiated. By analyzing the incident, we can quickly establish and implement solutions. Each step is continuously documented in the form of a security incident message. The security incident message provides a complete overview of the incident status at any time, including the status of the corresponding solutions.

In general, customers are informed of product security updates on the second Tuesday of every month. Known as "Security Patch Days," these days allow customers to download the security updates for SAP products, provided that the updates are issued through support in the SAP Support Portal destination.

Security Incidents Not Related to a Product

Security incidents not related to a product include the theft of a laptop or a smartphone or other incidents that affect an employee's ability to work but do not affect the operations of the overall company. All security incidents are investigated immediately without exception, including non-product-related incidents. The findings from this investigation are then acted on. Executive management and employees will be informed as appropriate, depending on the incident. All incidents are reported to the local responsible manager. Security incidents are confidential and are processed and documented by security officers.

IMMERSING EMPLOYEES IN SECURITY AWARENESS

Within the mix of security, technology, and processes, people themselves play a key role. Ensuring our employees are fully trained and aware of security measures is central to the protection of customer data. On a regular basis, all employees are required to complete an e-learning course on information security. Employees are made aware of the risks concerning information security during the normal working day, while the focus for managers is on their special management role in maintaining information security. This mandatory training is part of our global onboarding initiative – every new hire is required to complete the training in the first weeks of their employment at SAP.

In addition to this mandatory training, further training is available for all employees in special focus areas, such as security during business trips and social engineering.

In addition to the regular training courses, the corporate communications department regularly gathers up-to-date information about the latest security issues and sends out reminders about the importance of security.

Security Management at SAP

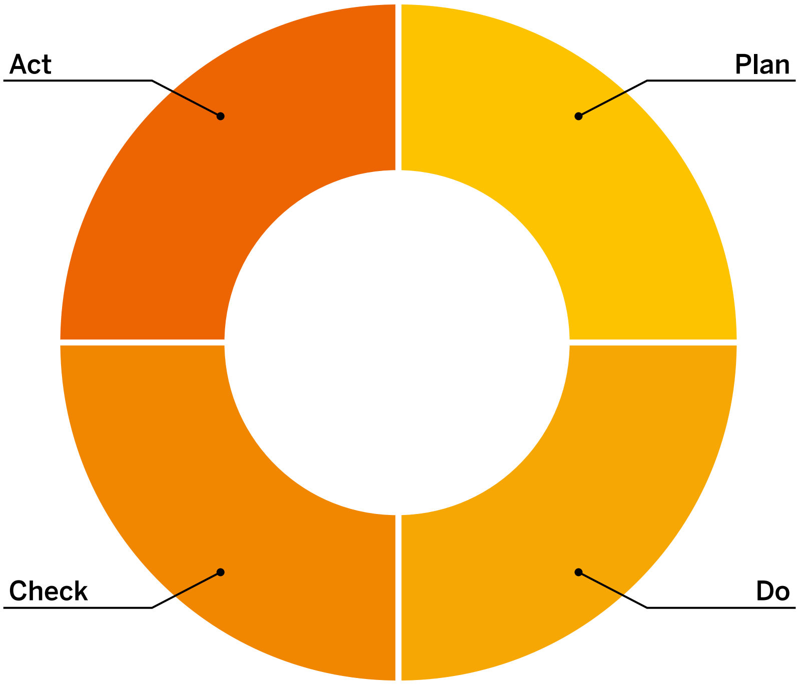
COORDINATING SECURITY VIA THE SECURITY ORGANIZATION AT SAP

The central global security department at SAP is assigned to the board area of development. The department is managed by SAP's chief security officer. Our global security department coordinates the topics of IT security, product security, corporate security, physical security, and cloud security. Our global security team works in strong cooperation with SAP's data protection and privacy office.

SECURITY MANAGEMENT FRAMEWORK

As shown in Figure 1, the "Plan, Do, Check, Act" (PDCA) cycle is an iterative four-stage management process typically used for improving business processes. The PDCA cycle can be applied to the security management framework as follows.

Figure 1: SAP's Security Management Framework – PDCA Cycle



Plan

The overall security strategy for SAP is developed by SAP's global security team and approved by SAP's security steering committee. Our strategy defines the organizational structure of the security management framework, the acceptable security risks for each business area, the security management processes, and the interaction of individual organizational security units.

Security requirements and associated standards are defined in SAP's security policy and own standards.

Do

Security requirements defined in the "plan" phase are implemented in the "do" phase. Security measures are implemented and maintained through mandatory training sessions and campaigns.

Check

The "check" phase is implemented in several stages:

1. Using continuous security risk management, we review and patch possible weaknesses in the established security controls. Measures that require increased investment are also approved by our security steering committee.
2. All significant security incidents are reported to our integrated security incident management organization within SAP's global security group. By conducting forensic analyses, the team can improve the established security controls.
3. Continuous testing and evaluation of the security controls use assessments developed by the operational security management organizations and external and internal security tests. (Internal tests are conducted mainly by our global internal audit services organization; external audits also include various ISO certificates.)

Act

In the "act" phase of our security management framework, the established security strategy is continuously adapted to new requirements on the basis of the risk and incident reports from the check phase. If necessary, we also modify security standards, controls, and measures.

If changes are likely to have a significant impact on the SAP organization as a whole, they must also be approved by SAP's security steering committee.

Security in the Digital Business Services Organization

DELIVERING SERVICES AND SUPPORT TO SAP CUSTOMERS SECURELY

This section discusses security standards and procedures employed in all SAP organizations involved in providing service and support to our customers. These organizations include Digital Business Services and the Products & Innovation (P&I) board area. Remote application management is subject to special regulations, due to the fact that SAP employees may be dealing with confidential and/or sensitive personal data stored on customer or partner systems. The same applies to SAP partners and other service or software providers. Later sections discuss relevant details specific to the different service and support organizations at SAP.

DELIVERING WORLD-CLASS SUPPORT

Our global organizations involved in support service delivery are responsible for processing customer and partner incidents securely and reliably – 24 hours a day, 7 days a week, 365 days a year.

Digital Business Services, in addition, provisions reactive and proactive remote and on-site support services for customers with a valid support and premium engagement agreement.

In SAP's support organizations, all customer incidents and support queries for SAP solutions are processed around the clock by one of our many qualified support technicians and developers.

Our support organizations comprise 10 global support centers and over 20 development labs in 22 countries. Since our global support centers and development labs are distributed around the world, incoming incidents can be processed and resolved quickly, regardless of the time of day or regional bottlenecks (see Figure 2). Which location processes a customer or partner incident depends on several factors. In addition to the time zone, factors include the language of the incident, the affected product, the incident priority, and the respective expertise of the support members.

Figure 3 shows the geographical makeup of our global support centers.

All SAP support organizations are fundamentally governed by the same security and data protection and privacy guidelines as outlined for the entire company in the previous section. Our support areas are also governed by supplemental regulations and guidelines, particularly concerning the management of confidential or personal data in customer systems. These are revised and, if necessary, expanded at least once a year by the security department and the management. These guidelines are part of the quality and security manual of the ISO 9001:2015 and the ISO 27001:2013 certificates and are subject to annual combined quality and security audits.

Figure 2: 24x7 Support – Incident Message Processing That Follows the Sun

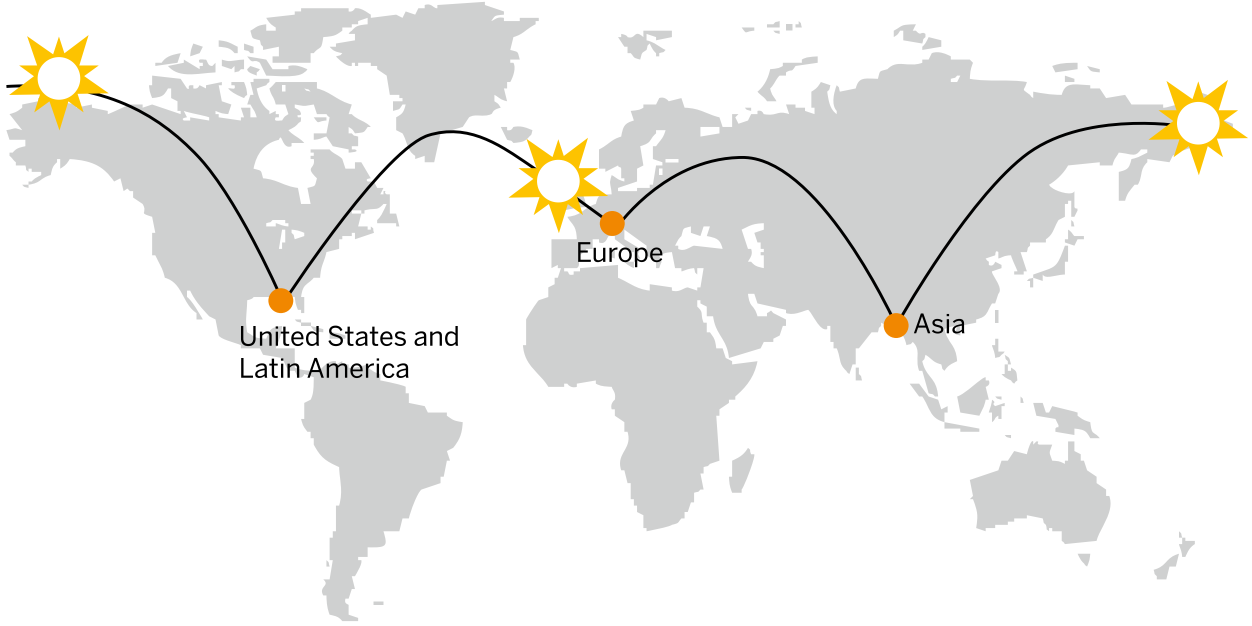
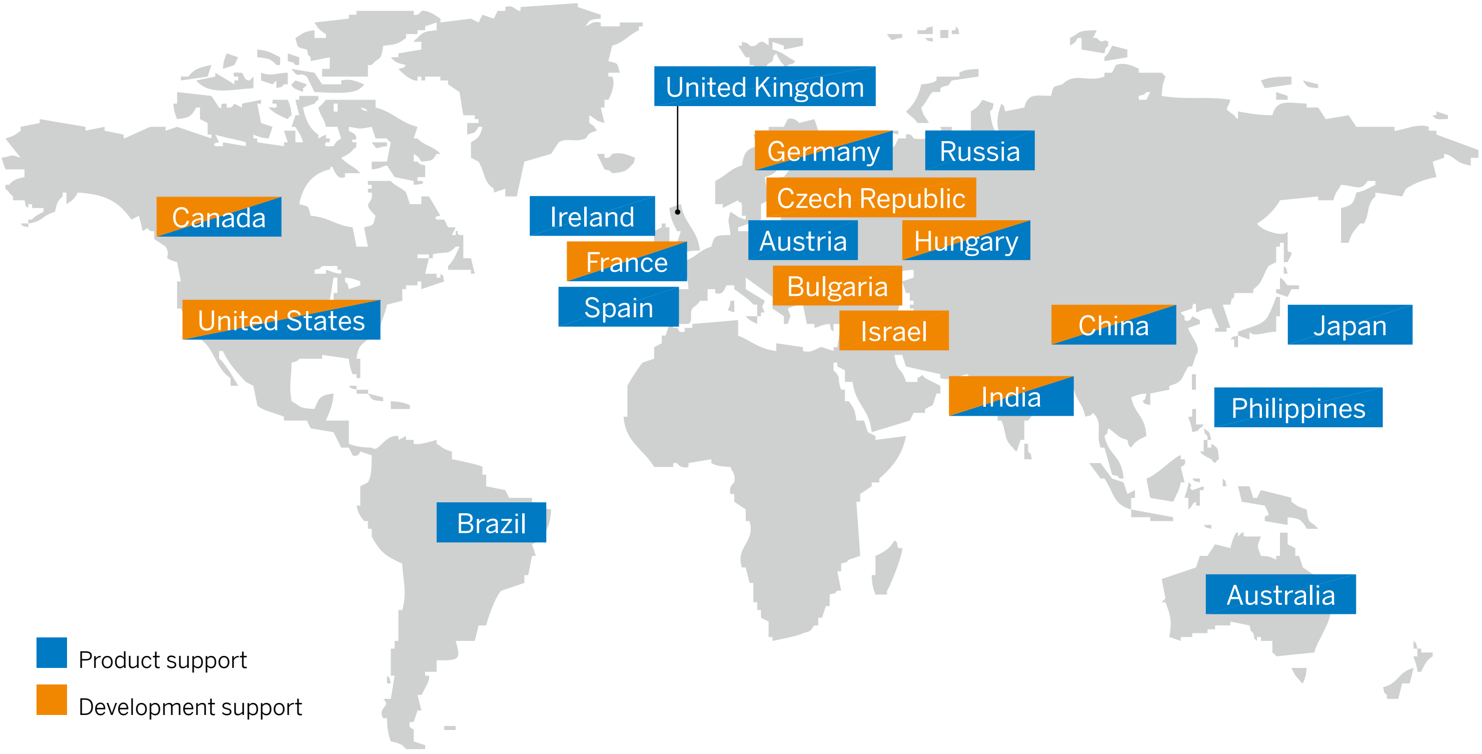


Figure 3: SAP’s Major Global Service and Support Locations Worldwide



PROCESSING CUSTOMER AND PARTNER INCIDENTS

Product support staff in Digital Business Services are responsible for processing customer and partner incidents securely and reliably. Incidents are entered either in SAP Solution Manager, an application management solution installed at the customer's site, or using the Internet-based SAP Support Portal. Both are provided by SAP. To process certain incidents, it may be necessary to access systems owned by the customer. In this situation, as our customer, you would need to grant the responsible SAP employee the necessary authorizations and open a remote support connection.

COLLABORATING WITH SERVICE PROVIDERS

Digital Business Services works with a range of partner companies for the provisioning of service and support. Our partner companies and their employees are contractually obliged to maintain the same strict guidelines regarding security and processing of confidential and/or personal data that govern SAP employees themselves. This obligation is written both into the contractual agreement between SAP and the respective partner organization and into the contracts of the partner organization's employees. Partner companies are subject to regular reviews by SAP, including on-site inspections and audits to monitor compliance with legal and contractual obligations.

APPLYING GLOBAL PROCESSING REQUIREMENTS FOR PEOPLE

When a new employee is recruited for Digital Business Services, the same general application and selection criteria apply as described for all SAP employees. Also, since 2015, our global processing guideline has required a background verification check for potential employees. We apply this processing guideline to all new hires into SAP and its subsidiaries. This global guideline respects local legal requirements and includes all external hires, as well as the external workforce (contingent workers) and employees, if the situation requires it and the employee accepts the request.

On commencing employment with SAP, all employees receive comprehensive training. Initial training covers a wide range of topics, including security, data protection, and privacy. Training also includes an internal mentoring system: each new service and support engineer receives support from an experienced colleague in the first few months of employment.

ACCESSING DATA PROCESSING SYSTEMS

A groupwide SAP authorization concept protects access to data processing systems. The concept depends on the respective user and the authorizations assigned to this user. Internal support systems in which customer incident messages are processed are protected by special, highly restricted authorization profiles. Authorization profiles govern access to customer incident messages and data within the SAP infrastructure, as well as access to customer systems via remote support.

All required authorizations of partner employees working for SAP are limited from a time perspective; authorizations are dependent on the SAP task and could be removed at any time based on the sole discretion of the related management.

ACCESSING CUSTOMER DATA THROUGH OUR REMOTE CONNECTIVITY FRAMEWORK

Customer data systems are generally accessed for remote support delivery, in areas such as incident processing and remote service delivery, using our remote connectivity framework. The remote-connectivity infrastructure of this framework is established for nearly all SAP customers with valid support agreements. Since sensitive customer data can be accessed via remote connectivity, this access method is subject to particularly high security requirements.

The Connection Process

In general, an SAP employee would request access to your system only when offline methods cannot solve the problem you've encountered. For example, in incident processing, at the request of the SAP support engineer, you would open the connection to SAP and save the logon data in the "secure area" of the customer incident. Special access restrictions include read-access logging, which enables the transfer of logon credentials in a way to meet the highest security standards.

As the customer, you have unrestricted control over the established connection at all times. An SAP employee may never access a customer system without the knowledge and active support of the customer. The remote analysis is generally attempted through the customer's test systems. Only in a very limited number of exceptional cases is access to the customer's production system necessary; this is only allowed after you, the customer, have given explicit consent.

Additionally, you are responsible for ensuring that the SAP support engineer is assigned only a limited role for your customer systems. Only the minimum authorization rights required for the troubleshooting process should be assigned. You can log all actions taken during the remote access session using tools that we provide.

Operating the Remote Connections

From a technical perspective, the remote support connection is opened as follows:

1. The customer opens the remote connection in the SAP Support Portal destination.
2. The service connector on the customer client establishes the network connection between the customer's SAProuter application and the SAProuter at SAP. The router connects with the service and support backbone at SAP. (The SAProuter is described separately in the section "Enabling a Secure Connection for Customers.")
3. SAP maintains the network connection through regular pinging. The connection status is updated in SAP Support Portal.
4. SAP uses the SAProuter to connect to the customer system.

Choosing Connection Types for Remote Connection

Once the technical prerequisites for establishing the remote connection are in place, you can choose from various connection types. You decide which type of access to grant the SAP employee (user, authorization, or customer system). The connection types offer various technical possibilities. The most important connection types are:

- SAP GUI–based connections
- HTTP Connect and URL access with access to HTTP-based applications
- Connection types with application sharing or access at the operating system level (for example, Microsoft Windows Terminal Server desktop and application sharing, Citrix MetaFrame desktop and application sharing, Telnet and SSH access to the operating system, and operating system access for the IBM iSeries)
- Citrix GoToAssist for screen sharing

All of these connection types offer encrypted data sharing.

Enabling a Secure Connection for Customers

SAP recommends that customers establish the following measures to help ensure secure connections:

- Use a hardware router (firewall) with filter functions (access lists) and connection logs (optional): Using a hardware router is a technical prerequisite for the remote connection.
- Use the SAProuter: The SAProuter is an SAP software component used to monitor the communication between the customer server and the associated front-end computers. The SAProuter increases network security and simplifies the configuration of the connection channels. The software is a gateway for communication with SAP at the application level and can be used on its own or together with an IP firewall. The SAProuter is installed in the actual logical communication channel between the participating systems and forms an additional access security level – both within the internal network and for connections to or from external partners.
- Employ user authorization as a further type of access control in addition to the normal security mechanisms: This enables greater protection against unauthorized access to critical data or systems. For connections established with the SAProuter, no end-to-end communication is necessary between participating systems at the network level. If, for example, a front-end PC accesses a server via a router, it is not necessary to define the complete route between the two systems at TCP/IP level. The two ends only have to establish a connection to the SAProuter itself. From the point of view of SAP communication, this forms the central hub in the network and acts as the starting point for each subconnection. Each subnetwork that is logically defined behind an SAProuter is therefore reduced to the network address of the SAProuter.

- Install a firewall configuration (combination of different security mechanisms): A firewall is used to restrict network access and to prevent unwanted access to the system based on sender or target addresses and the used services. The firewall monitors the data traffic that passes through it and uses specific rules to define which network packages should be permitted. This allows the firewall to prevent unwanted network access.
- Define administrator rights for critical systems (in particular, hardware routers and SAProuters) to help ensure controlled access to the hardware for authorized persons.
- Target activation of the necessary service types in SAP Support Portal and temporary remote connection in order to allow access to the affected system. Follow this with deactivation of the remote connection in SAP Support Portal once the support activities are complete.
- Create special user profiles for the respective service type.
- Deactivate the user or change the password once the connection is deactivated.

Digital Business Services supports only SAProuter connections – with one exception being GoToAssist screen sharing. Since SAP routes all access to customer systems through a corresponding SAProuter, the connection between SAP and the customer is reduced to a simple connection from SAProuter to SAProuter.

Enabling On-Site Access to Customer Systems
Service and support employees may access customer systems on-site only as part of a specific service delivery or for customers with a special premium engagement agreement. In case system access is executed using SAP equipment, such as laptops with SAP software images, the connection process will also follow the guidelines of our remote connectivity framework mentioned above.

If a service and support employee opens an incident on-site in the name of the customer as part of the service, this must be in all cases with the agreement of and in the name of the customer.

SETTING REQUIREMENTS FOR IT SECURITY

Sensitive customer data – for example, personal data relating to customers or customer incidents – must be protected by special, highly restricted authorizations in the support systems. SAP uses a specially designed backup concept to prevent any loss of this data.

RUNNING A DATA PROTECTION MANAGEMENT SYSTEM

Following the new requirements defined in the amended German Federal Data Protection Act, SAP has developed and implemented a management system for data protection that covers the Digital Business Services organization, as well as all other areas within SAP. To comply with the accountability obligations of customers, an independent certification authority tested and certified the management system. Since a suitable ISO certification did not yet exist on the market following the amended legislation, SAP developed a data protection management system (DPMS) on the basis of the BS 10012 standard. The BS 10012 standard covers most European data protection aspects and can easily be adapted to specific local legislation.

First implemented in 2010 in the SAP support organizations, the DPMS has been extended to the entire company and is now implemented in all board areas. The DPMS follows known ISO principles, such as annual audit programs, and also covers the ISO 19011 standard requirements for the proper auditing of management systems. The DPMS is regularly controlled by SAP's certification body for data protection, the renowned British Standard Institutions (BSI) in London.

The data protection management system builds on SAP's data protection and privacy policy, which contains the SAP security guidelines and standards. It is documented in the "General Book of SAP Data Protection Management System." The certification can be found on SAP.com and SAP Support Portal. This document and the annual audit report of the BSI are available for inspection by all SAP customers. The certificate is regularly updated.

ADOPTING REQUIREMENTS FOR CLASSIFYING INFORMATION

The guidelines outlined in the general security section of this document also apply to SAP organizations involved in the delivery of service and support.

PROTECTING INFORMATION IN CRISIS SITUATIONS

The central security department at SAP is responsible for handling crisis situations such as natural catastrophes, epidemics, or political unrest. General processes and measures are described in the general security section.

As for all areas within SAP, our Digital Business Services and P&I organizations have their own business continuity management section, which helps ensure that all business processes continue to run in crisis situations. Essentially, all SAP employees can continue to work from home if they are no longer able to work at the SAP offices. To enable 24x7 support, expert resources are distributed across various regions and locations around the world. In the event of a local crisis situation, this means that other locations can take up the support functions if one support location becomes inoperative.

All plans to ensure the continued operation of critical processes in the event of an emergency or crisis, and the emergency plans of the individual support organizations, are reviewed and audited annually. During these reviews, SAP adds new critical processes, conducts test runs, and trains employees.

PROTECTING INFORMATION IN INDIVIDUAL INCIDENTS

Individual incidents such as the theft of a laptop, the loss of a smartphone, or a medical emergency may also occur within SAP. Such incidents are managed in accordance with the general processes and regulations applicable throughout SAP.

CONTINUING SECURITY AWARENESS TRAINING FOR EMPLOYEES

In addition to the data protection and security training measures described in the general section, special awareness campaigns are regularly held for SAP support engineers. Internal ISO audits are conducted after special training courses for the individual SAP locations. SAP employees can also book and complete virtual classroom and e-learning sessions at any time using the internal training system of our service and support academy team.

APPOINTING A SECURITY OFFICER FOR ON-PREMISE DELIVERY

To meet particularly high security and data protection and privacy requirements, a specific information and business security officer is appointed for the service and support organizations. This officer oversees the implementation of strategic organizational security and data protection requirements, as well as monitoring these through targeted measures. Typical action areas include ensuring compliance with guidelines, processes, standards, and special instructions. The security officer acts as the point of contact for any new incidents and responds to internal and external queries regarding security and data protection.

SECURITY REGULATIONS FOR DIGITAL BUSINESS SERVICES

This section focuses on the security regulations that apply specifically to Digital Business Services. The service this group provides is characterized by rapid, customer-oriented solutions staff must deliver in response to incoming requests, sometimes through remote analysis.

Resolving Issues with Self-Support and Incident Processing

If a customer encounters a problem with their SAP solution, we offer various options to help ensure a swift resolution. The fastest method is customer self-support using one of our self-support tools, such as SAP Community Network, the SAP Help Portal service, SAP Service Marketplace, or SAP Support Portal. See the appendix for important links to additional information on our security tools.

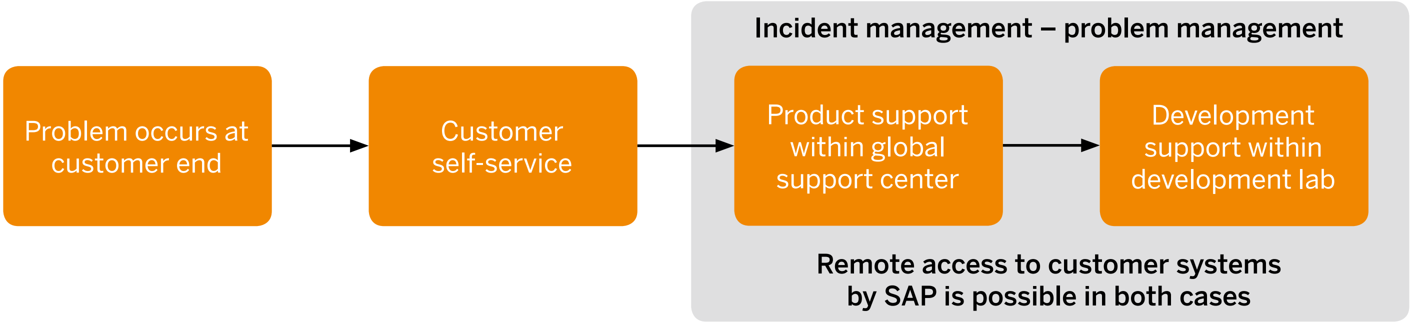
If self-service support doesn't yield a solution, you can escalate the issue to SAP as a customer incident message (see Figure 4). Once the responsible global support center has been identified, the message is automatically assigned to a support engineer and the problem is processed by our product support organization.

Using Product Support to Resolve Incidents

Our product support organization performs basic support tasks such as initial analysis, searching for existing solutions and information in the SAP Notes tool, and searching for similar previous queries. Secondary support tasks – such as program analysis or program troubleshooting – are also performed in our global support centers. Additionally, we offer rapidly implementable, short-term work-arounds. Digital Business Services expands on the initial analysis and delivers short-term implementable solution proposals to customers for their respective queries.

If the responsible support engineer can't resolve the problem, the incident is transferred to another organization within the global support network or escalated to an expert or developer team. Solutions at the development support level are processed in our development labs. Solutions developed here are delivered as program corrections or notes from SAP Notes. Development support is responsible for the entire product maintenance cycle – that is, providing enhancement packages, adapting the software to meet modified legal frameworks, offering upgrade tools, and performing similar functions.

Figure 4: Product Support Incident Processing


Incident management – problem management
Problem occurs at customer end
Customer self-service
Product support within global support center
Development support within development lab
Remote access to customer systems by SAP is possible in both cases

Often, however, problems can simply be solved through verbal or written communications between the customer and the support technician, or by referring to existing information in SAP Notes. In some cases, it may also be necessary to analyze the problem in the customer system. In this case, an SAP employee must access the customer system directly. See "Accessing Data Processing Systems" in the previous section.

For customers in security-sensitive and highly regulated industries mandated to comply with strict security regulations and data-privacy requirements, Digital Business Services offers advanced secure support services that are fully integrated with premium support engagements, SAP ActiveEmbedded and SAP MaxAttention™ offerings. These services satisfy company internal and industry-specific advanced security requirements and regulations by extending the level of security for support processes requiring remote system or data access. They include security-cleared support personnel, specially secured rooms in SAP Global Service Center locations and labs, tools to classify incidents for special processing, and last but not least, highly secure areas for storing customer equipment.

HIGHLIGHTING GOLDEN RULES FOR SAP SUPPORT AND SAP CUSTOMERS

Owing to the particularly sensitive nature of the work carried out at SAP, we have established a list of special security measures, summarized as "golden rules" for SAP staff and customers.

Ten Golden Rules for Digital Business Services Employees

Here we list our "top ten" rules for enforcing security:

1. Employees must always treat customer data in customer incident messages as "confidential" and handle this information in accordance with the guidelines governing its classification. This applies to all information types, such as customer self-service (SAP internal support systems) information, attachments, e-mails, printouts, or any other verbal or written communication.
2. SAP employees must transfer information from customer incident messages only in encrypted and protected form.
3. Customer data must not be saved on computers or servers outside the SAP internal support systems. If in exceptional cases it is necessary for SAP employees to save data locally, it must be sufficiently protected, encrypted, and securely disposed of after use.
4. SAP employees must observe all data protection and security guidelines without exception, even in the event of a crisis, such as message escalations or system downtimes.
5. Unsupervised computers must be automatically or manually protected against unauthorized access. Software must not be installed on any computer that has not been explicitly released by SAP IT.

6. In the past, only company-owned computers were allowed at SAP. Recently, SAP introduced the “Bring-your-own-device” initiative, with the result that privately owned mobile devices such as smartphones and tablets can be used for certain defined business use cases. In order to maintain security and to protect SAP’s intellectual property, access to the SAP network from these devices is possible only via the SAP Afaria® mobile device management solution.
7. SAP employees must keep all printouts of customer data in a locked location and dispose of them securely after use.
8. All data protection and security requirements also apply to off-site IT equipment – for example, home offices.
9. Any violations of the security and data protection guidelines must be reported to the line manager and the security and data protection officer immediately.
10. In the case of remote support, customer systems may be accessed only with the explicit approval of the customer. Prior to the remote support services, the affected system type must be established first. Access to production systems or changes to system parameters or application data must be avoided. Exceptions are possible in agreement with the customer and only if the customer requests it and gives the consent explicitly.

Six Golden Rules for Digital Business Services Customers and Partners

Here we list six rules for enforcing security among customers and partners:

1. In the event of remote support, the customer must save their logon information to the “secure area” of the customer notice.
2. The customer is reminded to provide the SAP support engineer with access to the test system but not the production system.
3. The data held in the test system should be made anonymous.
4. The customer must assign the minimum authorizations required to complete the troubleshooting; SAP_ALL rights must not be assigned.
5. When application-sharing tools are released, the customer should provide only selected access to the required windows.
6. The customer must close the connection once the troubleshooting is complete and restrict access to a specified period.

Appendix

RELEVANT CERTIFICATIONS

SAP holds the security certifications listed in the table. See also www.sap.com/corporate-en/about/our-company/quality-at-sap/iso-certificates.html.

Relevant Security Certifications

Standard	Description
BS 10012	Data protection standard – specification for a personal information management system
DIN EN ISO 27001:2013	Certified information security management system for critical business applications, including: • Support and maintenance processes in the Digital Business Services organization • SAP installed base maintenance and support (Products & Innovation organization and SAP IMS 365 mobile service) • SAP® Cloud portfolio support • SAP SuccessFactors® solutions support • SAP Business One® application support in Europe, the Middle East, Africa, Asia Pacific, North and Latin America
DIN EN ISO 9001:2015	Certified quality management system for Digital Business Services
DIN EN ISO 19011:2011-12	International standard that sets guidelines for auditing management systems
ISAE3402	International standard on assurance engagements
DIN EN ISO 22301:2012	Business continuity certification – SAP for Information Technology solution portfolio
BSI Data Protection Certificate N° 590244	• Customer incident management process of SAP support organizations worldwide – Digital Business Services product support, installed base maintenance and support, and cloud support • Proactive services – Digital Business Services • Delivery processes at offshore and nearshore centers – SAP Global Service Center locations • Data protection–related processes of SAP for Marketing solutions • Shared service center processes of SAP for Human Resources solutions

IMPORTANT LINKS

The table below provides important links on the subject of security.

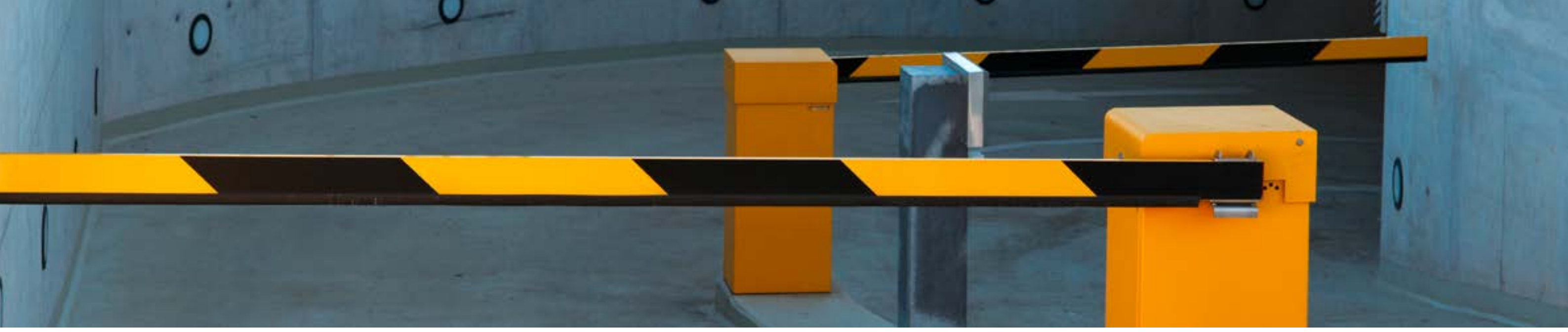
Link	Description
www.sap.com	Global Web site of SAP
www.sap.com/security	Security, data protection, and privacy on global Web site of SAP
http://scn.sap.com	SAP® Community Network (password protected)
http://sdn.sap.com	SAP Developer Network site (password protected)
https://support.sap.com	SAP Support Portal destination (password protected)
https://service.sap.com	SAP Service Marketplace extranet (password protected)

Managing crisis involves decision-making and response coordination from a strategic, tactical, and operational perspective, and it considers time constraints and pressures by internal and external stakeholders in the event of a disruptive incident.

FREQUENTLY ASKED QUESTIONS

This section presents frequently asked questions about SAP security.

Employees and Personnel	
How many employees have access to customer incidents and customer systems?	Access to customer incidents and systems is highly restricted. Only employees who have the necessary authorizations based on their role and work have access to customer incidents. Employees may access customer systems only if the customer has explicitly authorized a remote support connection.
How are employees made aware of data security and data protection?	All employees receive general and role-specific training when joining SAP. This training is repeated regularly, and employees are tested to check their knowledge of the subject.
Are all employees obliged to follow the code of business conduct and the security policy?	Yes. Employees are bound by their employment contract to follow these codes of conduct. Any violations may result in legal consequences, possibly leading to termination of employment.
How does SAP remind its employees of the importance of security?	The issue of security and data protection is frequently addressed in regular campaigns and training courses. Employees are regularly tested to assess their awareness. The central security department of SAP is responsible for planning, executing, and organizing the program.
Are the processes for revoking or modifying authorizations adequately explained should the role of an employee change?	Authorizations are revoked in the support area when an employee no longer works at SAP. Authorizations are also modified accordingly should the role of an employee change within the support area. Similar processes also apply in other areas if an employee switches from one group in the company to another. In this case, all authorizations are revoked, and the user receives new authorizations relevant to their role. If an employee leaves SAP, their user ID and all authorizations are canceled.



Access and Protection of Buildings	
Are SAP buildings access protected?	Technical access-protection systems are installed in all SAP buildings. Only SAP employees and authorized personnel have access to the buildings.
Is there a person or department responsible for physical security?	The central security department of SAP is responsible for physical security.

IT Security	
How does SAP help ensure the security of information?	SAP has established a dedicated management system, which is monitored and certified by independent, trusted third parties and described in detail in this paper.
Is antivirus software installed on network computers?	SAP's global IT security policy states that all computers connected to a network must have antivirus software installed.
Are there guidelines and processes at SAP that govern the use of networked services or services that use several computers?	IT security guidelines govern the use and operation of IT systems or networks.
Are there guidelines and processes at SAP that govern the use of e-mail, intranets, and the Internet?	Yes. These guidelines are defined and governed in the SAP security guideline "IT Security."
Are there guidelines and processes at SAP that govern the use of passwords?	Yes. The SAP security guideline "IT Security" governs the use of passwords.

Are there guidelines and processes at SAP that govern the use, storage, and deletion of sensitive and protected data?	Yes. These matters are governed by the SAP security guidelines "IT Security" and "Information Classification."
Are there guidelines and processes at SAP that govern access by third parties and remote access to SAP software systems?	Yes. See the information in this paper titled "Accessing Data Processing Systems" in both the "General Security at SAP" and "Security in the Digital Business Services Organization" sections. Also see the section "Security Management at SAP."
Are there multiple authentication levels for sensitive systems?	Yes. There are several levels that help ensure user-specific and authorization-specific access to individual systems and the information contained in these systems. First, each employee logs on to the PC or laptop using his or her user ID and password. The user's identity is verified again when he or she logs on to any system that requires authorization. When users are working in the system itself, roles, profiles, and individual authorizations govern which information and settings the respective employee is allowed to view and edit.
Do employees log on with a unique ID that is assigned to one employee only?	All employees use their own individual user ID for IT systems.
Do all employees with remote access privileges need this authorization to carry out their work? Are there appropriate control measures governing how management assigns remote access rights?	Remote access is protected by a user-specific authorization classified as "sensitive." Both the employee who requires such authorization and the manager who must approve the authorization are made aware that only privileged employees may be granted these rights. The employee is also reminded of the nondisclosure agreement and the sensitive nature of the authorization. The employee and the manager must agree to this and explicitly state the reason for this authorization request. The same regulations also apply to partner companies of SAP.

Guidelines and Audits

Is there a code of business conduct that outlines general codes of conduct for employees?	Yes. These rules are outlined in the code of business conduct and are fully accessible to and understood by all employees. The code of business conduct also forms part of the SAP employment contract.
Are there any data protection guidelines?	Yes. Data protection guidelines form an element of the SAP security policy, the SAP security standard on data protection, as well as the document *SAP Global Personal Data Protection and Privacy Policy*. SAP's data protection management system consists of data protection work instructions, regulations, and guidelines for all organizations in SAP.
Have processes for maintaining data protection laws and regulations been defined that help ensure the confidentiality and security of customer data?	A wide range of measures help ensure the confidentiality of customer and sensitive data. Current processes and standards for maintaining data protection laws are described in the section "General Security at SAP" (see in particular the information in "Maintaining Confidentiality While Handling Personal Data"). Data protection in relation to customer incidents is described in the section "Security in the Digital Business Services Organization."
Are there regular checks to monitor compliance with the SAP security policy?	A wide range of internal ISO 9001 and ISO 27001 audits are conducted to regularly check whether SAP employees adhere to the global policies and standards, so that compliance to the security policy is monitored thoroughly. All audit activities are centrally organized by the responsible auditing organizations and conducted by certified internal auditors with the support of the central SAP security department.
Does SAP have an information security team that oversees the implementation of the SAP security policy?	Each manager is responsible for implementing the security policy within their respective organizations. The central security department and the auditing and decentralized security units of SAP help managers in this process. Managers are informed about the performance and current implementation status of information security management systems in regular management reviews.

How are security incidents managed?

Security incidents at SAP are systematically documented and forwarded to the relevant officer. This security incident management process is described in detail in the information in “Protecting Information in Individual Incidents” in both the “General Security at SAP” and “Security in the Digital Business Services Organization” sections.

Does SAP have a guideline on classifying information?

The SAP security guideline “Information Classification” outlines how information is classified.

Is access to customer data restricted to specific employees, and is the distribution of such information prohibited?

Yes. SAP has guidelines and processes that govern access to customer data. In particular, such access is restricted by a dedicated authorization process; see also the SAP security guideline “Information Classification.” This guideline also specifies rules regarding the forwarding or publishing of confidential or sensitive information.

Are there any certificates that are accessible to customers?

Certificates acquired by SAP can be inspected at any time on the page www.sap.com/corporate-en/about/our-company/quality-at-sap/iso-certificates.html.

Is there an ISO 27001 certificate for information technology?

Yes. SAP possesses several ISO 27001 certificates. These can be viewed at www.sap.com/corporate-en/about/our-company/quality-at-sap/iso-certificates.html.

Is there a specific certificate for data protection?

Yes. Compliance with the data protection guidelines is maintained regularly in collaboration with BSI as SAP’s certification body for personal information protection. The certificate can be found at www.sap.com/corporate-en/about/our-company/quality-at-sap/iso-certificates.html.

Protection of Information in Crisis Situations

How does SAP prepare for possible crises and catastrophes?	The security departments are responsible for preparing for crises and introducing the measures that allow work to continue. With more than 20 locations, the Global Service & Support organization is distributed around the world. If a location becomes inoperative, another location assumes responsibility for message processing.
Are any plans in place to help ensure mission-critical processes continue in the event of an emergency?	Yes. There are plans for individual business areas, departments, organizations, and processes. The plans are regularly reviewed and updated.
Does SAP have a team that evaluates risks?	The central risk management unit of SAP is responsible for evaluating and handling risks. The team defines and manages the various risk profiles of the SAP infrastructure.
Are there any plans and guidelines for emergency protection?	Emergency plans to protect employees and buildings and emergency plans to protect mission-critical processes are available and accessible to all SAP employees via the intranet.
Are there any emergency response teams, and are these trained at all larger SAP locations?	Trained emergency response teams are present at all larger SAP locations. In the event of an emergency, these teams are immediately deployed and work closely with the responsible departments.
Does SAP have a network of crisis management teams that act at local, regional, and global levels?	Yes. These teams are trained and reviewed regularly.

Security Officers and Security Departments

Is there a person or department responsible for information security?	The central security department of SAP is responsible for information security.
Does SAP outsource any parts of its security management?	No. Security management is not outsourced. It is the full responsibility of the internal SAP security departments.
Does SAP have an information security team that oversees security awareness?	Yes. Both the central security department and the decentralized security units of SAP help the corporate communications department in this area.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

The Best-Run Businesses Run SAP®