BIZERBA

Information security annex
General requirements

Version from 04.02.2024

Internal - do not pass on to third parties

The following document contains three annexes on requirements for service providers and suppliers. These appendices are an integral part of our Information Security Management System (ISMS) and define the necessary security measures and policies that must be followed by our partners.

Annex overview

ISMS – Annex for supplieres and service managers – IT Security

This document defines the general security requirements that all suppliers and service providers must meet to ensure the security of our systems.

ISMS- Annex for supplieres and service managers – Maintenance

This annex describes the specific requirements and procedures for the maintenance of IT systems and equipment by external service providers to ensure that all maintenance work is carried out safely and reliably.

ISMS- Annex for supplieres and service managers – Software and Product development

This document defines the security requirements for software and product development. It describes the necessary measures to be taken by employees and suppliers to ensure the security and integrity of the software and products developed.

BIZERBA

Information security annex
General requirements for the contractor's IT security

Version from 04.02.2024

Internal - do not pass on to third parties

Change tracking

Revision	Date	Author	Comment	Release	Date
0.0	20.11.2023	J. Müller	Initial Version		
0.1	02.02.2024	J. Müller	Adjustments in context ISO27001		
0.2	05.02.2024	J. Müller	Adjustments in context ISO27001		
0.3	06.02.2024	J. Müller	Adjustments Bizerba CI		

Table of contents

1 General information

Further additive systems apply for remote maintenance and external programmers.

2 Contact person

a) The contractor must name a qualified contact person to the client who can provide information on IT security issues at any time. The contact person must provide the following information: Name, function, company, business address, telephone number and e-mail address.

b) The Client must name a contact person to the Contractor to whom the Contractor can provide information and communicate information in accordance with this Annex. The Client's contact person is:

Security contact person, contractor	Security contact person, client
Name: _____	Name: _____
Function: _____	Funktion: _____
Company: _____	Company: _____
Business address: _____	Business address: _____
Phone number: _____	Phone number: _____
E-mail adress: _____	E-mail adress: _____
	General Information Security Office requests: informationsecurityoffice@bizerba.com

3 General requirements

a) The Contractor is obliged to implement and maintain a recognized information security management system (e.g. in accordance with ISO 27001 or BSI Standard 200-2) in order to ensure adequate protection of all information.

b) The Contractor must use a recognized framework for the management and control of IT (IT governance) when organizing its IT processes. Recognized IT governance frameworks are ITIL (IT Infrastructure Library) or COBIT (Control Objectives for Information and Related Technology).

c) If the client so wishes, the contractor must ensure that certain data specified by the client is completely and reliably deleted within a specified period, subject to statutory retention periods.

4 Security of the Contractor's IT

a) The Contractor must implement appropriate virus protection (for servers, workstations and other IT components with access to information or systems requiring protection) and other security measures against malware (such as Trojan detection, spam protection) and keep them up to date with the latest technology.

b) The Contractor must ensure a secure basic configuration of its IT infrastructure, e.g. by using hardened operating systems on servers and clients and deactivating functions and network ports in its systems that are not required.

c) The Contractor is obliged to continuously monitor and log all activities of the administrators to detect attacks or operating errors and to keep the log files securely for at least three months.

d) The Contractor must carry out regular data backups.

e) The Contractor must ensure that the Contractor's data can only be read, changed and processed by persons who are involved in the services to be provided, the current project or collaboration.

f) Any portable data carriers used for the provision of services must be reformatted before each use and the data stored on them must be encrypted using Microsoft BitLocker or another state-of-the-art encryption technology and a password of at least 12 characters.

g) The Contractor must implement a risk management system to identify potential threats to information security and take appropriate measures.

h) The Contractor must draw up an IT contingency plan in order to be able to react quickly and effectively in the event of a security incident. A copy of the table of contents of the IT contingency plan must be provided upon request by the client.Der Auftragnehmer muss dem Auftraggeber auf Anfrage sein IT-Sicherheitskonzept sowie alle relevanten Dokumente, Zertifikate, Nachweise oder Berichte zur Verfügung stellen, die die Einhaltung der IT-Sicherheitsanforderungen belegen.

i) Upon request, the Contractor must provide the Client with its IT security concept and all relevant documents, certificates, evidence or reports that demonstrate compliance with the IT security requirements.

j) The Contractor shall be responsible for ensuring that its employees who have administrator rights can only access systems and applications operated on behalf of the Client via two-factor authentication. This ensures that access to sensitive data and systems is protected by an additional layer of security.

k) The Contractor shall ensure that all access rights are assigned on the basis of a clear, predefined role concept. This role concept shall be reviewed regularly to ensure that it meets current requirements. The client is responsible for ensuring that access rights are withdrawn immediately in the event of changes to the role concept or termination of this agreement in order to guarantee the security of the data and systems.

l) The Contractor is obliged to comply with the principle of separation of functions when allocating tasks. This means, in particular, working towards a distribution of administrative activities to ensure that no single person has excessive control over the systems and data. Particular attention must be paid to the separation of functions between operational and controlling functions and to the separation of functions in the administration of roles, approval and assignment of access rights. This helps to ensure the security of data and systems.

5 Requirements for the Contractor's personnel

a) The Contractor is obliged to train and sensitize its employees regularly, but at least once a year, with regard to ensuring information security at its own expense. Upon request, the Contractor must provide the Client with proof that the training courses correspond to the latest state of knowledge in information security and have been carried out.

b) The Contractor shall be obliged to inform the employees it deploys in the course of fulfilling its contractual obligations towards the Client of the special confidentiality requirements in connection with ensuring information security and the contractual confidentiality obligation with regard to the handling of the Client's data and systems prior to their deployment. The Contractor must document this in a suitable form.

c) If an employee of the Contractor does not comply with the Contractor's IT security rules, the Client reserves the right to reject this employee for further services. The Contractor shall then immediately provide another employee who meets the requirements.

6 Installations, systems and buildings of the contractor

The contractor must ensure that only authorized persons have access to areas with information or systems with high or very high protection requirements. This is achieved through continuous monitoring and access protection measures, such as intrusion protection, access control systems, video surveillance, security personnel and alarm systems. In this way, the integrity of critical areas is guaranteed.

7 Incidents at the contractor

a) The Contractor must immediately report to the Client all incidents that could impair or jeopardize the security, availability, integrity or confidentiality of the Client's IT systems, data or services. The information on the incident must be sent to informationsecurityoffice@bizerba.com in German or English.

b) The Contractor must provide the Client with all relevant information about the cause, scope, effects and the measures taken or planned to remedy and prevent the incident.

c) The Contractor shall cooperate with the Client in the investigation, analysis, evaluation and resolution of the Incident and shall follow all reasonable instructions of the Client.

d) De The Contractor must regularly report to the Client on the status and progress of the resolution of the incident and prepare a final report once the incident has been closed.

8 Data protection requirements

a) Introduction of a procedure to check and ensure that only the personal data necessary for the respective processing purpose is collected and processed. This also includes a regular review of data processing activities to identify and eliminate unnecessary data collection.

b) Encryption of personal data:
In addition to the aforementioned encryption of portable data carriers, it should be specified that all personal data that is transmitted, stored or processed must be protected using strong encryption methods. This also includes the encryption of data during transmission via public networks.

c) Access controls and authorisation management:
Detailed implementation of the processes and control mechanisms for managing access rights to personal data. This includes the implementation of procedures for granting, reviewing and withdrawing access rights as well as the use of the least privilege principle and segregation of duties to ensure that employees only have access to the data they need to fulfil their tasks.

d) Logging and monitoring:
Execution of logging and monitoring measures to ensure that all access to personal data and systems processing such data are logged and monitored. This should include regular review of logs for unauthorised access or suspicious activity.

e) Data protection-related training:
Specify the requirements for data protection training for employees who have access to personal data. This training should cover aspects of data protection, data security and rules of behaviour when handling personal data and should be regularly updated to comply with the latest legal requirements and best practices.

f) Procedure for data breaches:
Introduction of a specific procedure for the notification and handling of data breaches, including the notification of the client and data subjects in accordance with the requirements of the DSGVO.

g) Confidentiality agreements:
Introduction of a regulation that ensures that all employees who have access to personal data in the course of their work sign a confidentiality agreement. This agreement should clearly set out the obligation to maintain the confidentiality of this data and the consequences of breaching it.

9 General requirements for contractors and subcontractors

a) The Contractor must ensure that it and its subcontractors comply with the applicable statutory and contractual provisions for the protection of IT security and the personal data of the Client or third parties.

b) The Client shall have the right to inspect the IT documents and the IT infrastructure of the Contractor or its subcontractors at any time in order to ensure compliance with the IT security requirements.

c) The client can carry out remote audits as well as on-site audits or have them carried out. The client may determine the type, scope, time and frequency of the audits at its own discretion.

10 Management and return of information and company values of the client

a) If an employee of the Contractor is no longer working for the Client or the project or service is completed, the Contractor must ensure that all items, information, documents or similar assets (collectively referred to as ‘Company Assets’) received from the Client are properly returned.

   These include, among others:

   - Company ID and access cards
   - Company devices such as computer, mobile phone, tablet
   - Documents of the client
   - information stored on electronic media,
   - other information for which there is no right of retention,
   - other company assets handed over.

b) The Contractor shall ensure that all knowledge and information that is important for the ongoing business operations of the Client is documented and handed over in a form agreed with the Client.

c) Information and documents that are not handed over at the request of the client in accordance with paragraph (b) shall be deleted or destroyed. Written confirmation of the deletion or destruction shall be provided to the client upon request.

Annex maintenance

General requirements for maintenance

Version from 04.02.2024

Internal - do not pass on to third parties

Change tracking

Revision	Date	Author	Comment	Release	Date
0.0	20.11.2023	J. Müller	Initial Version		
0.1	02.02.2024	J. Müller	Adaptations in the context of ISO27001		
0.2	05.04.2024	J. Müller	Adaptations in the context of ISO27001		
0.3	06.04.2024	J. Müller	References to General Guideline		

Table of contents

1 Definition of terms

Maintenance
Maintenance refers to the regular checking, updating and repair of computer systems, devices and networks to ensure that they are working properly and are up to date. This may include installing software updates, checking security settings and rectifying faults or problems.

Remote maintenance
Remote maintenance is a process by which a technician or service provider remotely accesses a computer system or network to perform maintenance, diagnose or fix problems. This makes it possible to respond quickly to problems without having to be physically present and can improve the efficiency and reliability of IT systems. It is important that remote maintenance is only carried out by authorised personnel and that all security protocols are followed to ensure the integrity and confidentiality of data

2 General

The agreement applies in addition to the document ISMS ISMS - ISMS -Annex for suppliers and service managers - IT Security

3 General requirements for maintenance

a) an employee leaves the Contractor's company, immediate measures must be taken to ensure that this employee can no longer perform maintenance tasks. This includes, in particular, the immediate withdrawal of all access rights to systems and applications operated on behalf of the Client. The contractor is responsible for ensuring that these measures are implemented quickly and effectively in order to guarantee the security of the client's data and systems.

b) Any transfer of data such as database tables or configuration settings from the client to the contractor is only permitted for error diagnosis and with the written consent of the client. Furthermore, any personal data may only be transferred in anonymised form.Der Auftragnehmer muss für ein reibungsloses Patch- und Änderungsmanagement bei Wartungen sorgen, welches das zügige Einspielen von Patches, Updates und Service Packs ermöglicht. Daneben muss der Auftragnehmer ein Release Management etablieren und mit dem Auftraggeber abstimmen.

c) In order to ensure that the patches, updates and service packs function without retroactive effect during maintenance in live operation, the Contractor must check them beforehand on test systems. The Contractor is obliged to create test reports and make them available to the Client.

d) If an employee leaves the Contractor's company, immediate measures must be taken to ensure that this employee can no longer perform maintenance tasks. This includes, in particular, the immediate withdrawal of all access rights to systems and applications operated on behalf of the Client. The contractor is responsible for ensuring that these measures are implemented quickly and effectively in order to guarantee the security of the client's data and systems.

e) The contractor must ensure that the Bizerba ISMS guideline for system managers and administrators is complied with. This means that Bizerba's security standards must be adhered to when making adjustments to the configuration and other maintenance tasks. The contractor is responsible for ensuring that its employees acting as system owners or administrators are aware of and comply with this policy in order to ensure the integrity and security of the client's systems and data.

4 Additional requirements for remote maintenance

a) The client determines the technology and the authentication methods for remote maintenance access.

b) Any remote maintenance must be authorised or initiated by the client, unless other contractual agreements apply. This ensures that all remote maintenance activities are properly monitored and authorised to ensure the security and integrity of the client's systems.

c) The client reserves the right to terminate or interrupt the remote maintenance at any time if there are concerns regarding security or data protection.

d) With regard to remote maintenance, it is important that all remote maintenance sessions, including RDP sessions, are closed immediately after the respective activity has been completed. This also applies to short breaks. The reason for this is that open remote maintenance sessions pose a security risk and can allow unauthorised access to company systems and data. Closing remote maintenance sessions immediately ensures the security and confidentiality of company data and resources and minimises the risk of security breaches

Annex for software and product development

Version from 04.02.2024

Internal - do not pass on to third parties

Change tracking

Revision	Date	Author	Comment	Release	Date
0.0	20.11.2023	J. Müller	Initial Version		
0.1	02.02.2024	J. Müller	Adjustments in context ISO27001		
0.2	04.04.2024	J. Müller	Adjustments in context ISO27001		

Table of contents

1 General information

This annex specifies the general organisational security requirements and minimum standards that contractors must meet to ensure that their products, software and services comply with the required security standards.

The agreement applies in addition to the document ISMS -Annex for suppliers and service managers - IT Security.

General organisational requirements

1) The Contractor undertakes to ensure the security of the software development life cycle process by complying with generally recognised security standards. This includes in particular reviews, automated tests and vulnerability tests. Prior to commissioning, the Contractor must subject all applications for the Client to a review for application vulnerabilities and, if necessary, eliminate any vulnerabilities identified..

2) The Contractor shall guarantee the state of the art of information security in all its products and services. The Contractor shall always adapt the state of the art in existing maintenance contracts in appropriate maintenance cycles and take into account corresponding technical developments.

3) The Contractor is responsible for ensuring efficient patch and change management that enables patches, updates and service packs to be applied quickly. In order to ensure that the patches, updates and service packs work in productive operation without repercussions, the Contractor must check them beforehand on test systems. The Contractor is obliged to create test reports and make them available to the Client on request.

4) If very critical vulnerabilities (according to CVE ratings) become known, the manufacturer is obliged to check promptly and at his own expense whether his product is affected and to comply with the data minimisation and purpose limitation.

5) Introduction of a procedure to check and ensure that only the personal data necessary for the respective processing purpose is collected and processed. This includes a regular review of data processing activities to identify and eliminate unnecessary data collection.

6) Encryption of personal data:
In addition to the aforementioned encryption of portable data carriers, it should be specified that all personal data that is transmitted, stored or processed must be protected using strong encryption methods. This also includes the encryption of data during transmission via public networks.

7) Access controls and authorisation management:
Detailed implementation of the processes and control mechanisms for managing access rights to personal data. This includes the implementation of procedures for granting, reviewing and withdrawing access rights as well as the use of the least privilege principle and segregation of duties to ensure that employees only have access to the data they need to fulfil their tasks.

8) Logging and monitoring:

Execution of logging and monitoring measures to ensure that all access to personal data and systems processing such data are logged and monitored. This should include regular review of logs for unauthorised access or suspicious activity.

9) Data protection-related training:
Specify the requirements for data protection training for employees who have access to personal data. This training should cover aspects of data protection, data security and rules of behaviour when handling personal data and should be regularly updated to comply with the latest legal requirements and best practices..

10) Procedure in the event of data breaches:
Introduction of a specific procedure for the notification and handling of data breaches, including the notification of the client and data subjects in accordance with the requirements of the GDPR.

11) Confidentiality agreements:
Introduction of a regulation that ensures that all employees who have access to personal data in the course of their work sign a confidentiality agreement. This agreement should clearly set out the obligation to maintain the confidentiality of this data and the consequences of breaching it.

12) During the entire operating period, the Contractor guarantees that any vulnerabilities discovered in the deliveries and services will be remedied quickly and promptly and at its own expense (within the framework of existing maintenance contracts) or that a suitable workaround will at least be offered to mitigate the threat until it is finally remedied. For unpublished vulnerabilities, a maximum period of 60 days applies; for publicly known vulnerabilities, a maximum period of 3 days applies to mitigate the threat.

13) The range of functions and therefore the number of existing programmes, software modules, services and network protocols on components are reduced to the minimum required for system operation. All services that are not explicitly required are deactivated by default. If a system is accessible to a larger group of users or has very critical functions, a granular role and authorisation system must be enabled. Standard combinations of user names and passwords must be changed or be changeable during the initial configuration. By default, each component and each user only has the rights required to perform an action. For example, applications and network services are not operated with administrator privileges, but only with the minimum necessary system rights (least privilege principle).

14) Applications must be able to carry out person-specific identification and authentication. The system must not allow any actions without successful user authentication. Access to data and variables may only be possible after a successful authentication and authorisation check. If passwords are used, the system must enforce passwords with a strength and validity period defined by the client (password policies). There must be no hard-coded combination of user names and passwords. Ideally, the solution should offer the option of secure multi-factor authentication. Two-factor authentication is mandatory for deliveries and services that are directly accessible via the Internet and whose access is not restricted to legitimate network connections..

15) The Contractor undertakes to keep its products and services free of malware, spyware, hidden code, undocumented backdoors or other hidden functions (such as unauthorised data forwarding) that are

capable of compromising the information security of the deliveries and services. Accounts that are not absolutely necessary for operation shall be removed or at least deactivated.
If the Contractor uses standard software in the deliveries and services (e.g. operating system, database), it shall permit the installation of security software selected and licensed for this standard software by the Operator and enable its integration without the Customer losing any warranty claims to the deliveries and services. Common security software is, for example, software for inventory, malware defence, identity management, SIEM, intrusion detection, DLP, vulnerability detection, etc.
In addition, the deliveries and services must offer mechanisms that allow (D)DoS attacks to be mitigated or at least restrict network access to legitimate connections (e.g. based on firewall rules)..

16) The Contractor is obliged to take appropriate measures, such as the use of escrow (deposit of the source code and regularly updated data/information), taking into account the confidentiality agreements and data protection requirements, to ensure that the Client's operations are not significantly disrupted in the event of the Contractor's insolvency and that the contractual services can continue to be provided seamlessly by the Client itself or a third party.

17) If the Contractor uses test data for the development of applications and systems, these must be carefully and comprehensibly selected, protected and controlled. Anonymised or pseudonymised data shall be used. The use of real data requires the prior consent of the client. Furthermore, the test systems must fulfil the same security requirements as the production systems.

18) The Contractor must create and implement a written policy that defines the permissible cryptography algorithms to ensure that no outdated and insecure cryptography solutions are used in the products provided, sold or used by the Client. This guideline must comply with an industry standard (e.g. BSI TR-02102 in the current version) and be reviewed regularly. It must be made available to the client on request.

19) If an applied cryptography solution becomes known to be insecure, the policy and implementation must be adapted. If such a cryptographic solution is used in a product or application already deployed by the client, the contractor must assess and report it as a vulnerability as part of the vulnerability management process. The contractor must submit suggestions for circumventing the vulnerability.

20) If the Contractor develops web applications for the Client, the Contractor undertakes to carry out the development processes in accordance with the recognised web standards for secure software development. These include, for example, the principles of the Open Web Application Security Project (OWASP). The Contractor shall take all technically possible and reasonable precautions in the specific case to protect the contractual software against known attack techniques such as SQL injection, cross-site scripting, denial of services attacks, brute force attacks and man-in-the-middle attacks.

21) The Contractor shall ensure that only employees of the Contractor entrusted with the development have access to the source code.

2 Programming requirements

The Contractor undertakes to comply with at least the following security requirements when developing its devices, applications and cloud applications:

a) All applications and systems must not contain any backdoors or undocumented interfaces

b) All standard passwords of a system must be able to be changed by the client

c) The client-side source code should be free of sensitive business logic and must be free of secret keys.

d) Authentication controls must always fail in the event of incorrect access data in order to ensure that no unauthorised access is possible.

e) A ‘forgotten password’ function must never reveal the current password. In addition, all account access recovery functions must be at least as secure as the primary authentication mechanism.

f) New passwords must never be sent in plain text via insecure channels. Any security issues must be privacy compliant and strong enough to protect accounts from malicious recovery.

g) Admin interfaces must not be accessible to untrustworthy persons.

h) For server/client applications, old sessions must become invalid when a user logs out again and new session IDs must always be generated for login and authentication. The application may only accept self-generated session IDs that are sufficiently long, random and uniquely distributed across the set of sessions.

i) Access to sensitive and confidential data must be protected and directory browsing and listing must be disabled.

j) The application must be protected against LDAP and SQL injections.

k) The application must not log any sensitive data that could assist an attacker, including session identifiers, passwords, hashes or API tokens.

l) Sensitive data must not be stored unprotected. On the server and client, all cached or temporary copies of sensitive data must be protected against unauthorised access and cleaned up at the latest after the end of the session.

m) The same encoding must be used between client and server and alternative, less secure access paths are not permitted..