Aareal

Contract Annex

Information Security Specifications

Last revised: July 2023

2458

Table of contents

1. Purpose and objective of the Information Security Annex

These requirements and strategic objectives are firmly entrenched within the Information Security Strategy of Aareal Bank AG (the "**Bank**"). The Contractor is likewise subject to requirements as to the form and quality in which the confidentiality, integrity, authenticity and availability of information, data and systems (collectively referred to as "**protection objectives**") are to be ensured.

The Contractor shall meet these requirements by implementing the provisions on information security (collectively referred to as "**information security specifications**") set out in this "Contract Annex – Information Security Specifications" (the "**Information Security Annex**") in accordance with the required level of protection set out by the Bank (see section 3.1) as described or in an equivalent manner. This entails complying with all laws and regulations applicable to information and communication technology ("**ICT**"), which expressly includes regulatory requirements such as the Supervisory Requirements for IT in Financial Institutions (BAIT) or Cyber Resilience Oversight Expectations (CROE).

2. Scope of application

The information security specifications apply if and insofar as the services of the Contractor comprise the operation, customised creation and/or customised adaptation of software and/or the Contractor stores or otherwise processes data of the Bank (e.g., business data received from the Bank or generated by the Contractor in the course of rendering its services for the Bank) on its systems for the purpose of or in connection with rendering its services. In all other respects – i.e., issues, processes or activities of the Contractor which are not relevant to or not used for the services under contract with the Bank – the information security specifications do not apply.

If and insofar as the Contractor arranges for the aforementioned actions to be carried out by subcontractors, the Contractor shall ensure that its subcontractors also comply with the information security specifications and shall monitor this on an ongoing basis.

3. General

The Bank regularly reviews the implementation of the information security specifications.

3.1 Required level of protection

The information security specifications are guided by the required level of protection of the systems in question. Accordingly, in the following some requirements are divided in a matrix according to the required level of protection and the protection objective. If aspects overlap, the stricter interpretation must be selected.

If and insofar as the information security specifications differentiate between protection objectives, the following required levels of protection shall apply to the respective protection objectives:

	Low	Medium	High	Very high
Confidentiality				
Integrity				
Availability				
Authenticity				

Where no differentiation is made according to protection objective, the following required levels of protection shall apply:

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity				

The Bank reviews the required level of protection on an annual basis as well as ad hoc. It will notify the Contractor of any changes in writing or in text form; in this case, the Contractor must adjust its implementation of the information security specifications accordingly.

3.2 Deviations, target/actual comparison

The Contractor must compare the implementation of the information security specifications with the actual information security specifications ("**target/actual comparison**") both ad hoc and on a regular basis, but at least

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	every three years		annually	

and report the results to the Bank.

Moreover, the Contractor must inform the Bank without delay if it becomes aware, outside of the target/actual comparison (e.g., due to or as a result of findings by auditors, internal and external audits or security tests (e.g., penetration tests, vulnerability scans)), that one or more information security specifications have not been implemented or have not been implemented in full.

If one or more information security specifications are not (fully) implemented, a decision on how to handle these deviations must be made on a case-by-case basis. This decision ...

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	can be made by the Contractor without consulting the Bank.	can be made by the Contractor without consulting the Bank but must be communicated to the Bank.	must be approved by the Bank in advance.	

3.3 Definitions and interpretation of information security specifications

Unless otherwise defined in this Information Security Annex, the terms used in this document always have the meaning ascribed to them in the contract to which this Information Security Annex is annexed (the "**main contract**").

In addition, the interpretation of the information security specifications is subject to the following:

(1) **"Must" specifications:** Information security specifications containing the words "must", "shall", "is/are to", "shall not", "may not" or any derivative thereof are mandatory in all cases.

(2) **"Should" specifications**: Information security specifications that contain the words "should", "should not" or any derivative thereof are mandatory if and insofar as there are no justified reasons for a deviation. If and insofar as there are justified reasons for a deviation, the Contractor must document these reasons and the effects of the deviation on information security in writing and submit them to the Bank for review before deviating from the information security specification in question. Such documentation must generally be provided to the Bank upon request.

(3) **"May" specifications**: Information security specifications containing the words "may", "can" or a derivative thereof are not mandatory but are to be implemented by the Contractor on a voluntary basis.

3.4 Regulations, state of the art and standards

All specifications must be implemented in accordance with regulatory requirements, the state of the art and recognised industry standards. The Contractor is required to report any obsolete, missing or inadequate information security specifications to the Bank on an ad-hoc basis.

3.5 – content not yet available –

3.6 Information and communication technology (ICT) systems

According to EBA Guidelines EBA/GL/2019/04, **ICT systems** within the meaning of this Information Security Annex (also referred to herein simply as "**systems**") are an "ICT set-up as part of a mechanism or an interconnecting network that supports the operations of a financial institution".

ICT systems or components of ICT systems include servers, networks, databases, business-managed applications (BMAs) and IT-managed applications (ITMAs), for example.

3.7 Changes relevant to information security

Changes that may impact the level of information security or the risk assessment with respect to information security are relevant for information security. Such changes may, for example, arise in connection with projects, software changes or occurrences in IT operations.

4. Information security specifications for the organisation

4.1 Collaboration

The Contractor is required to support the Bank in managing information security and to make the necessary information available.

4.2 – content not yet available –

4.3 Documented operating processes

The Contractor shall prepare documentation on systems and company processes that

a.) comprises all major operating processes,

b.) is available to the relevant users and

c.) …

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	at least once a year		at least once a year and ad hoc	

... and, where necessary, updated and completed.

4.4 Segregation of duties

The Contractor must ensure that conflicting duties and areas of responsibility are segregated and that the various roles are designed accordingly. The roles for the development, testing, acceptance and deployment of new systems and applications or changes to existing systems and applications must be designed to be free of conflicts of interest and documented in the respective authorisation policy.

Duties, areas of responsibility and/or roles conflict with each other if they are supposed to be separate in organisational/procedural terms in the interest of risk mitigation (for example, principle of dual control/segregation of duties (SoD)).

4.5 Education, awareness and training

All employees deployed must receive regular, target group-specific training on security awareness topics. The Contractor must ensure that the employees deployed know the specific procedures and guidelines with security relevance in their specific field of work.

4.6 Inventory-taking

The Contractor must ensure that all of its systems are documented and regularly maintained in inventory systems.

4.7 Segregation of systems

When creating source code or making individual adjustments to software, i.e., amending software beyond the planned configuration settings, the Contractor ...

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	can	should	must	

... operate the development, test and operating environments separately from each other to reduce the risk of unauthorised access to, or modification of, the data and source code.

4.8 Physical access rules

Premises at which the Contractor performs its services and/or at which other information-processing facilities are located, in particular security-critical areas, must be protected against access by unauthorised persons. Visitors, workmen and other external third parties should not be allowed to move freely and unchecked or without an escort on the premises except where required under the scope of their activities.

Especially ICT infrastructures (e.g., server and distribution rooms, data centre) and other areas of the company deserving special protection (e.g., Management Board) must be protected against unauthorised access/entry by means of suitable physical and logical measures.

If an employee is absent for a longer period of time, the employee's access authorisation must be temporarily blocked by the system. Points of access such as delivery and loading areas as well as other points through which unauthorised persons could enter the premises must be monitored and, where possible, kept separate from information processing facilities in order to prevent unauthorised access.

4.9 User access management

4.9.1 System and data access rules

System and data access authorisations for networks, systems, applications and information must only be provided if and for as long as they are required to fulfil the relevant task (*need-to-know principle*).

User accounts may only be assigned those access rights that are absolutely necessary for the performance of tasks – no more and no less (*least-privilege principle*).

All applications featuring authorisation management must have an authorisation concept, which is to be reviewed at least annually.

For this purpose, a system and data access policy must be created, taking into account the following security-relevant and business requirements:

- The allocation of authorisations may only be carried out via authorisation applications and must be verifiably documented, including the release process.
- Accounts and their authorisations must always be assigned to a responsible person.
- Before granting user authorisations, the person to receive the authorisation must be unmistakably identified.
- The modification, deactivation or deletion of authorisations is subject to the processes in the corresponding authorisation concepts and must be verifiable.

- Standard authorisations based on certain user attributes (e.g., belonging to an organisational unit) can be assigned automatically. These kinds of rules must be documented in the authorisation concept.
- The authorisation concept must define approval levels that meet at least the following requirements:
    - Business-critical authorisations (as defined in section 4.9.2) and critical authorisations (as defined in section 4.9.3) must be approved according to the principle of dual control as a minimum (i.e., a dual control system must be in place).
    - Self-approvals in the role of a manager are not permitted.
    - The person responsible for the authorisation must be involved.

4.9.2 User management

All user accounts must be subject to a formal process for creating and deleting/deactivating users and their authorisations, as well as for regular recertification. This also includes technical users.

Business-critical and critical authorisations (as defined in section 4.9.3) must be reviewed (recertified) at least twice a year and other authorisations at least once a year.

Authorisations are considered **business-critical** if they allow users to access sensitive data that is of client-specific or business-specific relevance to the Bank. This includes personal data, such as master or transaction data, as well as key risk indicators that are not publicly accessible.

In the context of user management, the same control authorities must be involved as for the initial creation of users and their authorisations (e.g., the person with functional responsibility). Self-recertification shall not be permitted.

In the event that users plan to be absent for a longer period of time, the user accounts concerned must be blocked in all applications and services whose required level of protection is high or very high. The same applies if an unplanned absence goes on for an extended period of time.

In all other cases, user accounts that are no longer required must be blocked and the authorisations withdrawn.

4.9.3 Highly privileged users (HPUs)

Highly privileged users must be identified and monitored separately to ensure that they carry out their daily tasks without deviating from the framework provided and that no unauthorised activities take place.

Highly privileged users or **HPUs** are to be understood as users who possess or are able to manage one or more of the following authorisations in bank processes, in regulatory, accounting, risk- or management-relevant systems or on their infrastructure components, and who are to be dealt with accordingly (e.g., with regard to monitoring or risk mitigation through technical/organisational measures):

- Creating and deleting user accounts
- Configuring software or hardware components (including interfaces)
- Deleting log files
- Managing cross-system security mechanisms (e.g., switch on/off)

- Managing backups and system restorations
- Configuring communication channels

The Contractor must ensure that only sufficiently qualified employees possess user authorisations that lead to their being classified as HPUs and work for the Bank with such user authorisations.

If technical users (especially with hard-coded HPU login details) hold such rights they must be monitored accordingly.

"**Critical authorisations**" conform to the criteria for the definition of HPUs. As soon as an account holds a critical authorisation, it is classified as an HPU.

"**Emergency accounts**" or "**emergency IDs**" are IDs for user accounts with critical authorisations (HPUs) for use in emergency activities that cannot be performed using administrative user accounts.

4.9.4 Auxiliary programmes with privileged rights

Auxiliary programmes capable of circumventing system and application protection measures such as those mentioned in section 4.9.3 must only be available to authorised users. The options for the use of such software must be restricted and monitored.

4.9.5 Remote maintenance access

If and insofar as external access to IT components in the local network is set up for the purpose of maintenance or troubleshooting, with such access usually established via the Internet, the following must be implemented in addition to the user access regulations and authorisations:

(1) Support or remote maintenance sessions must always be initiated by the Contractor (principle of dual control).

(2) All remote maintenance connections must be encrypted.

(3) The person carrying out the remote maintenance must be authenticated reliably before gaining access to the system. Strong multi-factor authentication should be used.

(4) Access must be created so that the person carrying out the remote maintenance has no access to computers outside the specified area of activity.

(5) Modifications made to the central security gateways in order to establish the remote maintenance access shall be kept to a minimum.

(6) The performance of remote maintenance must be logged.

(7) Once the tasks have been completed, the remote maintenance session shall be terminated.

4.9.6 Password rules

The following technical minimum standards apply for passwords:

(1) Password validity: The duration may be unlimited if the password includes at least 2 factors from the categories of knowledge, possession and inherence/biometrics; otherwise, the password must be changed regularly.

(2) Password length: Must have a minimum of 16 characters; if the password includes at least 2 factors from the categories of knowledge, possession and inherence/biometrics, the length can be reduced to 8 characters.

(3) Password complexity: Must contain a minimum of three from the following four options: upper and lower case letters, special characters and numbers.

(4) Password history: May not be the same as the last 10 passwords used.

(5) Passwords may not be displayed and transmitted in plain text (however, displaying plain text at the user's request through a deliberate action is permitted).

(6) After several (5-10) incorrect password entries, the user must be locked. The user can be automatically unlocked after a specified period of time (e.g., 15 minutes).

(7) Initial password changes must be enforced.

(8) If technically possible, HPUs should have a regular rotation of passwords.

The following additional minimum standards must be implemented at least in organisational (but not necessarily technical) terms:

(1) Passwords may not correspond to or include user names or IDs or parts thereof.

(2) Passwords must not be entries in the Duden or a foreign language dictionary.

(3) Passwords must not be programmed into scripts.

(4) Passwords must only be submitted in plain text in the password manager, otherwise a password hash must be used (exceptions for business continuity management must be clarified individually).

If parts of the rules cannot be implemented for technical reasons, e.g., because the software is not able to map the rules, the deviation must be reported to the Bank and/or additional security measures taken. The procedure in connection with such deviations is ...

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	to be developed/		to be developed with the Bank's consent.	

This must be documented and noted as part of the target/actual comparison.

4.9.7 Choosing passwords

When choosing a password, the technical password rules (see section 4.9.6) must be applied. Passwords automatically assigned during software installation must be replaced immediately with your own passwords.

Initial passwords must be unique and randomly generated.

Passwords created by third parties must be replaced immediately by a password of your own.

Newly created, reset or default passwords must be changed after their first use. This must be a mandatory system feature.

4.9.8 Resetting passwords

Wherever possible from a technical and organisational point of view, an automated procedure must be used for password resetting.

Reset passwords must be replaced immediately by a password of your own.

4.9.9 Transmitting passwords

An initially assigned password must be communicated to the user in such a way as to prevent unauthorised third parties from gaining knowledge of it.

4.9.10 Storing passwords

Passwords required for BCM and security purposes and thus to maintain operations may be physically stored. Such passwords must be

- kept in custody and protected against unauthorised access and
- changed after being used.

Moreover, such passwords may also be stored in a suitable password manager within the Contractor's systems. The password for these files must only be known to the emergency users (users of emergency accounts) in question.

4.10 Change management

Changes to ICT systems or applications or to the underlying architectures and technologies are to be recorded and controlled in a traceable (documented) manner.

Security-critical changes may not be implemented without the consent of the Bank if they could adversely affect the Bank's security level.

Time-critical faults can lead to the need for *emergency changes*. In these cases, the change must be coordinated with the Bank afterwards.

4.11 Upholding information security within the framework of BCM

In the event of emergencies/crises or disasters, the Contractor must attain the best possible protection depending on the situation. In the process, the required levels of protection for the respective protection objectives must be taken into account.

During a disruption relevant to business continuity management (**BCM**), the protection objectives must be safeguarded as much as possible. It is likely that the level of protection according to these information security specifications cannot be maintained during a BCM-relevant disruption. Therefore, it is necessary to determine within the framework of BCM which level of protection is acceptable. This level must be communicated to the Bank insofar as it concerns the service provided to the Bank or the Bank's data. Processes, procedures and measures on how the relevant protection levels are to be achieved or maintained must be documented. The BCM documentation must be regularly reviewed and, if necessary, updated.

4.12 Lifecycle security requirements for ICT systems

The information security specifications must be taken into account when introducing new and changing existing ICT systems.

This means that the information security specifications must be incorporated in the requirements governing a new system (requirements specifications) or in any changes (see section 4.10).

4.13 Special provisions governing transfers within networks

Information which is transferred by public networks must be encrypted in accordance with section 5.5. This must be ensured through the corresponding transmission channels which are made available by the ICT operators. End user communications such as e-mail do not fall under these rules but must also be subjected to secure handling.

In addition, it is necessary to

- set out which information may be transmitted and who may authorise its release,
- ensure that the communication partners are clearly identified prior to the transmission of information, and
- select appropriate transmission methods to protect the integrity of the information.

If services of the Contractor are involved in financial transactions, the following special security measures must be taken:

- User authentication information is valid and has been verified.
- Transaction data must be secured at a storage location that is not publicly available.

4.14 Application development and deployment

Internal guidelines must exist for the development of software and systems. When creating and adapting programs, security aspects for the protection of information must be taken into account in accordance with the s*ecurity-by-design principle*.

Changes to systems must be processed, managed and documented as part of the change process (see section 4.10).

To ensure that changes to the technical platforms of the material applications do not have an adverse impact on operations and information security, the applications must also be tested on a risk basis in such cases.

Standard software should be used in the form provided by the manufacturer without changes wherever possible. Should changes to the standard software be unavoidable, the consequences - such as ability to be maintained, updates to new versions, compatibility with other software and effects on control mechanisms - should be taken into account

For internal development processes/projects, procedures should be used that take into account the information security specifications in terms of analysis, development and maintenance.

Access to the development environment and, in particular, to the source code of programmes must be restricted on the basis of the *need-to-know principle*. The documentation of sensitive system information, configurations or source code (possibly in repositories) must be protected against unauthorised access and loss.

4.14.1 Outsourced development

If the Contractor (or a subcontractor of the Contractor) creates or adapts software at the request of the Bank, best practices in the field of secure application development must be taken into account. The specifications of the Federal Office for Information Security (BSI), for example, serve as a reference.

4.14.2 Acceptance test and system security

New or changed hardware or software must be tested before the first use.

The tests performed during the development of systems must always also include a test of the relevant information security specifications. The scope of tests should correspond to the importance and characteristics of the system. The type of change should also be taken into account.

4.15 Test data

The data of the Bank may not be used for testing purposes without first obtaining the Bank's consent in writing or text form.

4.16 Information security incidents, incident management

Term	Definition in accordance with ISO27000
Information security	Maintaining the confidentiality, integrity and availability of information. Note on the term: in addition, other characteristics such as authenticity, accountability, deniability and reliability can be included.
Information security event (ISE)	Identified emergence of the status of a system, service or network which indicates a possible violation of the information security policy or the ineffectiveness of measures or a previously unknown situation which may be security-relevant.
Information security incident (ISI)	Individual unwanted or unexpected information security event or a series of such events materially likely to jeopardise business activities and to threaten information security.

An information security incident may be, for example:

- Unauthorised **physical access** to the data centre or other security-critical rooms;
- Unauthorised **system access** through use of an account by an unauthorised third party (e.g., the password was identified), or
- Unauthorised **data access** by interception or tampering with files, e.g., if a user account was misused to this end or sensitive data/data transfers were not encrypted.

The Contractor must report information security incidents immediately and directly using the contact details provided by the Bank in accordance with the operating documentation.

For information security incidents in relation to the services to be provided to the Bank, reports to external third parties (e.g., public authorities) must only be made by or in coordination with the Bank's Chief Information Security Officer or his named deputy. Statutory reporting obligations of the Contractor remain unaffected by the aforegoing.

The responsibilities and procedures must be determined to ensure a rapid, effective and orderly response to information security incidents. Insights gained from the resolution and the analysis of information security incidents must be used to create risk-mitigating measures in order to sustainably improve the level of security by preventing the respective scenarios from occurring again.

Processes to establish, secure and store evidence material in a court-approved manner must be used.

All internal and external employees must be made aware of their responsibility to report information security events as quickly as possible.

4.17 Security tests

Testing and checking information security assets for information security within the scope of the ISMS (information network) is a central measure to determine the effectiveness of the protective measures and to detect any as yet unidentified vulnerabilities. The Contractor must subject systems that are of relevance to the services for the Bank to regular, risk-based security tests, e.g., penetration tests or vulnerability scans.

Test results that are relevant for the Bank (e.g., if systems or infrastructure are affected on which the Bank's data is processed) must be reported to the Bank regularly and promptly. Removal of the identified vulnerabilities must also be reported to the Bank.

If the security tests reveal critical vulnerabilities, these must be communicated to the Bank in writing without delay. **Critical** vulnerabilities are those with a score of 9.0 or higher under the Common Vulnerability Scoring System (CVSS) or those that have been classified as critical by a qualified authority (e.g., BSI, NIST).

5. Technical information security specifications

5.1 System hardening

5.1.1 Least functionality

Systems must be installed according to the *principle of least functionality*. This means that only components which are absolutely essential must be installed/active. This includes the intended application and its components, components necessary for integration into the local infrastructure and components necessary for maintenance. All services of software components not required for the provision of the service, for integration in the infrastructure or for maintenance must be deinstalled. Should de-installation not prove possible, these services must be deactivated.

Software used must be

- an official version approved by the developer which is stable and secure (*stable release*);
- intended for the release of the operating system; and
- configured securely (manufacturer standard configurations are considered not to be secure).

5.1.2 Network hardening

The network must be operated in separate groups (by users, services etc.). Only necessary ports must be open. All other ports must be closed. In addition, the configuration must be regularly reviewed and, if necessary, updated.

5.1.3 Protection against malware

To protect against malware, adequate identification, prevention and restoration measures must be implemented. In particular, this includes the use of virus protection on clients and servers.

5.1.4 Patch management

Any decision to update IT-specific solutions must take into account the business requirements for the change and the security of the specific version from the perspective of the information concerned.

Adjustments to the security architecture must be made at regular intervals to comply with the state of the art. This includes in particular system and security updates (see list below) and appropriate protection through an antivirus programme with daily signature updates.

A rollback strategy must be considered during planning. Previous versions of systems must be kept as a fallback.

The deployed systems must be checked for updates and release changes (minor and major) at least monthly and on an ad hoc basis.

Patches must be tested and applied ...

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	after 3 months at the latest		after three months at the latest in the case of BIOS/firmware and drivers, and otherwise after one month at the latest, unless the risk assessment requires a shorter period.	

If it is not possible to adequately review the patches, e.g., due to cost or lack of resources, patches may be deferred in order to first assess the associated risks on the basis of experience reported by other users.

Tests and upgrades of minor and major releases must be decided on and planned as part of change management. The procedure must be determined within...

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	any period.	3 months.	1 month.	

The patch/update/hotfix/bugfix must be tested before being implemented.

The patch-relevant systems include, as a minimum:

- BIOS/ firmware;
- operating systems;
- drivers of other components belonging to the operating system;
- middleware;
- operating and maintenance software;
- application software;
- mobile devices.

Deviating target periods apply for security patches designed to remedy critical vulnerabilities within the systems. In these cases, the time periods depend on the severity of the vulnerability to be remedied and must be determined by the Contractor in consultation with the Bank.

5.2 Data backup and recovery, data transport

Alongside availability and authenticity, the integrity and confidentiality of information are equally important from the Bank's point of view. Therefore, unauthorised access to data backups and data carriers must be prevented by both logical and physical means. Backup copies must be stored in such a way that the data carriers can be held there on a long-term basis. Stored backup media should be easily accessible.

As a minimum, the following qualities and frequencies must be adhered to:

	Low	Medium	High	Very high
Integrity	monthly backup	weekly backup	daily backup	
Availability	monthly backup	weekly backup	in line with the Contractors's own BCM stipulations, but daily backup as a minimum	

An annual check must be carried out to ensure that the existing backup copies are capable of being restored. The proper functioning of the backup copies must be tested on a random basis at the following intervals:

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	annually	half-yearly	quarterly	

Real cases of a restore during operation can be counted towards test cases.

Backup media are to be protected against access by unauthorised third parties by logical and physical means.

If backup media are transported between data centres outside the secured premises of the Contractor, the data carriers must be encrypted for physical transport and secured using appropriate physical measures.

5.3 Logging

Event logs which record user activity, exceptions, disruptions and information security incidents must be generated, stored and checked regularly by the Contractor.

Event logs may contain sensitive information and must therefore be protected from unauthorised viewing and manipulation. System administrators should have no authority to delete logs. Any deactivation of the logging function must follow the principle of dual control and must be documented in writing (reason, time period, persons involved).

The storage of the logs is guided by business-relevant requirements, but must not violate statutory provisions or regulatory requirements.

To prevent manipulation of the log files, they can be transferred to a suitable SIEM (s*ecurity information and event management*) system.

5.4 Time synchronisation

The clocks of all information processing systems are to be synchronised with a reference time source.

5.5 Cryptography

Cryptographic systems must be used as a minimum when data has to be transported via the public network (Internet) or in a network which is not considered to be sufficiently secure. Care must be taken to ensure that cryptographic systems conform to the state of the art at all times. Details must be discussed with the Bank.

Sensitive and personal data shall be protected appropriately and, where technically feasible, encrypted for storage.

The Contractor must document in writing which cryptographic procedures are permissible or are in use and to what extent data at the storage location as well as data and communication transfers are encrypted. The Contractor must also document the use, protection and entire lifecycle of key material.

Keys that have come to the knowledge of unauthorised persons, have been falsified during distribution or even come from an unverified source can compromise the cryptographic security mechanism, as can poor-quality keys that have been generated improperly. Such keys and keys that have been generated improperly shall be replaced immediately.

5.6 Network security management

The following aspects are to be dealt with by the Contractor:

- Responsibilities and procedures for the management of network technology;
- whether and how segmentation into security zones is implemented;
- in which cases a logical or physical network separation is implemented;
- which network and application logs are permitted; and
- how internal and external communication as well as communication between different locations takes place, including the necessary encryption.

5.7 Firewall rules

All communication with external systems or services must go via a firewall (internal/external). Furthermore, it must be ensured that only authorised connections from the Internet into the internal network (or vice versa) are established (whitelisting approach).

To support this, clear firewall rules must be defined for data traffic. All available infrastructure components (e.g., servers) which rely on connections with unreliable networks (e.g., Internet) must fulfil specific criteria as part of their data traffic. These are referred to as **firewall rules**.

As a minimum, the management of firewall rules must fulfil the following criteria:

- Regulated approval process: All change requests (creation, change, deletion) must be formally decided by set persons who are not identical to the applicant prior to their implementation.
- Documentation: All application and approval processes must be documented in writing. The last written decision for each firewall rule must be stored for 24 months.

- Recertification: All firewall rules must undergo regular recertification, at least every 12 months after their last change. Rules no longer required must be deleted as part of recertification following consultation with the persons concerned.
- Sets of rules: If required (e.g., in the event of an internal/external audit), all firewall rules must be presented to the Bank in complete and clearly understandable form (e.g., extract in Excel format).

5.8 Purchasing and maintenance of software

Prior to purchasing hardware and software for the services (and before obtaining web applications), the Contractor must determine the precise requirements for information security resulting from this Information Security Annex.

The Contractor must therefore check which information security specifications from this Information Security Annex are to be implemented and whether the software or hardware is capable of fulfilling them. If the new software or hardware to be purchased is not capable of meeting these requirements, ...

	Low	Medium	High	Very high
Confidentiality, integrity, availability, authenticity	it may not be used for the services unless it complies with specific conditions imposed by the Bank.		it may not be used for the services.	

5.9 Installing software in operations

When installing software during operation, care must be taken to ensure that

- change control for software on systems is observed during operation;
- the tasks are performed by trained administrators;
- the necessary internal approvals of the Contractor have been received;
- the software has been tested;
- a rollback strategy exists; and
- the replaced software versions are retained in the long term – the last 2 versions (minor release).

5.10 Redundancies

Unless stated otherwise in the main contract, ICT systems shall be designed as follows:

- Minimum availability of 95% if the required level of protection is low or medium and 99% if the required level of protection is high or very high.
- Operation in separate data centres if the required level of protection is high or very high. The distance between the data centres must follow the recommendations of the BSI.

5.11 Capacity management

One of the objectives of information security is to sustainably uphold the availability of information and thus of information-processing systems and resources. Use of IT resources must be monitored

and coordinated internally. Forecasts of future capacity requirements are to be made to ensure the necessary system performance.

5.12 Mobile devices

The employees deployed are to be given instructions for secure handling of mobile devices. The Contractor shall ensure that supplementary technical protective measures are implemented which mitigate the risks arising from the use of mobile devices, e.g., by encrypting the data carriers.

5.13 – content not yet available –

5.14 Mobile working / teleworking

The employees deployed are to be given instructions for secure handling of mobile working/teleworking. The Contractor shall ensure that supplementary technical protective measures are implemented which mitigate the risks arising from mobile working/teleworking.

5.15 Disposal of data carriers and other operating equipment

Data carriers no longer required must be disposed of securely using formal procedures. Disposal of all operating equipment must also include the secure disposal of data carriers.

Data carriers which cannot be disposed of must be securely deleted. To this end, the deleted data carrier must be overwritten with random data repeatedly, at least ...

	Low	Medium	High	Very high
Confidentiality	3		7	

... times.

The disposal or secure deletion of other hardware (e.g., leased or owned by the Contractor) must be agreed with the Bank in advance in each case.

5.16 Transfer of data to movable data carriers

Data may not be transferred to data carriers (e.g., USB sticks, external hard drives, CDs, DVDs, etc.) without the prior approval of the Bank.

5.17 Transport of data carriers

Data carriers must be protected against unauthorised data access and misuse and stored and transported securely, e.g., by means of encryption.

***