Information security requirements for suppliers (Technical and organizational security measures - TOMs)

A. INTRODUCTION

1. General

This document defines technical and organizational measures for processing ZKW information and for using IT systems in order to process ZKW information, which must be observed by suppliers and service providers - hereinafter referred to as **"contractors"** - of ZKW Group GmbH and/or of its affiliated companies in the sense above (a list of all companies is available here https://zkw-group.com/home/unternehmen/standorte/), referred to jointly or individually as "**ZKW**" or the **"client"**. The purpose of this is to ensure the protection of confidentiality, integrity, and availability for ZKW information.

These information security requirements are directed to the general management of the contractor, its employees, and its agents. If the contractor makes use of subcontractors who receive access to ZKW information, the contractor must conclude contractual agreements with such subcontractors to ensure that the requirements regulated in this document continue to be complied with in full.

If these TOMs are an attachment to a contract, for instance the contract regulating specific services ("primary contract"), then the following applies: These TOMs, which contain more specialized regulations, always take precedence over any (contradictory) regulations in the primary contract with respect to information security.

The client has the right to review compliance with these information security requirements at any time during normal business hours following prior notification.

Violations of these information security requirements are considered contractual violations.

ZKW works exclusively with contractors who have committed to maintain the confidentiality of ZKW information and trade secrets under a signed non-disclosure agreement. In individual cases, if the provided ZKW information is subject to elevated security requirements, the client will reserve the right - even after the contract has been signed / order awarded - to request that the contractor implement additional measures in order to meet the elevated security requirements.

2. Document Structure and Target Group

The following table outlines the document structure and target audience for each section:

Section	Target audience	Remarks
A, B and C	All contractors	The requirements in this section must be complied with by all contractors.
D	Contractors which • use IT equipment from the client (such as PCs, work stations, laptops) and/or • receive access to the infrastructure (remote / on site) through IT devices belonging to the client or the contractor	The (additional) requirements of section D "only" have to be complied with by the target audiences shown in the left column. For clarification purposes: Sections A, B, and C also apply for these target audiences.

3. Term Definitions

"**Personal data**" is all ZKW information that relates to an identified or identifiable natural person (Art 4 clause 1 GDPR). Personal data must be classified and treated as "confidential" – except for simple names and contact information which are classified as "internal" – or as "strictly confidential," in the case of "special categories of personal data."

"ZKW information" is physical and digital information of the client which is provided by the client and/or created by the contractor on behalf of the client, and which must be protected under information security and data protection requirements in order to ensure its availability, integrity, and confidentiality, including personal data.

A "data protection and information security incident" is an incident or suspected incident which may have a negative effect on the client's IT systems or ZKW information, and which may result in a potential violation or impending violation of data protection and/or information security. This includes violations of information security regulations and applicable data protection laws that relate to ZKW information or the client's IT

systems, presumed vulnerabilities and weak points in IT systems, suspected unauthorized access, change to or loss of confidential or strictly confidential ZKW information of the client.

The "**processing of ZKW information"** includes the collection, processing, transmission, archiving, and saving of ZKW information.

B. REQUIREMENTS TO MAINTAIN INFORMATION SECURITY

Within its scope of responsibility, the contractor must design the internal organization such that it meets requirements for information security and data protection.

The contractor is required to implement and maintain an information security management system in accordance with the requirements of established information security standards (pursuant to ISO 27001/27002, TISAX, BSI).

The contractor must take **state of the art** technical and organizational security measures in order to appropriately ensure the confidentiality, integrity, and availability of ZKW information.

Depending on the type of collaboration, there may be specific requirements for the security measures to be implemented. The type of collaboration – as well as the security measures to be implemented in this respect – may change during the course of the business relationship.

The following is a non-exhaustive list of (minimum) requirements for the contractor's information security management system. The contractor is responsible for defining and implementing necessary additional measures based on the individual risk situation.

C. GENERAL TECHNICAL AND ORGANIZATIONAL MEASURES WHEN PROCESSING ZKW INFORMATION

1. Managing Organizational Assets of the Client

1.1 Confidentiality

ZKW information may only be disclosed to an authorized group of persons for the purpose of carrying out agreed duties, and in compliance with relevant regulations. ZKW information must be protected during the entire life cycle according to its current confidentiality classification. The current and respective confidentiality classification will be declared by the client. **Non-labeled documents / ZKW information must always be classified at least as "confidential."**

The following categories and regulations apply to classifying ZKW information:

Classification	Definition	Designation	Requirements
Public	ZKW information which, if is disclosed to unauthorized persons or improperly transmitted or used, will not influence the achievement of product or project goals because it is already publicly available, and which is therefore not subject to any specific protection requirements. Publicly available personal data	Confidentiality level "public" stated on the first page of a document or in the Legal Notice	ZKW information classified as "public" is not subject to any restrictions, and therefore there are no measures to be observed.
Internal	ZKW information which, if it were disclosed to unauthorized persons or transmitted or used improperly, could have only a small influence on the achievement of product or project goals, and which therefore may be disclosed to an authorized group of individuals. Confidentiality violations may result in minor negative effects, such as minor reputation damage, minor financial impacts.	Confidentiality level "Internal" stated on the first page of a document by the client	In addition to the measures from sections A to D, measures for the "internal" classification indicated in section D must be observed.

	Personal data containing only the business communication data of a natural person (name, phone number, e-mail address)		
Confidential	ZKW information which, were it disclosed or transmitted to unauthorized persons, could endanger the achievement of product or project goals, and which therefore may be disclosed only to a limited group of authorized persons. Confidentiality violations could result in measurable negative effects, such as loss of customers, significant drop in revenue figures, claims for damages. Personal data that goes beyond only business communication data and that is not considered a special category of personal data (such as salary data, banking information, etc.)	Confidentiality level "confidential" indicated on every page of the document in electronic or printed form by the client	In addition to the measures from sections A to D, measures for the "confidential" classification indicated in section D must be observed.
Strictly confidential	ZKW information which, were it transmitted or disclosed to unauthorized persons, could greatly endanger the achievement of corporate objectives. Confidentiality violations will result in very significant impacts on the image or appearance of the company, as well as economic consequences such as significant loss of customers, major drops in revenue figures, very high claims for damages, and exclusion from certain market territories. Special categories of personal data (Art. 9 and 10 GDPR) include: A. data relevant to criminal proceedings B. data indicating racial and ethnic origin, political opinions, religion or worldview, or membership in a trade union, C. genetic data, biometric data which can be used to uniquely identify a natural person, health data or data on a natural person's sex life or sexual orientation.	Confidentiality level "strictly confidential" indicated on every page of the document in electronic or printed form by the client	In addition to the measures from sections A to D, measures for the "strictly confidential" classification indicated in section D must be observed.

1.2 Integrity

ZKW information must always be protected against unauthorized changes. The measures from sections A to D must be observed.

1.3 Availability

The availability of ZKW information must be ensured. The measures from sections A to D must be observed.

2. Management of Data Protection and Information Security Incidents

The contractor must implement measures designed to manage information security incidents (theft, system malfunctions, data loss, etc.).

Technical and organizational measures:

- Establish processes to identify, handle, react to, and prevent / repeat data protection and information security incidents
- Log data protection and information security incidents
- Immediately report information security incidents to the client

  In case of a suspected data protection and information security incident that involves ZKW information and/or the IT systems of the client, a prompt reaction is essential in order to avoid impacts on the client's business processes.

Data protection and information security incidents must be reported promptly to the following office:

ZKW Group GmbH – ZKW Global IT Services & Support Center (GISSC)
E-Mail: gissc@zkw-group.com

3. Deletion of ZKW information after the end of the contract

The contractor is obligated to delete and/or return the ZKW information as defined in the primary contract. If not otherwise defined in the primary contract, ZKW information must be demonstrably and returned deleted promptly after performance of the agreed service, and at the latest by the end of the contractual relationship. Legal requirements (such as statutory retention periods) must be observed.

4. Organizational Control

The contractor must implement measures to ensure that its internal organization meets the special requirements for data protection and information security.

Technical and organizational measures:

- Establish a standard of information security and an information security management system (ISMS)
- Information security guidelines and processes (such as an information security policy, password policy, clean desk and clear screen policy, teleworking policy, etc.).
- Establish an information security risk management process
- Document technical and organizational measures taken
- Evaluate the effectiveness of technical and organizational measures in order to ensure the security of processing
- Review the information security management system via regular audits (annually) to ensure it is appropriate and efficient.
- Define roles and responsibilities related to information security and data protection (appoint a Data Protection Officer / Coordinator and Information Security Officer with the necessary professional expertise)
- Define the distribution of duties between organizational units and employees with respect to data usage
- Establish representative and absence regulations for employees
- Establish a data protection management system (data protection policy, processes for data subject rights, Data Privacy Declarations, index of processing activities, etc.)
- Regularly carry out awareness training programs on information security and data protection for employees (for new hires, and annually thereafter)

5. Order Control

The contractor shall take measures to ensure that ZKW information is processed only in accordance with the client's instructions and conclude relevant regulations with its subcontractors as well.
The contractor must agree on the data protection and information security requirements that apply to him, also with his subcontractors, and verify compliance with them.

Technical and organizational measures:

- Concluded non-disclosure agreements or contracts on the protection of trade secrets with company personnel, third parties and subcontractors that receive access to ZKW information
- Concluded data processing agreements (DPA) with third parties and subcontractors if they process personal data
- The contractor must train or instruct subcontractors on compliance with these information security requirements (annually).
- Content of the contract processing agreements is subject to compliance with the statutory regulations of the EU GDPR.
- Clear contractual designs and versions must be defined.
- A group of individuals to whom orders may be issued has been defined.
- Orders are issued and accepted in only written or electronic form as well.
- The services, competencies, and obligations of the contractor or subcontractor are clearly described in the service descriptions and service level agreements.
- The use of ZKW information must be bound to the availability of valid orders from organizational units and employees entitled to issue orders.
- Data processing agreements must be reviewed regularly in order to validate the data protection and information security requirements.

6. User Control

The contractor shall ensure that all IT systems and applications it uses to process ZKW information cannot be used by unauthorized persons. The

contractor must take measures to prevent data processing systems from being used by unauthorized persons with the help of data processing equipment.

Technical and organizational measures:

- Use of user Ids and passwords
- Regulation on transmitting means of identification (such as hardware tokens for 2 factor authentication)
- Unique assignment of user accounts to users
- No use of group accounts or passwords without additional measures
- Limiting rights of privileged user accounts (administrators) by scope and time
- Separating rights of privileged user accounts (administrators) by activity
- Monitoring the activity of privileged user accounts
- Established password policy that in particular fulfills the following criteria:
    - Generating passwords with appropriate complexity, length (min. 8 characters, lower- and upper-case letters, min. 1 special character and one number)
    - At least 20 characters for service accounts, preventing interactive login
    - Forced password change interval (min. 90 days)
    - Limited incorrect password attempts during login (5 failed attempts)
    - No reuse of the last 10 passwords
    - Changing initial password upon first use (for instance for new user accounts)

7. Data Integrity

The contractor shall take measures to ensure that stored ZKW information cannot be damaged by malfunctions in the IT systems and applications. It must be ensured that any failures or malfunctions can be detected, and that these will not impact the ZKW information to be protected.

Technical and organizational measures:

- Establish a multi-layer security strategy to protect against unauthorized changes
- Establish and document a data backup and restoration concept (create data backups each day)
- Data deliveries must be carried out only using tested and approved input programs.
- If data is changed, integrity tests must be carried out. In case of an error, ZKW information will not be accepted, and the error must be logged.
- Firewalls and anti-malware protection (such as for different systems like firewalls, email, server, clients)
- Detection and alarm in case of security incidents (security monitoring)
- Highly available IT systems (ensuring redundancy) - unless otherwise agreed in written form with the client
- Regular updates to operating systems and installed applications approved by IT
- Regular technical testing (penetration tests)
- Regular reviews of security measures by external auditors

8. Data Input Control

The contractor shall take technical and organizational measures to ensure that a subsequent review can be carried out regarding whether, and by whom, ZKW information was entered into, changed in, or removed from data processing systems.

Technical and organizational measures:

- Logging of all security events (user created, failed login) and data access (such as change/new creation/deletion) and event logs for IT systems and applications
- Logging and archiving in consideration of internal company retention periods
- Restricted access to log data
- Regular review and analysis of log data (min. every 30 days)

9. Data Storage Media Control

The contractor must ensure that data storage media cannot be used by unauthorized persons, that mobile data storage media are encrypted, and that electronic data storage media that are no longer needed are destroyed.

Technical and organizational measures:

- Regulations regarding the protection and handling of data storage media in the contractor's information security regulations
- Proper destruction (data protection garbage bin, shredder)
- Secure storage of data storage media
- Regular employee training and establishment of binding IT usage regulations

Additional measures above the "confidential" classification

- Encryption of mobile data storage media (laptops, USB)
- Controlling and logging the transmission of ZKW information on data storage media
- Secure, repeated overwriting of data storage media (7 cycles)
- Secure, proper disposal in accordance with security level 4 pursuant to ISO 21964

Additional measures above the "strictly confidential" classification

- Secure, proper disposal in accordance with security level 5 pursuant to ISO 21964 (shredder only)

10. Data Deletion and Destruction Control

The contractor shall take technical and organizational measures to ensure that ZKW information is deleted after the end of the retention period, or after it is no longer needed (in particular in compliance with data protection regulations).

Technical and organizational measures:

- Regulations for deleting ZKW information (deletion concept)
- Deletion of ZKW information from IT systems, databases and data backup copies, log information
- Proper disposal (data protection garbage bin, shredder)

Additional measures above the "confidential" classification

- Secure, proper disposal in accordance with security level 4 pursuant to ISO 21964

Additional measures above the "strictly confidential" classification

- Secure, proper disposal in accordance with security level 5 pursuant to ISO 21964 (shredder only)

11. Storage and Retention Control

The contractor shall ensure that only authorized persons have relevant access rights to ZKW information. The contractor shall implement measures to prevent unauthorized access, change, storage, or deletion of saved ZKW information.

Technical and organizational measures:

- Physical access control system (approval of access by a supervisor)
- Authorization and roles concept with access rights based on "need to know" and "least privilege" principles
- Internal control system ("ICS") to ensure the defined procedures (assignment, change, and revocation of rights)
- Ensuring traceability of database activities (tracking)
- Secure authentication with user ID and strong password (see the "User controlling" section)
- Logging data access
- ZKW information must be stored in a non-accessible location

Additional measures above the "confidential" classification

- Encryption of stored ZKW information
- Confidential documents must be stored in locked cabinets and/or rooms which can be opened only by a defined, authorized group of individuals.

Additional measures above the "strictly confidential" classification

- Strictly confidential documents must be stored in locked steel cabinets with anti-burglary protection and/or rooms which can be opened only by a defined, highly restricted, authorized group of individuals.

12. Data Transmission and Transport Control

The contractor shall take measures to prevent ZKW information from being read, copied, changed, or deleted by unauthorized persons during electronic transmission of such information, or during transportation on data storage media. It must be ensured that ZKW information on mobile data storage media (laptops, USB sticks) is always stored encrypted, and is received only by the authorized recipient. It must also be ensured that ZKW information is not deleted, changed, or copied during electronic transmission, and that transmissions are logged.

Technical and organizational measures:

- Secure transportation and shipping of ZKW information, depending on its classification
- Definition of transmission pathways (description of interfaces between systems and the external data connection)
- Connections with subcontractors and other third parties (if connection is permitted in the individual case) with whom ZKW information is exchanged must always be secure (such as VPN)
- Certificate issued by a trusted/recognized certification body
- Use of secure authentication processes (user ID with strong passwords – see the "User controlling" section)
- Firewalls with activated security functions (such as IDS/IPS, web filter)
- Anti-malware protection in the firewall and email systems
- Ensuring secure transport of data storage media (reliable company or personnel)
- There are regulations for handling data storage media in the contractor's information security regulations. For instance, these regulations define that ZKW information must be encrypted on physical data storage media during transportation outside of company premises, if this is reasonable from a technical and economic standpoint.
- Use of locked transportation containers and authorized courier services
- Established processes for secure deletion/destruction of ZKW information, if it is no longer required
- Logging of data transmission

Additional measures above the "confidential" classification

- Encryption during transmission and exchange of ZKW information must be ensured (for instance using VPNS, https, email encryption or encrypted exchange of files using the platform specified by the client, encryption when writing to mobile data storage media, etc.) using state of the art technology.
- Confidential documents and mobile data storage media must be transported in two envelopes and as registered mail, or in locked containers.

Additional measures above the "strictly confidential" classification

- Strictly confidential documents must be transported in two envelopes or in locked containers. Transportation must be carried out personally.
- Transporting strictly confidential information on mobile data storage media is not permitted.

13. Transmission and Duplication Control

The contractor shall implement measures to ensure that ZKW information is copied only under specific requirements and disclosed only to authorized persons.

Technical and organizational measures:

- ZKW information is disclosed only to a restricted group of individuals of the contractor and authorized third parties in the course of their duties, or within their scope of application (on an order-specific basis)
- ZKW information is not subject to any copying restrictions

Additional measures above the "confidential" classification

- ZKW information is disclosed only to a restricted group of individuals at the contractor and authorized third parties in the course of their duties, or within their scope of application (on an order-specific basis)

Additional measures above the "strictly confidential" classification

- ZKW information is disclosed only to a greatly restricted group of individuals of the contractor and authorized third parties in the course of their duties, or within their scope of application (on an order-specific basis), and **only following prior approval from the client.**
- Duplication of ZKW information is permitted **only with the prior approval of the client.**

14. Cloud Control

The contractor shall implement measures to prevent ZKW information from being read, copied, changed, or deleted by unauthorized persons in the cloud.

Technical and organizational measures:

- Encryption of data between each application level and between application interfaces
- Client separation for using cryptographic keys

Additional measures above the "strictly confidential" classification

- Cryptographic keys are managed by the client (generation, change, revocation)

15. Separation Control

The contractor shall implement measures to ensure that ZKW information collected for different purposes is processed separately.

Technical and organizational measures:

- Strict client separation as the highest principle in all technical and organizational considerations, in particular client separation within ZKW information by affected company / legal entity of the client.
- Separation of processing of ZKW information and data storage (logical and/or physical level)
- Separation of productive and testing systems
- Ensure that the test system complies with the same technical and organisational measures as the productive system.
- Execution of tests by the contractor only with anonymised data (no tests with ZKW information by the contractor).

16. Availability Control and Recoverability

The contractor shall implement measures to ensure that ZKW information is protected against accidental loss or destruction. It must be ensured that, in case of a fault (such as: theft, destruction, loss), ZKW information can be restored.

Technical and organizational measures:

- Complete data backup and archiving concept for critical and significant IT systems (daily data backup)
- Data stored on the contractor's servers
- Central storage of ZKW information in systems that are integrated into the regular data backup
- The hardware used by the contractor for IT systems is tested, maintained, and used according to current state of the art technology
- Redundant data storage by operating two computing centers (use of cluster systems for data storage, and use of hard drive mirroring by RAID processes) - unless otherwise agreed in written form with the client
- Redundant / additional computing center in separate fire compartment
- Use of uninterruptible power supply systems (UPS, generators, etc.) and regular maintenance and testing
- Fire protection measures (fire alarm system, extinguishing system, resistance classes for doors, etc.)
- Data backup systems must be stored in separate safety zones and in a separate fire compartment
- Professional use of safety functions (firewalls, IDS/IPS systems, anti-malware protection, SPAM filters, etc.)
- Establishment of business continuity management (BCM) and disaster recovery process (DR) to ensure that emergency plans are available and reviewed on an ongoing basis.
- Regular tests of BCM & DR processes (regular simulation of information security incidents and tests of restoring data and IT systems)

17. Physical Access Control

The contractor shall implement measures to ensure that access to data processing systems used to process or use protected ZKW information is granted only to authorized persons.

Technical and organizational measures:

- Physical access only for authorized internal personnel of the contractor and authorized third parties in the course of their duties or the scope of application (order-specific)
- Defining safety areas / zones
- Securing the outer shell of the building (fences, gates, doorman)

- Controlled reception area in all company buildings
- (Electronic) access control system (such as via a chip card)
- Locked doors and closed windows outside of business hours
- Video surveillance, burglary alarm system and/or security service outside of business hours
- Strict security measures apply to all computing centers, supported as needed by a security service, surveillance cameras, motion sensors and 2-factor authentication, in order to protect systems and equipment belonging to computing centers against unauthorized physical access. Only authorized persons are permitted physical access to data center systems and infrastructure.
- Safety locks with key regulation for highly protected areas (such as HR department offices)
- Visitor management (visitor registration, supervision / chaperon by internal company personnel, wearing visitor ID and/or employee ID)
- Authorization concept for physical access control (authorization matrix) and access right assignment based on a "need to know" principle
- Processes for assigning, changing, and revocation of physical access control
- Logging of physical access
- Documented and regular control of physical access rights

Additional measures above the "confidential" classification

- Physical access only for a restricted group of personnel of the contractor, and authorized third parties in the course of their duties or scope of application (order-specific)
- Buildings, individual areas, and surrounding facilities may be protected by additional measures depending on the security classification

Additional measures above the "strictly confidential" classification

- Physical access only for a greatly restricted group of personnel of the contractor, and authorized third parties in the course of their duties or scope of application (order-specific)
- Buildings, individual areas, and surrounding facilities may be protected by additional measures depending on the security classification

18. Access Control

The contractor shall ensure that use of the IT systems or system components and networks, as well as access to ZKW information in analog and digital form, is permitted only with access authorization. This access authorization is only assigned based on the specific position carried out, and only assigned with approval of the supervisor.

Technical and organizational measures:

- Access only for authorized internal personnel of the contractor and authorized third parties in the course of their duties or the scope of application (order-specific)
- Secure process for user authentication (user ID and password)
- Compliance with the specifications and password policy in the "User controlling" section
- Authorization concept for access control
- Access rights assigned on the "need to know" and "least privilege" principles
- Processes for assigning, changing, and revocation of access rights
- Logging access (such as authorized and unauthorized login)
- Regular review of access rights
- Automatic activation of a screen protector with password protection
- Protection of the company network from the public network (firewall with activated security function)
- Perimeter firewall at external entry points (internet, partner network, etc.)
- Secured network segments and isolation of critical systems (internal network segmenting)
- Terminating external connections in a demilitarized zone (DMZ)
- Activated security services on all firewalls (IDS/IPS, web filter, application controlling, etc.)
- Network access control
- Anti-malware protection on all relevant IT systems (firewall, e-mail gateway, data server, clients, etc.) and regular updates of virus definitions and signature data
- Established patch and vulnerability management (such as regular updates to all IT systems)
- Hardening of IT systems (such as deactivating of services that are no longer required, firewall regulations, etc.)
- Clean desk and clear screen policies, as well as policy for printer access

Additional measures above the "confidential" classification

- Access only for a restricted group of personnel of the contractor, and authorized third parties in the course of their duties or scope of application (order-specific)
- 2-factor authentication at least for remote access and administrator access

Additional measures above the "strictly confidential" classification

- Access only by a greatly restricted group of individuals of the contractor and authorized third parties in the course of their duties, or within their scope of application (on an order-specific basis), and only following prior approval from the client
- Exclusively 2-factor authentication

19. Usage Control

The contractor shall implement measures to ensure that the persons authorized to use a data processing system can only use data that falls within their usage authorization, and measures to ensure that ZKW information cannot be read, copied, changed, or removed without authorization during its processing, use, and after storage.

Technical and organizational measures:

- Usage only for authorized internal personnel of the contractor and authorized third parties in the course of their duties or the scope of application (order-specific)
- Protection against unauthorized usage (password protection)
- Authorization concept for usage control
- Access rights assigned by the "need to know principle" and "least privilege principle" for access rights (such as reading, writing, changing, deleting)
- Processes for assigning, changing, and revocation of access rights
- Logging the assignment, change, and revocation of access rights
- Logging data usage (such as usage, reading, writing, changing, deleting)
- Regular review of access rights

Additional measures above the "confidential" classification

- Use only for a restricted group of personnel of the contractor, and authorized third parties in the course of their duties or scope of application (order-specific)
- Lock for locked cabinets.

Additional measures above the "strictly confidential" classification

- Usage only by a greatly restricted group of individuals of the contractor and authorized third parties in the course of their duties, or within their scope of application (on an order-specific basis), and only following prior approval from the client
- Steel lock for locked cabinets

20. Cryptographic Control

The contractor shall implement measures to ensure that procedures are defined for handling cryptographic keys securely.

Measures above the "confidential" classification

- Process for cryptographic key management
- Generating keys with approved key lengths
- Secure distribution, activation, storage, restoration, exchange and update of cryptographic keys
- Backup and archiving of cryptographic keys, including maintaining cryptographic key history
- Immediate deactivation of cryptographic keys if they are compromised
- Restoration of cryptographic keys in case of compromising, loss, or expiration
- Assignment of a defined date for activating or deactivating cryptographic keys
- Restricted access to cryptographic keys only by authorized personnel

D. ADDITIONAL INFORMATION SECURITY REQUIREMENTS WHEN USING IT DEVICES / ACCESSING THE CLIENT'S INFRASTRUCTURE

This section defines additional provisions that must only be complied with by contractors if the contractor

- uses IT equipment from the client (such as PCs, work stations, laptops) and/or
- receives access to the infrastructure (remote / on site) through IT devices belonging to the client or the contractor at the instruction of ZKW

1. General Requirements and Rules of Conduct

The following requirements must be complied with, in particular, in order to prevent data theft, spying, and cyber security attacks:

- IT equipment belonging to the contractor may only be brought onto the client's company premises in compliance with the instructions of the client's group company personnel.
- Integrating (IT) equipment into the network infrastructure belonging to the client without approval from the client's personnel, is prohibited.
- Using software to process ZKW information that has neither been provided nor approved by the contractor or client is prohibited.
- Written advance approval by the Information Security authority (via ZKW Global IT Services & Support Center (GISSC) of the client is required to process ZKW information on platforms besides those that have been provided by the client, or that are owned by the contractor or its subcontractors. This includes any kind of outsourcing or cloud platform.
- The contractor may only process ZKW information in those IT systems / with those IT services which have been provided by the client or that are operated in the contractor's computing center. Any further processing of ZKW information in IT services that are not operated by the contractor (outsourcing, cloud services) shall require written approval by the Information Security authority (via ZKW Global IT Services & Support Center (GISSC) of the client.
- The contractual agreements apply to the transmission of ZKW information to third parties.
- The client's regulations on the collection, processing, and use of ZKW information must be complied with.
- Employees of the contractor must be obligated by their general management to maintain confidentiality in the sense of the existing non-disclosure agreement between the client and contractor. The client must be entitled to review these agreements at any time. If ZKW information is stored on mobile systems or IT devices, they must be encrypted with state-of-the-art hardware or software.
- Before international travel, country-specific regulations on the use of security technologies (such as encryption) must be observed.
- Documents classified as "confidential" or "strictly confidential" may never be left unsupervised, in order to prevent them from being viewed by unauthorized persons.
- Only secure internet connections may be used, if there is no connection to the client's network.
- "Anonymous surfing" is required to prevent local storage of the websites visited (even if the internet provider still has access to this data)
- Secure HTTPS connections (instead of http) must be used.
- No ZKW information may be published on social media.
- Emails with unusual texts or links must be deleted immediately.
- External data storage media like hard drives and USB sticks must be encrypted.
- IT equipment belonging to the client or on which ZKW information is processed may not be lent to or used by third parties.
- IT equipment must be packaged and sealed during transportation (handed over to customs, etc.) so that any review/manipulation can be tracked.
- Updates must be installed promptly.
- Use caution to prevent anyone from physically monitoring use of IT equipment by "looking over your shoulder." High-quality privacy protectors must be used on laptops.
- A password manager must be used to store passwords securely. Passwords may not be stored in browsers or in plain text files.
- Unnecessary network protocols (like WiFi, Bluetooth or infrared) must be deactivated.
- Since integrated cameras and microphones can be accessed remotely on any IT device, integrated cameras must be covered or sealed off, or stored in protected rooms.
- IT equipment recording functions may be used only with the approval of the client and in compliance with applicable data protection provisions. Secretly recording online and offline meetings (for instance by activating the dictation function on a smartphone) is strictly prohibited.
- No photos / videos may be taken on the company premises of the client, and no photos or videos of ZKW information may be taken without the approval of the client (and in compliance with applicable data protection and secrecy provisions).

2. Use of Passwords

- The requirements of the *"General technical and organizational measures when processing ZKW information"* must be observed when generating and using passwords.
- No use of trivial passwords, or passwords containing a personal reference
- If passwords are to be stored securely, a password manager must be used

- Using the same password for private and professional purposes is not permitted when accessing the client's IT systems / applications
- Using user IDs or accounts belonging to another person is not permitted.
- Passwords or PINs used for user recognition and intended for personal use (called "personal user IDs") must be kept secret and may not be shared.
- If the password or PIN is disclosed to an unauthorized person, or there is a suspicion that this has occurred, immediately change the password and inform the ZKW Global IT Services & Support Center (GISSC).

3. Remote Connections

Remote connections to the client's network infrastructure must be carried out via 2-factor authentication (provided by the client).

The client's following minimum requirements must be upheld for remote connections for which 2-factor authentication is not possible for architecture-related reasons (such as site-to-site VPN):

- Approval of the remote connection by the client
- Strong state of the art encryption
- Access restriction to network segments
- Connection formation initiated by the client

If the connection is no longer required, it must be disconnected.

4. Backups

If the contractor processes ZKW information on IT devices belonging to the client, ZKW information must be stored on the higher-level network drives and not on the local hard drive of the IT device.

The client is not responsible for backing up data that is not stored on central network drives (such as on local hard drives, mobile data storage media) or systems with comparable functions. Backup data and media must be treated in the same manner as productive data.

5. Exchanging ZKW information

- When carrying out meetings (including phone calls, video and web conferences), ensure that unauthorized persons cannot eavesdrop.
- Professional contact data (such as email addresses) must be taken from current directories or requested from the recipient, to prevent incorrect transmission.

6. Using and Returning IT devices belonging to the Client

- Changes to hardware, the system (such as changing a fixed IP address) and security settings (such as browser settings) must always be agreed upon with the client's contact person.
- No data from other customers that do not belong to the client's group may be processed on the provided IT devices.
- The express approval of the client is required for the contractor's employees to use IT equipment belonging to the client.
- The client is entitled to prohibit access or use at any time (for instance in case of abuse).
- The client's IT equipment must be used in such a way that unauthorized persons cannot view or access this data. By way of clarification, please note that this also applies to mobile IT devices belonging to the client.
- The IT devices provided by the client must be handled properly and protected against loss or unauthorized modifications. Devices provided by the client (such as laptops) may only be taken out of the client's company premises with approval. The contractor is responsible for protecting devices against loss or theft.
- Devices (such as laptops) and data storage media provided for use must be returned to the client after the end of the contract, or once they are no longer required. If a user is provided with IT devices or media for the purpose of authentication and these are lost, the user must report the loss promptly to the ZKW Global IT Services & Support Center (GISSC).

7. Revocation of Access Rights

- The contractor must ensure that access accounts and rights are revoked from its employees immediately once they are no longer needed (such as at the end of a project, if the employee leaves their company).
- If a user ID or access right to ZKW information provided to the contractor is no longer required, and/or if access to the client's network or applications is no longer needed before the end of the contractual relationship, this must be reported by the contractor's employee promptly to the contracting office (such as the responsible user administrator of the client, ZKW Global IT Services & Support Center (GISSC), internal contact person for the project).

Contractor:

_____

Name: _____

Date: _____

E. CHANGE REGISTER

Version	Change date	Changes
01	2022-06-07	Initial release
02	2023-09-22	Change of name ZKW Service Desk -> ZKW Global IT Services & Support Center (GISSC) Change chapter 2, contact details ZKW Global IT Services & Support Center (GISSC)