The Cybersecurity Standard for Suppliers is addressed to all persons (f/d/m) with equal appreciation. In order to improve the readability and comprehensibility of this Standard, the masculine form is used for personal designations and personal nouns.

Instruction / Communication				
Activity	**OU**	**Name**	**Date**	**Approval**
Setup	Group Cybersecurity (CHV-C)	Governance & Risk Team Cybersecurity	01.07.2023	by E-Mail
Functional release/ Instruction V1	Group Cybersecurity (CHV-C)	CISO	25.07.2023	by E-Mail
	Procurement (OFP)	Head of Procurement	25.07.2023	by E-Mail
Review/ Revision	Group Cybersecurity (CHV-C)	Governance & Risk Team Cybersecurity	31.10.2025	by E-Mail
Functional release/ Instruction V2	Group Cybersecurity (CHV-C)	CISO	01.12.2025	by E-Mail

Contents

List of tables

1 Modifications

Date	**Modification** (latest 10 modifications)	**Author** (First name, surname, OU)
24.04.2024	Information classification changed to “public”	AB, HS (CHV-CG)
01.12.2025	Major Revision, version 2	AB, HS (CHV-CG)

2 Objective

Cybersecurity aims to protect all tangible and intangible assets as well as employees. Company information - as well as the systems that process this information - represent assets that are particularly worthy of protection at RWE. For this reason, cybersecurity is part of the comprehensive security strategy of RWE and is intended to ensure the confidentiality, integrity, and availability of information and IT and OT systems.

The increasing digitalisation and networking of companies requires the establishment of supply chains and the use of service providers. In addition to many advantages, this also entails certain risks that need to be identified, mitigated as best as possible and tracked within the framework of a holistic risk management.

This Cybersecurity Standard for Suppliers (“Standard”) contains cybersecurity requirements that must be met/fulfilled by all RWE partners and suppliers as well as their subcontractors.

3 Area of application

This Standard applies to all partners and Suppliers of RWE AG and all Group companies (individually and collectively referred to as “RWE”).

It is the responsibility of partners and suppliers, hereinafter referred to only as suppliers, to cascade, and enforce the security requirements of this Standard with all subcontractors.

Different regulations may apply to the Operational Technology (OT) area. The requisitioner will provide RWE's Cybersecurity Standards (s. section 4.8) to the relevant Supplier. The Supplier is responsible to instruct its personnel to adhere to the mentioned documents.

All security measures are carried out on the basis of the applicable laws and current jurisdiction, including co-determination rights, taking into account different responsibilities where applicable.

4 Requirements

In the following the requirements are defined. All requirements are carried out on the basis of common cybersecurity standards like ISO/ IEC 27001 (2022). The requirements differ in “must” and “should” requirements. To the extent permissible by applicable law, “must” Requirements have to be implemented by all RWE suppliers and their subcontractors. “Should” Requirements are recommendations and do not necessarily have to be implemented.

4.1 Information Security Organization, Policies, and Procedures

The supplier must establish clear information security organization, policies and procedures to minimize potential security risks:

- The Supplier must appoint a qualified and experienced Security Manager who holds overall accountability for information security and risk-related matters within the organization. This Security Manager must be granted the authority, resources, and organizational positioning necessary to effectively oversee, coordinate, and monitor all security activities across the organization of the Supplier.
- The Security Manager must maintain awareness of all applicable statutory, regulatory, and contractual obligations, including but not limited to those arising from this Standard, and factor these into the Supplier's organization's security controls and practice.
- The Supplier must ensure that the number, qualifications and competencies of its security personnel are appropriate and commensurate with the nature, scope, and complexity of its operations, and to the risks associated with the services and goods provided to RWE.
- The Supplier must create, maintain and enforce written information security policies approved by management and communicated to personnel, who must understand their obligations for protecting sensitive information and acceptable use of all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE. Reviews and, where necessary, updates of the information security policies must take place at least once a year, to ensure their continued relevance and effectiveness.
- The Supplier must segregate duties and areas of responsibility in the areas of security and IT to reduce the risk of accidental or deliberate system or application misuse.
- The Supplier must establish and maintain processes to select, manage, and monitor subcontractors involved in the service provision. Subcontractors must confirm in writing their ability to meet applicable statutory, regulatory, and contractual obligations, including but not limited to those arising from this Standard. These obligations must be contractually passed down to subcontractors. The Supplier must review subcontractor compliance on a regular basis (at least once per year) and retain the right to audit or assess such compliance.
- The supplier must maintain an accurate, current inventory of all assets and information processing sites used in delivering services to RWE, including the responsible asset owners.

4.2 Personnel/Human Resources (HR) Security

The Supplier must have implemented HR procedures and processes that include all personnel involved in the service provision to RWE to minimize potential security risks.

- The Supplier must have systematic and documented processes in place for vetting all of its personnel (including contractors and temporary personnel) related to the service provision to RWE to check their identity and background. This should encompass the verification of the highest obtained diploma, address of residence in recent years, references of previous employment, checking the validity of identity documents presented and the absence of any (serious) criminal offence. The verification must be carried out in accordance with the applicable law of the respective jurisdiction.
- The Supplier must ensure that, at least once during the pre-employment phase, each individual undergoes a physical, in-person meeting during which their identity is verified through an official government-issued photo identification document (e.g., passport or national ID card). Full remote onboarding without a physical identity check is not permitted.
- In jurisdictions where such HR procedures and processes are restricted by law and regulations, the Supplier must carry out the vetting process to the fullest extent permitted by law and regulations.
- The Supplier must ensure that, before commencing work for RWE, all supplier personnel have completed the information security education and training required for their role, with completion verifiably documented. A comprehensive security awareness program is mandatory for all personnel and must include education, training and updates on security policies, procedures and requirements. Should personnel have access to OT environments, it is essential to ensure that OT specific cybersecurity awareness training is included, with a particular focus on OT-specific safety training. Training must be regularly repeated and reinforced (at least once per year) through appropriate activities and materials. The Supplier must further ensure, that its subcontractors provide equivalent information and training to their personnel and ensure compliance with these requirements.
- The Supplier must ensure its personnel sign non-disclosure or confidentiality agreements prior to being granted access to any information, related assets, or facilities associated with the services provided to RWE. In addition, the Supplier's personnel must provide written agreement to comply with Supplier's security requirements and organizational policies.
- The Supplier must establish and communicate formal disciplinary procedures for addressing violations of the Supplier's security policies and procedures by its personnel. Such actions must be proportionate to the nature and severity of the violation.
- The Supplier must establish processes and procedures for joiner/leaver/movers, e.g., to manage access regarding the chapters 4.6.9 Account Management and 4.6.10 Identity and Access Management.

4.3 Security Incident Management and Reporting

The Supplier must have implemented documented procedures for managing security incidents, enabling effective and orderly handling of all incidents. These procedures must include:

- Monitoring, detecting, classifying, analysing, reporting, response and resolution of events, with clear roles, responsibilities and post-incident reviews (including root cause analysis and lessons learned).
- Suspected security incidents must be verified and analysed to determine their impact.
- Confirmed security incidents must be classified, prioritized and documented.
- Only trained personnel (e.g. a dedicated Security Incident Response Team) may handle and assess incidents
- All incident management activities must be logged, and logs protected against tampering.
- The Supplier must use an appropriate tool or application to manage security incidents. The solution must support tracking of tasks and activities, assignment of roles and responsibilities, status monitoring, and provide audit trails for accountability, traceability, and effective coordination throughout the incident lifecycle.
- The Supplier must report any security incidents, events, and/or weaknesses of which they become aware involving or impacting RWE without undue delay (but at the latest within 24 hours) to RWE via email (csirt@rwe.com). This reporting obligation applies to the signatory legal entity and all subsidiaries, affiliates, or other associated legal entities, including but not limited to those sharing IT infrastructure with the supplier. This includes but is not limited to:
    - **Lost or stolen equipment of RWE** including laptops, smartphones, external drives, or other mobile storage devices containing or accessing RWE data.
    - **Use of unapproved or insecure software or hardware**, especially shadow IT components that bypass standard controls.
    - **Unauthorized access attempts or access violations**, including privilege misuse and use of shared credentials.
    - **Malware infections**, including viruses, worms, ransomware, spyware, or trojans.
    - **Hacking attempts**, including successful or attempted intrusions into systems, networks, or applications.
    - **Physical security breaches**, such as unauthorized access to secure areas, tampering with hardware, or theft of physical documents.

4.4 Information Classification

4.4.1 Classification and Labelling

The Supplier must establish and maintain an appropriate, comprehensive, and organization-wide Information Classification scheme, supported by a documented policy and operational processes. All information received from RWE must, by default, be treated confidential and classified with the appropriate information classification category/level within the Supplier's scheme, clearly labelled in accordance with the Supplier's classification and labelling requirements, and handled in line with the protection measures applicable to the corresponding classification category. The Supplier's classification scheme shall align with applicable legal, regulatory, and contractual obligations, and ensure that classification requirements are consistently applied throughout the information lifecycle, including creation, storage, processing, transmission, and disposal.

Sensitive information of RWE represent a special case, which are referred to as "RWE sensitive information" in this context and for which special protective measures must be taken. Examples of "RWE sensitive information" include, but are not limited to:

- Technical documentation (e.g. network plan, construction plans etc.)
- Operational plans
- Security concept (e.g., for the annual general meeting)
- Information on compliance violations
- Information / Cybersecurity related information
- Personal information about the employment relationship (e.g. salary data)
- Bank details of company & employees
- M&A Projects
- Business development projects
- Business secrets (e.g. patents/inventions, business reports before publication etc.)
- Medical data
- Biometric data for unique identification of a natural person
- Criminal convictions and offences

4.4.2 Handling information

Information is a critical asset for RWE and must be safeguarded throughout its entire lifecycle from creation, recording, storage and deletion, to disposal. Therefore, the following measures are also to be implemented by all Suppliers in order to achieve holistic protection of RWE´s information:

- The Supplier should maintain an inventory of RWE´s information and other associated assets, including but not limited to OT Operational Data (e.g., process set-points, alarm logs, SCADA data). It is imperative that each asset is assigned a designated owner.
- Clear screen and clean desk regulations to avoid unauthorised access to information in the workplace.
- Regulations and associated measures for secure communication (use of E-mail and messenger).
- Definition and formal approval of communication tools for business communication.
- Regulations for destruction/disposal of information at the end of its lifecycle.
- E-mails with RWE sensitive information should be encrypted wherever feasible (see chapter 4.6.7 Cryptography).
- Media with RWE sensitive information must be kept under lock and key.
- For the permanent storage of media containing RWE sensitive information, a suitable storage facility (e.g., safe or steel cabinet) must be used. In the course of daily use, media containing RWE sensitive information must be kept under lock and key as far as possible using the available technical possibilities.
- Use of any kind of RWE data / information for the training, fine-tuning, or improvement of any Artificial Intelligence (AI) systems or models is strictly prohibited. This includes, but is not limited to, generative AI, machine learning, and large language models. Exceptions are only permissible where explicitly and unambiguously defined and regulated within the contractual agreement between RWE and the Supplier.

4.5 Physical and Environmental Security

The premises/facilities relevant for the service provision to RWE must be adequately protected to prevent unauthorized physical access. Therefore, the Supplier shall implement the following measures.

- Physical protection measures (fences, physical barriers, use of locked doors, security guards, intruder alarm systems, video monitoring systems etc.) must be evaluated and selected for implementation in accordance with the requirements related to the assets within the premises/facilities. The level of the applied measures must always be proportional to the criticality of equipment and systems stored in the facilities and risk to the business operations arising from their compromise or destruction.
- Physical access must be limited to those individuals with a business need and must be documented accordingly and be protected by appropriate measures. Authentication mechanisms like access cards must be in place.

- A documented access management process is required and must include the request for access rights, a periodical review and the revocation of authorizations.
- Any external third-party access to the information processing facilities in question must be rigorously controlled, documented and kept at a minimum.

If "RWE sensitive information" is processed by the Supplier, the following additional measures must be implemented:

- Physical access to premises/facilities where sensitive RWE information is processed must be protected by appropriate physical access measures (e.g., turnstiles or mantraps) in order to prevent tailgating. Physical access must be implemented so only one person at a time can access the restricted areas.
- If the Supplier's personnel work on other engagements/contracts (i.e., other companies besides RWE) on the same floor within a building/facility, dedicated workspaces/areas should be established for the services provided to RWE. These spaces/areas should (at a minimum) be protected by organizational controls such as special signs and employee awareness campaigns to ensure information protection and reduce the risk of unauthorized access to the specific area where RWE sensitive data is processed.

The premises/facilities relevant for the service provision to RWE must be adequately protected to prevent damage caused by physical and environmental threats. Therefore, the Supplier shall implement the following measures:

- Adequate measures to protect against physical and environmental threats (for example: fire, flooding, electrical surges) must be commensurate with the importance of the buildings and the criticality of the operations or IT systems located in these buildings with regards to the service provision to RWE. Facilities need to have appropriate protections in place for early detection of smoke, fire, humidity and water in the facility.

4.6 Operations Security

4.6.1 Technical Vulnerability and Patch Management

The Supplier must implement a comprehensive and documented vulnerability and patch management process for all systems, applications, network-, infrastructure- and endpoint-devices in order to reduce attack service and to minimize potential security risks. Attackers are always identifying new attack methods or identifying vulnerabilities in existing services. It is therefore important that software and hardware are regularly checked for vulnerabilities and that existing updates and patches are applied.

Discovery of vulnerabilities:

- Supplier should track information from software and hardware vendors and other relevant sources relating to technical vulnerabilities. In addition, the Supplier must carry out vulnerability scans on a regular basis and must promptly evaluate exposure to discovered vulnerabilities in order to ensure that appropriate measures are taken to address potential risks.
- Vulnerabilities must be assigned a severity score using a recognized industry standard, e.g. the Common Vulnerability Scoring System (CVSS Scoring). Furthermore, vulnerabilities must be addressed in a timely fashion, according to the assigned level of criticality.

Treatment of identified vulnerabilities:

- The Supplier must ensure that discovered vulnerabilities are addressed either with a corresponding software patch to remediate the vulnerability OR with a formalized and documented risk treatment plan approved by the accountable management to reduce the risk of the vulnerability to an acceptable level. This must be carried out in a timely fashion, according to the assigned level of criticality.
- Relevant systems, applications, network-, infrastructure- and endpoint-devices must be configured to receive software patches and other relevant updates automatically from a centralized management and distribution service where technically feasible.

4.6.2 Change Management

Effective change management is essential to maintain the confidentiality, integrity, and availability of systems and services. Uncontrolled or undocumented changes can introduce vulnerabilities, disrupt service delivery, or compromise compliance obligations.

- The Supplier must ensure that formal change control procedures are established within the Supplier to ensure all changes performed on IT / OT systems and infrastructure (e.g. configurations, upgrades, new applications/components, etc.) are duly documented, tested and approved by the accountable management of the supplier.
- Changes that may negatively affect the contractually agreed services must be notified to RWE by the supplier within a reasonable period of time in advance (by mail to cybersecurity@rwe.com). This includes but is not limited to:
    - extensive changes to Supplier's technical infrastructure (e.g., major upgrades to operating systems or application software or significant reconfiguration of systems)
    - extensive reconfiguration of Supplier's services and/or security measures
    - relocation of the contractor's technical infrastructure to another geographic region or jurisdiction

- processing of information in a new geographic region or jurisdiction.

4.6.3 Endpoint / Device Security

All Supplier resources relevant for the services provision to RWE must be subject to endpoint protection, malware controls and end-user software installation controls in order to reduce attack surface and to minimize potential security risks.

- All endpoints should be centrally managed and must have updated and properly configured endpoint protection software (including regular scans and definition updates) in order to prevent the spread of malware. In addition, endpoints must be kept up to date with the latest security patches and software updates.
- Access to RWE systems (e.g. via Virtual Desktop Infrastructure (VDI) or Azure Virtual Desktop (AVD)), portals (e.g. via Microsoft Online (MSOL) or M365 via office.com or microsoft365.com), or any service provision activities must not be performed from non-managed or unauthorized devices. Only devices that are fully managed and compliant with the Supplier's security policies may be used.
- End-user software installation refers to the process of allowing or denying personnel from installing software on their workstations. Unauthorized software installations can introduce vulnerabilities and malware to the organization's network.
    - Software installation on supplier-owned devices should be managed (e.g., by whitelist or blacklist approach).
    - All software installed on supplier-owned devices must be licensed and properly maintained to ensure security and compliance. This includes keeping track of all software versions and applying necessary updates and patches.

4.6.4 Hardening

The Supplier must harden all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE in order to reduce attack service and to minimize potential security risks.

- Hardening must be done before deployment in production, including patching known vulnerabilities and implementing a secure baseline or using secure baseline builds.
- All generic, guest, maintenance and default accounts should be disabled.
- All laptops and mobile devices must be protected by Secure Boot with PIN and full disk encryption (e.g., BitLocker). Controls must be configured to prevent unauthorized access and tampering with devices or data.

- USB ports should be disabled wherever feasible.
- Configuration areas (e.g., BIOS, UEFI, Windows Control Panel) must not be accessible/modifiable by regular users.
- All default passwords must be changeable and changed to an individual, non-standard value (see 4.6.11 Password Management).
- The use of legacy or insecure protocols, such as SMBv1, that no longer meet current security standards should be avoided. Where such protocols cannot be fully eliminated, their use must be justified, risk-assessed, and appropriately mitigated.
- The use of local administrator accounts must be limited to the minimum necessary. These accounts must be strictly controlled, monitored, and used only where technically required and must be promptly deactivated and decommissioned once no longer required for operational purposes. Local administrator accounts must be separated from regular user accounts to reduce the risk of privilege misuse.

4.6.5 Secure Development

The following section exclusively concerns Suppliers, which are involved in the context of software development for RWE.

- The development of software must meet state of the art security requirements and follow a common security framework respectively a common secure software development lifecycle (S-SDLC), e.g., OWASP and/or a common secure product development lifecycle (SPDL), e.g. IEC 62443-4-1 and IEC 62443-4-2. Appropriate additional measures and requirements should be developed and met for the project being developed according to criticality and intended purpose.
- Supplier must follow and adhere to the requirements outlined in the “Secure Software Development Lifecycle (SSDLC) Standard”.
- A development pipeline or staging process should be set up to ensure that only tested and approved changes are implemented in productive systems. This includes functionality as well as security aspects and should include quality checks like software code scanners and peer review.
- Supplier must resolve all security issues that are identified before delivery. Security issues discovered or reasonably suspected after delivery should be handled in assisting RWE in performing an investigation to determine the nature of the issue and in fixing in a reasonable time frame related to the connected risk.
- Comprehensible documentation should be prepared in accordance with the requirements and specifications.

4.6.6 Network and Architecture Security

The Supplier must protect all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE in order to reduce attack surface and to minimize potential security risks. Protecting the network and clients from unauthorized access, misuse, or theft is essential to contain the impact of attacks and prevent them from spreading. Network security combines multiple layers of defense at the perimeter and in the network.

- The Supplier should implement an appropriate network architecture and encompassing/incorporating different segments, with each segment serving a specific purpose and containing only the necessary systems and data. This helps to limit the scope of a potential security breach and makes it easier to identify and contain any issues.
- Operational Technology (OT) and Industrial Control System (ICS) networks shall be logically separated from corporate IT networks and operated on physically distinct network devices wherever feasible. Segregation should be enforced using appropriate security controls, such as stateful firewalls, unidirectional gateways (data diodes), and demilitarised zones (DMZ). The implementation of a zone-and-conduit segmentation model should be consistent with IEC 62443, ensuring that OT/ICS environments are divided into security zones based on process criticality. Communication between zones shall be restricted to controlled conduits and DMZs, with only the minimum required traffic permitted, thereby reducing attack surfaces and ensuring resilience of critical operations.
- The Supplier must implement appropriate network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and comparable security controls. These components and must be maintained regularly. The firewall (if technically feasible) must be configured to address all known security issues.
- The Supplier must approve and restrict the remote access into the supplier's network to authorized personnel only. If remote access to the Supplier's networks and clients is necessary, secure and encrypted methods must be used, such as virtual private networks (VPNs) and MFA.
- The Supplier must implement measures to secure the Supplier 's email systems. This can include the use of spam filters, email encryption, and the implementation of email policies to prevent the sharing of sensitive information.

4.6.7 Cryptography

The Supplier must ensure the implementation of cryptographic mechanisms to prevent unauthorized disclosure and modification of information which are relevant for the service provision to RWE.

- The use of cryptography solutions must be considered in regard to regulatory requirements.
- Cryptographic solutions should take into account best practices regarding secure versions and configurations that are available within global information security standards (e.g., ENISA, FIPS, BSI, etc.).
- A cryptographic key management system should be in place with procedures to cover the entire key lifecycle (from generation to revocation/destruction) and with measures to ensure their protection.

If RWE sensitive information is processed by the supplier, the following additional measures must be applied:

- RWE sensitive information must be encrypted in transit and at rest using approved encryption algorithms with adequate key length and cryptographic strength.

4.6.8 Logging and Monitoring

The Supplier must monitor and create event logs for all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE. In addition, the physical access measures (e.g., doors, turnstiles or mantraps) of premises/facilities where RWE sensitive information is processed must also be monitored and logged to track physical access at any time.

- Event logs must provide enough detail to assist in identifying the root cause of an issue and allow reconstruction of the sequence of events. This includes but is not limited to recording the date, time, and source location (IP address/hostname) for all access attempts, as well as capturing system and network security event information, alerts, failures, events, and errors.
- Event logs must be continuously monitored and periodically reviewed to analyse and identify anomalous, suspicious, and/or unauthorized activity.
- Event logs should be stored and consolidated on a centralized system (e.g., centralized log server) to ensure the integrity of the log files and protect them from tampering.
- Access to the centralized systems that store the log files must be restricted. Users, including those with privileged access rights, should not be granted permission to delete or deactivate logs of their own activities, in order to maintain an accurate and unaltered record of events.
- Supplier should integrate their logging and monitoring systems with a Security Information and Event Management (SIEM) platform, ensuring real-time analysis.

4.6.9 Account Management

The Supplier must have an account management in place to protect information through controlled use of user accounts which are relevant for the service provision to RWE to minimize potential security risks.

- The Supplier must establish and maintain an up-to-date inventory of all accounts which are relevant for the service provision to RWE.
- The Supplier must establish and maintain an up-to-date list of all individuals who are involved in the provision of services and goods to RWE, including those employed by subcontractors. This list must include separate columns for first name, last name, email address, service location and role and must be made available to the RWE upon request.
- The Supplier must perform rigid account management on the systems provided to RWE and the principle of least privileges must be applied.

4.6.10 Identity and Access Management

The Supplier must implement the following requirements to ensure that only authorized users get access to information which are relevant for the service provision to RWE.

Identification

- **User registration and de-registration**: The Supplier must have appropriate user account creation and deletion procedures. This includes appropriate approvals by RWE if new user accounts, relevant for the service provision to RWE, are to be onboarded. The de-registration process must be regularly reviewed by the supplier and a current status of the Suppliers used access accounts, relevant for the service provision to RWE, can be produced at RWEs request.
- **Unique Use of User IDs**: User IDs are assigned in a one-to-one relation; each individual receives a personalised user account and is restricted to this account.
- **User Access Reviews:** All granted access rights are reviewed by the Supplier on a regular base.

Authentication

- To access resources every individual must be authenticated to confirm the individual's identity and accountability for the actions taken within the systems.
- Considering that passwords are used as primary authentication mechanism when accessing RWE IT resources, requirements defined in the chapter 4.6.11 Password Management must be followed.

- User authentication must be managed whenever supported by the system, so that user credentials are provided only once and passwords and or PINs are non-guessable. Users must be required to change them after the first use.
- Additional authentication factors (Multi Factor Authentication - MFA) must also be introduced to further secure access to systems (e.g., tokens, smart cards, biometric traits) depending on the nature and sensitivity of the information/system.
    - External, i.e. public/internet facing Services/Systems/Portals must enforce MFA.

Authorization

- The Supplier acknowledges, that RWE may be providing access to sensible information and complies with the fact, that granted access is used solely for the purpose of the contractual agreement. The Supplier will not use granted access rights to gain access to information that has not been explicitly approved by RWE and thus is needed to perform the contractual agreement.
- The Supplier must protect the access to the information according to the confidentiality level. Please also refer to the Chapter "Classification of the need for protection of information" within this document.

4.6.11 Password Management

The Supplier must enforce strong password requirements for all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE to protect sensitive information and prevent unauthorized access to systems and data. Strong passwords are a crucial defence against cyber threats such as hacking, phishing and malware attacks.

- All accounts must be protected with (changeable) strong passwords. A password policy should be enforced as a minimum to meet the following requirements:
    - minimum password length (e.g., 12 character)
    - complexity requirements (e.g., no dictionary words, use a mix of alpha numeric characters, require special characters, etc.)
    - No reuse of passwords (e.g., password history)
    - Encryption of passwords when transmitted or stored
    - Distribution of passwords separately from account information to ensure confidentiality of information
- MFA must be implemented depending on the nature and criticality of the service and the security/protection requirement.

- External, i.e. public/internet facing Services/Systems/Portals must enforce MFA.

4.6.12 Back-up and Recovery

To prevent the loss of data the supplier must ensure that backup processes (appropriate to the protection requirements) are implemented for all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE.

- The Supplier must ensure that the requirements in terms of backup storage, the frequency of execution and protection against unauthorized access are met in relation to the protection requirement of the services provided for RWE.
- The implemented processes for backup and recovery must be tested regularly, i.e. regularly testing backup media to ensure that they can be relied on for emergency use when necessary.

4.6.13 Business Continuity and Disaster Recovery

To minimize the impact of process interruptions in the context of service provision to RWE, the Supplier must have a Disaster Recovery (DR) program or a Business Continuity Management (BCM) in place.

- These must be designed to prevent the loss of data and to ensure the Supplier can continue to function through operational interruption and continue to provide services as specified in its agreement with RWE.
- The services provided to RWE must be covered by a Business Continuity Plan (BCP). Associated assets need to be subject to a corresponding Disaster Recovery Plan (DR Plan). The Supplier must ensure the scope of the BCP and DRP encompasses all locations, staff involved and information systems used to perform or provide services to RWE.
- The BCP and DRP must be maintained and tested on a regular basis (at least once per year).
- The documentation about the testing scope and outcome must be provided to RWE on request.

4.6.14 Cloud Security

The following section exclusively concerns suppliers' providing / using cloud environments, which are relevant for the service provision to RWE.

Cloud environments and tenants provisioned and managed by the Client (e.g., RWE's Microsoft Azure or AWS tenant) shall be the preferred and primary option for service provision. The use of any other cloud environments by the Supplier is only permitted where explicitly defined and contractually agreed as part of the service provision.

Where those kind of cloud environments (including those hosted by hyperscalers such as AWS, Azure, or Google Cloud) are used in connection with the provision of services to RWE, the following conditions apply:

- Only cloud tenants and environments that are provisioned, administered, and managed by the Supplier (i.e., under the Supplier's administrative control) shall be used.
- The Supplier must not use personal, consumer, or otherwise unmanaged cloud accounts or services for service provision (e.g. filesharing via private Dropbox-account from an external employee).
- Cloud services must be configured in accordance with recognized security standards and must include:
    - Role-based access control (RBAC) and MFA
    - Logging and monitoring of security-relevant events
    - Data protection measures including encryption in transit and at rest
    - Segregation of client environments to prevent cross-client access
    - Hosting in data centres and regions compliant with applicable legal, regulatory, and contractual requirements (e.g., data protection laws, export controls)
- Use of any cloud service must be pre-approved by the Supplier's security governance and compliant with contractual, legal, and regulatory requirements applicable to RWE.

Use of unmanaged or unapproved cloud services ("shadow IT") is strictly prohibited.

4.7 Compliance and Assessments

Maintaining transparency and verifiable adherence to security requirements is essential to ensure trust and accountability in the supply relationship. Regular assessments and compliance reviews provide assurance that appropriate controls are in place, effectively implemented, and continuously improved. To this end:

- Upon request, the Supplier shall answer a security questionnaire issued by RWE (or a third party commissioned by RWE who is not a direct competitor of the Supplier) and submit a written response (including corresponding evidence) so that RWE can assess compliance with the requirements of this Standard.
- After reasonable advance notice, RWE (or a third party commissioned by RWE who is not a direct competitor of the Supplier) shall be entitled to verify compliance with the requirements of this Standard by means of an on-site assessment at all relevant branches and/or premises of the Supplier. The specific scope, duration and setup of the on-site assessment shall be agreed and coordinated with the Supplier.

- The Supplier shall provide qualified employees to support RWE during the on-site assessment. This support shall include, in particular, access to all relevant physical premises, systems and employees as well as the provision of relevant documents, which shall include, among others, process documentation, (security) policies and guidelines as well as security-related performance monitoring reports of the Supplier. All requested documents, whether in digital or physical form, shall be made available to RWE, including those initially classified as internal by the Supplier. In such cases, the classification shall be adjusted accordingly (e.g. to “Client Confidential”) to reflect the information sharing with RWE.
- Should weaknesses, deviations and/or non-conformities with the requirements of this Standard be identified during the self-disclosure or on-site assessment, the Supplier must promptly submit suitable risk mitigation plans and corrective measures to the Principal and implement them. The implementation must be communicated to RWE without delay.

The Supplier must impose the same obligation on its Contractors and Subcontractors.

4.8 Subcontractors

If the Supplier engages subcontractors, the Supplier is obliged to establish and maintain a comprehensive third-party risk management and supplier security program, incorporating clear requirements and controls for overseeing and managing its subcontractors in alignment with both RWE’s "Cybersecurity Standard for Suppliers" and the “Cybersecurity Standard for External Employees”, hereinafter referred to as the “RWE's Cybersecurity Standards”.

The Supplier must treat and manage all subcontractors involved in the provision of services and goods to RWE as critical suppliers. This includes, but is not limited to, the rigorous application of third party cyber risk management procedures including due diligence, regular quality assurance and risk assessments, as well as continuous monitoring. On request, the supplier must provide RWE with all risk acceptances related to these subcontractors.

The Supplier must have binding agreements in place with all subcontractors that require them to meet RWE’s Cybersecurity Standards. On request, the Supplier must confirm in writing to RWE that such agreements have been concluded. The Supplier is responsible for ensuring subcontractor compliance by conducting regular assessments, at least once per year, to identify and address any potential gaps as part of a continuous improvement process.

5 Group regulations out of force

IT Security Policy for RWE Group (V: 2.2, valid from 20.06.2008 including Annex 1: Minimum Standard of IT security for IT User as well as Annex 2: Minimum Standard of IT security for the IT Service Provider).

6 Annexes

6.1 Annex 1: Definition of Terms

Terms	Explanation
Agreement	All applicable arrangements between RWE and supplier including Vendor Services Agreement, Master Service Agreement, Professional Services Subcontract Agreement, supplier Base Agreement and applicable licensing and other agreements under which the supplier Performs.
Asset	Any tangible or intangible item owned by RWE for which a supplier is responsible.
Authentication	The act of verifying identity i.e. user, system.
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, the German upper-level federal agency in charge of managing computer and communication security for the German government)
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
Cryptographic key	A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext.
CVSS	Refers to Common Vulnerability Scoring System.
ENISA	European Union Agency for Cybersecurity
Facilities	Buildings, pieces of equipment or services that are provided for a particular purpose.
FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission

Integrity	The guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Partners	Any organization associated to RWE that participates in a common activity or pools it resources to achieve a common goal.
Personal information	Any data relating to an identified or identifiable living individual; an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.
Risk Assessment	A process used to identify and evaluate risk and potential effects. Risk assessment includes assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
Role-based access	Assign users to job functions or titles. Each job function or title defines a specific authorization level.
Security incident	Defined as a violation or imminent threat of violation of security policies, acceptable use policies or standard security practices.
Security Manager	Refers to a professional who oversees and implements security measures to protect an organization's employees, assets, and operations from threats. This involves developing and enforcing security policies, conducting risk assessments, managing security personnel, and responding to security incidents. Their primary role is to safeguard the company by mitigating risks and ensuring a safe environment.
Sensitive information	Refers to data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. “RWE sensitive information” refers to a special kind of information for which special protective measures must be taken (cf. chapter "Information Classification and Labelling).
Services	Work to be performed by supplier for RWE as specified in an Agreement, contract, or statement of work.

Supplier	Refers to the person or legal entity, regardless of the form of organization that provides a product or service to RWE within a contractual agreement.
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Table 1: Definition of Terms