The Standard 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 Cyber Security (CHV-C)	Governance & Risk Team Cyber Security	01.07.2023	by E-Mail
Functional release/ Instruction	Group Cyber Security (CHV-C)	CISO	25.07.2023	by E-Mail
	Procurement (OFP)	Head of Procurement	25.07.2023	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)

2 Objective

Cybersecurity aims to protect all tangible and intangible assets as well as employees. Company information - as well as the systems that process these information - represent assets that are particularly worthy of protection at RWE. For this reason, cyber security is part of the comprehensive security strategy of RWE and is intended to ensure the confidentiality, integrity, and availability of information and IT 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 Standard contains cyber security requirements that must be met/fulfilled by all RWE partners and suppliers and their subcontractors.

3 Area of application

This Standard applies to all partners and suppliers of RWE AG and of 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 the security requirements of this Standard towards any of their subcontractors.

An exception to this Standard exists for suppliers who exclusively work on RWE's devices. These suppliers do not have to implement the following requirements but they must align with the Group Business Rule ´GBR 002 Cyber Security- Minimum Standards for Employees`. Furthermore, different regulations may apply to the Operational Technology (OT) area. The requisitioner will provide this Standard to the concerned suppliers. The supplier is responsible to instruct its personnel to adhere to the mentioned document.

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 cyber security standards like ISO/ IEC 27001 (2022). The requirements differ in "must" and "should" requirements. "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 establish clear information security roles, responsibilities and accountability for effective security management. Depending on the size and scope of responsibilities, the supplier must appoint at least one security officer(s) with the necessary knowledge, experience, and authority to oversee information security in the organization and ensure that security rules and procedures are coordinated and monitored.
- 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 confidential information and acceptable use of all systems, applications, network-, infrastructure- and endpoint-devices, which are relevant for the service provision to RWE. Reviews and, if necessary, updates of the information security policies should take place at least once a year, in order to ensure their relevance and effectiveness.
- The supplier must have processes in place to manage their sub-contractors involved in delivering services, which must confirm their ability to meet security control standards in writing.
- The supplier should 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 persons involved in the service provision to RWE to minimize potential security risks.

- The supplier must perform background checks or pre-employment screenings on all personnel (including contractors and temporary personnel) involved in providing services to RWE. The checks or screenings should encompass the criminal and employment background of the personnel. The level of verification must be proportionate to the criticality and risk associated with the role or task within the organization and in compliance with applicable law.
- The supplier should ensure, that before the supplier's personnel start working for RWE, the information security related education and trainings required for their role has been (verifiably) completed. A comprehensive security awareness program for all personnel that encompasses

education, training and updates for security policies, procedures and requirements is mandatory. Appropriate training should be regularly repeated and reinforced through adequate activities and materials.

- The supplier's personnel should sign non-disclosure or confidentiality agreements before being given access to information and other associated assets as well as facilities related to the services provided to RWE. In addition, supplier's personnel must agree in writing to comply with supplier's security requirements and organizational policies.
- The supplier should have formalized and communicated disciplinary procedures to take actions against personnel who violate supplier's security policies and procedures, depending on 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 procedures for security incidents, enabling effective and orderly management of security incidents for processes, which are relevant for the service provision to RWE.

- These procedures must be documented and should cover the monitoring, detecting, classifying, analysing and reporting as well as the response and resolution of security incidents and define associated roles and responsibilities. In addition, root cause analysis as well as lessons learned procedures must be conducted for each security incident with impact on RWE assets.
- Reported security incidents must be verified and then analysed to determine their impact.
- All confirmed security incidents must be classified, prioritized and documented.
- Security incidents must be handled by personnel who are trained in handling and assessing security incidents (e.g., a dedicated Security Incident Response Team).
- All incident management activities must be logged, and logs must be tampered proof.
- 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).

4.4 Handling information

Information is an important asset for RWE and must be adequately protected at all times of its existence (information life cycle). This applies from information creation, to recording and deletion,

right through 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 owners.

The supplier must have implemented regulations for working with information:

- The supplier must have clear screen and clean desk regulations in place to ensure that unauthorised persons cannot access information at the workplaces.
- Regulations for secure communication (use of E-mails and messengers) should be in place.
- The supplier should define and approve communication tools for the communication of business information.

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

- Regulations for destruction/disposal of information at the end of its lifecycle should be defined. For the destruction of “Confidential” and "Strictly confidential" RWE information, a shredder/file shredder must be used.
- E-mails with RWE sensitive information should be encrypted in any case (see chapter 4.6.7 Cryptography).
- Media with RWE confidential information must be kept under lock and key.
- For the permanent storage of media containing strictly confidential RWE information, a suitable storage facility (e.g., safe or steel cabinet) must be used. In the course of daily use, media containing strictly confidential RWE information must be kept under lock and key as far as possible using the available technical possibilities.

4.4.1 Classification and labelling

The specifications of Information classification and labelling are based on RWE´s internal regulations. The requirements are also to be implemented by the supplier to achieve holistic protection of RWE´s information by ensuring a consistent approach. All information (belonging to RWE and its customers) must be protected by RWE suppliers and their subcontractors in accordance with the given requirements and, if necessary, with in addition to the contract attached regulations for handling information.

- Any information related to the service provision to RWE must be classified and must be labeled according to the given requirements (see Annex 1: Information classification and labelling).

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, 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 should always be proportional to 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 should be documented accordingly and be protected by appropriate measures. Authentication mechanisms like access cards should 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 sensitive RWE 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 piggybacking. In any case, physical access must be implemented in a way, that 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 must be established for the services provided to RWE. These spaces/areas must (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) should 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 Security Requirements for IT Operations

4.6.1 Technical Vulnerability and Patch Management

The supplier should implement a comprehensive and documented vulnerability- and patch management process for 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. 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 (relevant for the service provision to RWE) 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 should be addressed in a timely fashion, according to the assigned level of criticality.

Treatment of identified vulnerabilities:

- The supplier must ensure that discovered vulnerabilities (relevant for the service provision to RWE) 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 should be carried out in a timely fashion, according to the assigned level of criticality.
- Relevant systems, applications, network-, infrastructure- and endpoint-devices should 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

- Changes to information processing facilities, information systems, applications, platforms, infrastructure and/or underlying physical and technical premises relevant for the service provision to RWE must be subject to formal change management procedures, which should be documented and approved by the accountable management of the supplier. The supplier should maintain records of all relevant changes, including information on date, time and authorization of the changes.
- Changes that may affect the contractually agreed services must be notified to RWE by the supplier within a reasonable period of time in advance (by mail to informationsecurity@rwe.com). This includes but is not limited to:
    - changes to the physical infrastructure (e.g., moving to a different facility or building/floor) as well as the technical infrastructure (e.g., major upgrades of operating systems and/or applications, or significant reconfiguration of systems and/or services)
    - relocation of the physical and/or technical infrastructure to a different geographical region or legal jurisdiction
    - processing information in a new geographical or legal jurisdiction

4.6.3 Endpoint / Device Security

All supplier resources relevant for the services provision to RWE should 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 should 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.
- 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 should 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.
- Hard-disk encryption should be enabled.
- USB ports should be disabled wherever feasible.
- Configuration areas (e.g., BIOS, EFO, Windows Control Panel) should 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).

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. Appropriate additional measures and requirements should be developed and met for the project being developed according to criticality and intended purpose.
- 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.
- The vendor 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.
- Especially Operational Technology (OT) networks and Industrial Control System (ICS) network should be logically separated from the corporate network on physically separate network devices.
- The supplier should implement appropriate network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and comparable security controls. These components and should 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 preferred way for suppliers to access RWE networks and information systems should be via virtual remote desktop (VDI) technology.
- 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 (classified as confidential and strictly confidential) 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 should 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.

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 inventory of all accounts which are relevant for the service provision to RWE.

- 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 should 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) should 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.

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 ensures confidentiality of information
- Multifactor authentication must be implemented depending on the nature and criticality of the service and the security/protection requirement.

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 should 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 should be covered by a Business Continuity Plan (BCP). Associated assets need to be subject to a corresponding Disaster Recovery Plan (DR Plan). 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.
- 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 or using cloud environments, which are relevant for the service provision to RWE:

- The use of cloud environments to provide services to RWE must be indicated.
- Depending on the information security requirements, appropriate (state of the art) security measures must be applied in the cloud environment.
- The security measures must be applied to the entire lifecycle of the cloud environment.

4.7 Compliance and Assessments

- Upon request, the supplier must respond to a security questionnaire issued by RWE (or a third party appointed by RWE) and provide a written response (including associated evidence) in order to enable RWE to assess compliance with the requirements of this policy.
- Furthermore, in order to enable RWE to confirm/assure compliance with the requirements of this Policy, RWE (or a third party appointed by RWE) may also conduct on-site assessments at all relevant premises of the supplier. The specific scope, duration and arrangement of the on-site security assessments shall take place in consultation and alignment with the supplier and upon reasonable notice.
- The supplier ensures support and cooperation with the designated representatives from RWE involved in such on-site security assessments. This support includes access to all relevant physical premises, systems and personnel as well as the provision of relevant documents, which

includes but is not limited to process documentations, (security) policies and guidelines as well as security-related performance monitoring reporting. In addition, the supplier must require its contractors and subcontractors to comply with these obligations in the same way.

- In case of any weaknesses, deviations and/or non-conformities found during the (documented) security self-disclosure process and/or the on-site security assessments, the supplier will ensure that appropriate risk mitigation and corrective action plans are implemented in a timely manner, and accomplishments will be reported to RWE.

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: Information classification and labelling

How protective measures are set up depends on the need to protect information. This level of protection is not dependent on the medium (analogue or digital) in which the information is available.

To this end, RWE divides information into three confidentiality classes based on the effects of potential damage:

Internal	Consequential damage may be limited and manageable (e.g., internal guidelines, process descriptions; personal data that is generally required to fulfil business tasks, e.g., address books).
Confidential	Consequential damage may be considerable (e.g., premature publication of project plans, publication of contract documents; Personal data which, in the event of loss, damage, disclosure or unlawful processing, may cause substantial damage to the data subject, e.g., bank data).

Strictly confidential	Consequential damage may be catastrophic and threaten the existence of the company (e.g., decisions on intended company purchases/sales, business secrets; Personal data that provides information about health, sex life, ethnic origin, political opinion, religious or philosophical beliefs, trade union membership and genetic/biometric data).

In the following, information of the protection classes 'confidential' and 'strictly confidential' shall be collectively referred to as 'sensitive information'.

The information owner defines the classification for their information at the beginning of the lifecycle (e.g. using the criteria in **Table 1:** Classification of the need for protection information).

- If the initial information owner has not made any classification, the (next) information owner must make the classification after the information has been transferred.
- In the case of sensitive information, the information owner must be clearly identifiable from the document.
- Please note that the need for protection of information can change over time.

Information labelling using Confidentiality classes

- Information must be labelled with a confidentiality class. Always only use the highest applicable classification.

Internal	- Documents should be labelled on the first page.
Confidential	- Documents must be labelled on each page. - Labelling of the data media/ envelope is necessary.
Strictly-Confidential	- Documents must be labelled on each page. - Labelling of the data media/ envelope is necessary.

- **'Public'** information occupies a special role. It does not have to be labelled, but must be classified and published by the authorized business functions (e.g., Corporate Communications).

- Information without visible label can be considered **'Internal'** if it is not obviously sensitive information. This does not apply if the information is obviously **'Public'** (e.g., advertising brochures).
- An adjustment to the labelling is only to be made after consultation with the information owner.

  The information owner must adapt the classification if the need for protection changes.

Note:

- Documents with the lowest protection class are labelled as 'Internal'. This labelling indicates that this information may be passed on to RWE employees without restriction. However, these documents should only be passed on to external parties if necessary.
- Only one labelling is assigned per document. The highest applicable labelling is to be used. A document cannot thus be labelled 'Internally confidential'.

6.1.1 Classification of the need for protection of information

Classification	Public (Öffentlich)	Internal (Intern)	Confidential (Vertraulich)	Strictly confidential (Streng Vertraulich)
Protection requirement	No protection requirement	Low to medium	High	Very high
Potential impacts	None.	– Very little impact on RWE, its employees and its customers and business partners.	– Violation of personal rights. – Significant disruption/termination of a business relationship of value. – Important tasks can only be performed to a limited extent.	– Massive violation of personal rights, severe loss of reputation. – Significant disruption/termination of a business relationship of value with consequences for other business relationships. – Important tasks can no longer be performed.
Examples	– Product information – Press releases – External job advertisements – Names and official contact information of employees with connections to the public (e.g., contact person for recruiting, press spokesperson)	– Communication within the RWE Group – Internal directives – Process Descriptions – Address Books – Organization charts – Personnel number & R-UI	– Customer data – Operational plans – Security concept (e.g., for the annual general meeting) – Unpublished security incidents – Personal information about the employment relationship (e.g., salary data) – Bank details	– M&A Projects – Business development projects – Business secrets – Compliance issues – Medical data – Biometric data for unique identification of a natural person – Data on sexual life or sexual orientation – Criminal convictions and offences

Classification	Public (Öffentlich)	Internal (Intern)	Confidential (Vertraulich)	Strictly confidential (Streng Vertraulich)
Sharing	Information in this category is not restricted.	Information in this category may only be used within the RWE Group and with relevant external business partners.	Information in this category may only be made available to bodies and/or employees who need this data to perform their tasks.	Information in this category must not be released to the public and are only to be shared following the need to know principle.
Labelling	Public information does not have to be labelled, but must only be classified and published by the authorised business functions (Corporate Communications).	Internal information should be labelled on the cover page with the words 'general .	Confidential information must be clearly labelled with 'Confidential' on every page or on any part of the information. Data media must be labelled accordingly.	Strictly confidential information must be clearly labelled with 'Strictly confidential' as such on every page or on any part of the information.

Table 1: *Classification of the need for protection information*

6.2 Annex 2: 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
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.
Sensitive information	Refers to data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.
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 2: Definition of Terms