The Standard was issued in German and translated into English.

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

Instruction / Communication				
Activity	**OU**	**Name**	**Date**	**Approval**
Setup/ Change	Group Cybersecurity (CHV-C)	Stefan Wigchers	18.02.2025	by E-Mail
Functional release	Group Cybersecurity (CHV-C)	Nikk Gilbert	19.02.2025	by E-Mail

1 Modifications

Date	**Modification** (latest 10 modifications)	**Author** (First name, surname, OU)
01.04.2020	First issue	Stefan Wigchers (CEV-DC)
01.10.2020	Editorial revision and adaptation of the password specifications.	Stefan Wigchers (CEV-DC)
03.03.2021	Editorial update and adding the definitions for IT and OT Updating of Disclaimer.	Stefan Wigchers (CEV-DC)
01.12.2023	Editorial update (date, OU, Unbundling clause etc.)	Stefan Wigchers (CHV-C)

2 Objective

Cybersecurity not only has the objective of protecting material and immaterial assets, but also protecting all employees associated with RWE. Company information and data – as well as the systems that process this data – represent assets that are particularly worthy of protection at RWE. For this reason, Cybersecurity is part of the comprehensive security strategy at RWE and is intended to ensure the confidentiality, integrity and availability of information and IT systems.
This Group Business Rule includes binding rules for Cybersecurity and provides external employees with a reliable framework for securely handling information and securely using information and telecommunications systems. Deviating specifications for IT administrators are defined in the currently valid specifications for IT security.
Should you have any questions, comments etc. which refer to the implementation of this Group Business Rule, please address your feedback to the Cybersecurity department part of Group Security (CHV-C). You can also simply and conveniently send your feedback by e-mail to Konzernrichtlinien@rwe.com.

3 Area of application

This Group directive applies to external employees working for RWE AG and all Group companies insofar as there exists and can be exercised legal or factual influence. In the case of minority companies, the best possible implementation of this Group directive should be sought depending on the possibility of influencing it; at the very least, information flows are to be secured.
All security measures are carried out on the basis of the applicable laws and the current jurisprudence including co-determination rights, whereby different jurisdictions may have to be considered.
Where necessary, these Guidelines provide for partial deviations regarding group companies that are subject to the unbundling requirements. These provisions ensure, in particular, that the legal requirements regarding the independence of the group companies being subject to the unbundling requirements, with respect to organisation, decision-making powers and the operation of the respective business are fulfilled and that the confidentiality of economically sensitive information as well as compliance with the principle of non-discrimination are ensured.

Group companies that are subject to the unbundling requirements must ensure that economically sensitive information, of which they become aware in the course of their business activities, is treated confidentially. In particular, such information has to be protected properly against disclosure to competitive and non-competitive units of the group. In case of disclosure of information which may give rise to economic benefits, compliance with the principle of non-discrimination is

ensured. Different regulations may apply to the Operational Technology (OT) area. Please contact your OT manager or line manager if you have any questions.

4 Definition of terms

Term	Explanation
Group Security (CHV-CG)	Group Security controls and monitors security within the RWE Group.
Information owner	The person who issues the order to produce a document or information.
Messenger	(Instant) messaging is a method of communication in which two or more participants communicate by text message. Examples include Threema and Skype.
IT	Information Technology is the constellation of transactional systems used to support and automate administrative and supporting processes in organizations.
OT	Operational technology (OT) is focused on supporting technical processes and process automation. This is all about controlling and monitoring equipment which performs the production process, such as generating electricity.
Security organisation/ security management	The totality of all persons, structures and processes within RWE that are entrusted with the implementation, safeguarding and further development of security.
Single Sign-on	Single sign-on (SSO) enables access to services, applications or resources via a single authentication process. SSO replaces individual logon procedures with different user data and uses a comprehensive user identity.
Social engineering	Social engineering is the name given to interpersonal influencing with the aim of inducing certain behaviour in people – for example, the perpetrator may coerce others into revealing confidential information, purchasing a product or transferring financial resources.
Virtual Desktop Infrastructure (VDI)	Virtual desktop infrastructure allows a virtual RWE computer to work via the Internet.

Virtual Private Network (VPN)	A VPN (Virtual Private Network) connects two networks, one computer to a network or two computers via public connections such as the Internet.

4.1 Symbols used

Symbol	Description
	Cybersecurity requirements to be complied with ('Do's')
	Cybersecurity prohibitions to be complied with ('Don'ts')
	Supplementary information on the implementation of the requirements and prohibitions listed above.

5 Rules, processes and responsibilities

5.1 Handling information

Information is an important asset for the RWE Group and must be adequately protected at all times of its existence (information life cycle). This applies from creation, to recording and deletion, right through to disposal. 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 the need for protection of each piece of information into three protection classes based on the effects of potential damage:

Low to medium	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).
High	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).

Very high	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).

Criteria for the classification of the need for protection can be found in **Annex 1** to this Group Business Rule.
In the following, information of the protection classes 'high' and 'very high' shall be collectively referred to as **'sensitive information'** if both are intended.
In terms of Cybersecurity, RWE pursues the three protection goals of confidentiality, integrity and availability:

Confidentiality	Information may only be made available to authorised persons.
Integrity	Information may not be changed without authorisation and must be correct and complete.
Availability	Information must be available without restriction within the necessary, agreed scope or timeframe.

5.1.1 Classification and labelling

The adequate protection of information throughout its entire lifecycle forms the basis for Cybersecurity.

Classification:

- The information owner defines the need for protection for their information at the beginning of the lifecycle (e.g., using the criteria in Annex 1).
- The protection classes 'low to medium', 'high' and 'very high' should be used to classify the need for protection.
- If the information owner is outside of RWE and the latter has not made any classification, the (first) information owner at RWE 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.

Labelling using confidentiality classes:

- Information must be labelled with a confidentiality class according to its protection requirements. Always only use the highest applicable classification.
- Information of the protection class 'low to medium' shall be labelled **'Internal'**. In this case:
  - Documents must be labelled on the first page at a minimum.
- Information of the protection class 'high' must be labelled with **'Confidential'.** In this case:
  - Documents must be labelled on each page.
  - Labelling of the data media/envelope is necessary.
- Information of the protection class 'very high' is to be labelled with '**Strictly confidential'** in red. In this case:
  - 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 authorised business functions (e.g., Corporate Communications).
- Information without visible label can be considered **'Internal'** if it is not obviously sensitive information. The marking must be made up. 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 exchanged with RWE employees without restriction. See Annex for the type of information qualifying as 'Internal'
- Only one labelling is assigned per document. The highest applicable labelling is to be used. A document cannot thus be labelled 'Internally confidential'.
- The different protection classes and their labelling have requirements that build on each other, as explained below.

5.1.2 Retention and storage of information

Information must also be protected when it is stored and retained. The following rules apply:

- Only store and retain information that you need to perform your job.
- Information must be protected against unauthorised access according to its protection requirements, regardless of the medium in which it is available (e.g., on paper, per e-mail or as a file).
- Media with confidential information must be kept under lock and key.
- For the permanent storage of media containing strictly confidential information, a suitable storage facility (e.g. safe or steel cabinet) must be used. In the course of daily use, media containing strictly confidential information must be kept under lock and key as far as possible using the available technical possibilities.
- Sensitive information on drives and data media must be encrypted or stored in the provided secure data rooms.

Note:

- Contact your responsible RWE contact if you have any questions about data encryption or the use of secure data rooms.

- Inform the RWE IT Service Desk if you have stored sensitive information on an IT component intended for repair so that this information can be adequately protected or, if necessary, deleted.
- Ensure that the level of protection is maintained continuously during transfer to another or additional storage or filing location.

5.1.3 Working with information

When working with information, its security must also be guaranteed. Therefore, the following regulations must be observed:

- Ensure that unauthorised persons cannot access information at your workplace. This applies to when you leave your workplace in particular.
- Keep your workplace tidy and avoid leaving sensitive information exposed.
- Information carriers (e.g., screens, flipcharts) with sensitive information must be placed in such a way that they cannot be seen by unauthorised persons (e.g., from the outside).
- Avoid unintentionally disclosing information when sharing desktops (e.g., when using Teams).
- Do not leave sensitive information on answering machines, in voicemails or in automatic e-mail replies.
- Use the 'secure printing' function for sensitive information.
- If your printer does not yet support secure printing, your line manager is responsible for determining a process for printing sensitive information.
- If you have sent a job to the wrong printer despite all due care, immediately make sure that the printout is destroyed or forwarded to you.
- Collect the printout from the printer immediately. Do not leave your printouts and copies unattended.
- Make sure that you also handle information safely when you work on the go or at home.

Note:

- The technical implementation of the secure printing function can be set up for different levels of convenience depending on the printer and/or RWE company. On some devices, printing starts only after identification via the RWE Service Card, while other devices start printing only after you enter an appropriate password on the device.

5.1.4 Sending and sharing information

Special rules apply to the sending and sharing of information in order to guarantee the protection of the information.

- **Internal** information may
  - only be shared with employees of the RWE Group.
- **Confidential** information may
  - only be shared when required (need-to-know-principle)
  - and only be shared relevant RWE contacts after a confidentiality agreement has been signed.
- **Strictly confidential** information may
  - only be shared on a need-to-know-basis
  - and may only be disclosed to external parties after a specific confidentiality agreement has been signed.
  - At the request of the owner of the information, the disclosure can be limited to a named group of persons. This group must then be listed on the cover page or in the appendix.
- Only use communication media and the associated security measures (e.g., encryption) approved by RWE for sending and forwarding information.
- Sensitive information sent by e-mail must be encrypted (e.g., using MIP, S/MIME etc.).
- Please observe restrictions resulting from confidentiality agreements with third parties and copyrights.

- As the recipient of information, you must ensure that sensitive information cannot be read by unauthorised persons (e.g., by putting privacy film on laptops).
- If you receive information that is not intended for you, please inform the sender and delete this information.

Note:

- Even information that is not sensitive may only be communicated to external parties if necessary and may not be published without permission.
- Your line manager must tell you whether a confidentiality declaration or a confidentiality agreement exists.
- Please contact your line manager for information on approved communication and protective measures.

5.1.5 Destruction/disposal of information

Carefully destroying information and data at the end of its lifecycle helps to prevent sensitive information from falling into the wrong hands.

- Delete or destroy information when you no longer need it. Please observe the statutory retention periods.
- You must use a shredder/shredding machine to destroy **confidential and strictly confidential** information. Alternatively for confidential information, you can use the data protection bins that have been set up.
- You must use a secure method to destroy **strictly confidential** information.
- Please contact the RWE IT Service Desk to properly destroy digital media.

Note:

- Non-sensitive information can be disposed of in the normal waste paper basket.
- For the destruction of "**strictly confidential**" information, a shredder/file shredder of level 3 Cross-Cut or higher (according to DIN 32757) can be used.

- If in doubt, contact your responsible RWE contact to clarify retention periods and how to properly dispose of information.
- Contact the RWE IT Service Desk if you have any questions about the secure deletion of data.

5.2 Secure communication

The exchange of information is part of our daily work. However, the security of this information must also be guaranteed. It is therefore important to take appropriate measures in all communication.

5.2.1 E-mails and messengers

E-mail correspondence is not only used for communication, but also for business-relevant and even business-critical processes. It is therefore necessary to protect e-mails containing sensitive information.

- For company e-mails, please only use the e-mail account provided by RWE.
- Always use a digital signature for messages and data where your identity as sender or the integrity of the message must be established beyond doubt.
- You must encrypt e-mails with sensitive information in any case (MIP, S/MIME or equivalent encryption programs).
- Only use the messengers approved by the RWE Group for the communication of business information. The same requirements for e-mails apply to the encryption of confidential documents.

- You are prohibited from setting up automatic forwarding of company e-mails to non-RWE e-mail addresses.

Notes:

- If an e-mail is suspected of being spam during the automatic check, then it will be marked e.g., as ‘spam’ in the subject line.

- Despite having taken due care, it may happen that proper e-mails are wrongly marked as spam. Therefore, please also check e-mails marked as spam and the 'junk e-mail' folder regularly.
- Be skeptical if you receive an e-mail, for example, with a request to provide personal information. Do not perform actions that unknown people ask you to perform via e-mail. Links in such e-mails often redirect you to fake websites that serve to steal the information entered on them, or can infect your computer with malware.
- Report suspicious e-mails via the Hoxhunt button (if enabled) in Outlook or write to spam@rwe.com or csirt@rwe.com.

5.2.2 Telephone and video conferencing

Information is also shared during telephone and video conferences. These conferences often take place with several participants. It is therefore important to comply with security specifications.

- You must ensure that no sensitive information can be accessed by unauthorised persons during telephone and video conferences (e.g., dial-in with PIN).
- Check the participant list before a telephone or video conference.
- Make sure that no unauthorised individuals are listening in during meetings, telephone calls, in hotel rooms, in the waiting area at the airport, on the train or in a taxi.

- Discussions regarding strictly confidential information may not be held in public.

Notes:

- Contact your RWE IT Service Desk if you have questions about secure telephone and video conferencing solutions.

- If your contact person is familiar with the process, he or she will understand you without you having to provide details or specific names.

5.2.3 Meetings

Information is exchanged with other people during meetings. Therefore, the following security measures must be observed.

- Sensitive information is only to be exchanged between authorised participants during meetings.
- You must know the group of participants; in particular, you should know who is and who isn't an RWE employee.
- Meeting rooms containing sensitive information must be locked when not in use.
- At the end of a meeting, the chairperson/organiser must ensure that no documents, information on whiteboards or flipcharts or mobile IT components brought along are left behind.
- As organiser and chairperson of a meeting, you must check whether **strictly confidential** information can be exchanged. If so, rooms which are not visible from the outside and make it difficult to listen in (e.g. closed door) should be used for this purpose.
- Make sure that participants do not connect any external IT components (e.g., mobile devices, USB sticks etc.) to the RWE infrastructure (e.g., RWE laptop or network). The use of RWE projectors and screens is not affected by this regulation.

Notes:

- Make sure that the rooms are not left unattended during breaks in the meeting.
- Contact your responsible RWE contact, if you have any questions about suitable secure rooms.

5.2.4 Internet

The behaviour of employees when using the Internet makes an essential contribution to the protection of information.

- You are obliged to access the Internet exclusively via the designated secure channels that are protected with specific systems (e.g., firewalls) of your RWE IT service provider.

- You are prohibited from changing any configuration set up by RWE IT service provider for using the Internet. Only this person has the authorisation to install and configure the Internet access software.

Notes:

- The retrieval or storage of certain content (e.g., content harmful to minors, gambling) on the Internet can be prosecuted under criminal law. Please bear in mind that this can have consequences under labour law.
- If you discover irregularities when using your browser on RWE owned infrastructure (e.g., RWE laptop or network), please notify the RWE IT Service Desk.

5.2.5 Social media

The information posted on social media (e.g. Facebook and Instagram) is publicly accessible to a larger group of people. External parties are often unable to ascertain whether these are professional or private expressions of opinion.

- Clearly mark private statements about RWE as your personal opinion (e.g., 'I think' or 'My personal opinion is...').

- Never disclose company information on social media. This also applies to non-sensitive information. This can have an impact on the company and affect RWE AG's share price, for example.
- Do not share any pictures or videos in which safety devices (e.g., fencing, camera technology, barrier systems etc.) are visible.

- Never communicate sensitive information on social media.

Notes:

- Remember that e.g., insults/defamation regarding the employer can have consequences under labour law. The same applies to the violation of company and business secrets.
- Be vigilant when publishing personal information! Attackers may try to spy on this information in order to use it for an attack (e.g., phishing).

5.3 Secure handling of IT components and access points

It is difficult to imagine working without IT components and having access to them today. It is therefore all the more important to uphold the security of these components.

5.3.1 Passwords and access protection

Passwords serve to identify the user. Access protection is an important means of ensuring the confidentiality of information.

- Change default and initial passwords immediately.
- Use different passwords for different systems and applications. This is not applicable for systems and applications which are using a single sign-on.
- Do not write down passwords in plain text (e.g., unencrypted in a file).
- Your passwords must be at least twelve characters long.
- Do not use keyboard patterns, names, dates or terms from dictionaries. Instead, use the first letters of a sentence, for example.
- If technically possible, use at least three of the following character types: uppercase letters, lowercase letters, special characters and numbers.
- Make sure that nobody can see the screen or keyboard when you are entering your password.
- If you suspect that your password has been compromised, change it immediately and contact the RWE IT Service Desk and/or the responsible RWE contact, if necessary.

- If you notice that you have been given erroneous access to data, IT components or applications, please inform your responsible RWE contact immediately.
- Do not deliberately try to gain access to data for which you do not have access authorisation.

- Never share your passwords with anyone else. This also includes colleagues, responsible RWE contact and the RWE IT service provider or RWE IT Service Desk.
- Never hand your access data over to other people.
- Never enter passwords on websites you are unfamiliar with or in unfamiliar applications.
- Do not use access data such as usernames or passwords that you use in your operational environment outside of RWE (e.g., on the Internet).

Notes:

- One way to create a password is to come up with a basic password from the first letters of a sentence, for example. The sentence 'It is usually 30 degrees in the summer' would produce the basic password 'Iiu30dits'. The other passwords could then be systematically derived from this, for example, for SAP it would be 'Iiu30ditsSAP'.
- Please remember to use a different basic password than the one given in this example.

5.3.2 Using IT components

The IT components provided for your work (computer, laptop, smartphone, tablets etc.) meet the requirements of Cybersecurity. This protection cannot be guaranteed if you make changes to them or use other components.

- Use provided IT components only for business activities.
- Set up an access or device password, activate an existing screen or keyboard lock and protect access with a password.

- Only use properly licensed standard/application software or data (e.g., no unauthorised copies of licensed programs).
- You must install system updates promptly and independently if you receive a request to do so from RWE IT service provider.
- When leaving your workplace, you must ensure that no unauthorised person can use your PC by locking the computer.
- Never leave mobile IT components unattended outside of your workplace (e.g., in meeting rooms or on the train)
- Secure your device against theft. Use the provided anti-theft protection (e.g., Kensington lock) or lock the office when leaving.
- In the event of loss, theft or suspected unauthorised use of your IT components, please inform the RWE IT Service Desk immediately.
- You must use an encrypted connection (e.g., VPN or RWE VDI solutions) to connect remotely to the corporate network.
- Only use public networks (e.g., Wi-Fi) in exceptional cases.
- You must contact RWE IT Service Desk if IT components need to be repaired or disposed of.
- Make sure that the SIM card is removed (if present) and the data is deleted when you send a mobile IT component for repair.

- You may not independently install hardware or software on operational components. This is the task of the RWE IT service provider.
- You are not permitted to make any changes to IT components (especially security settings).
- Non-RWE IT components (e.g., laptops, mobile devices etc.) may not be connected to RWE's IT infrastructure.
- The processing of company data on smartphones is allowed using only devices installed with the RWE mobile device management (MDM) solution.

- You are not allowed to process sensitive information on mobile IT components without encryption.
- Synchronising operational data to other devices/IT components or to cloud services not licensed by the company is not permitted.
- You may not use cloud storage solutions that have not been licensed and approved by the company (such as storage providers like Dropbox or Google Drive etc.).

Note:

- If assigned RWE laptop, then being the 'local admin user' does not entitle you to change the protective measures set by the RWE IT service provider.
- You can lock your computer using the key combination 'Windows button + L', for example.

5.3.3 Protection against malicious programs

Malicious programs pose a threat to Cybersecurity. They are distributed via the Internet, by e-mail or on mobile data media.

- Do not open or share files from dubious sources, such as attachments from e-mails of unknown origin or from mobile data media.
- Contact the RWE IT Service Desk immediately in the event of a suspected or identified malware infestation.

- You are prohibited from overriding, modifying or circumventing the protective measures of the RWE IT service provider against malware.

Notes:

- Check information/data that you receive from external sources before opening it for the first time, e.g., with your workplace computer's virus scanner. The RWE IT Service Desk will be happy to support you.
- An IT component's unexplained system behaviour (frequent error messages, program crashes, computer crashes etc.) can indicate that a malicious program has corrupted it. Inform the RWE IT Service Desk

immediately even if, for example, pop-up windows with dubious advertising offers appear frequently.

- Report suspicious e-mails via the Hoxhunt button (if enabled) in Outlook to have such e-mails checked or write to spam@rwe.com or csirt@rwe.com.

5.3.4 Using apps on smartphones and tablets

An app is a software application for mobile devices such as smartphones and tablets.

- The installation and private use of installation platforms/app stores on service devices within RWE companies is only permitted if company data is protected by suitable technical/organisational measures (e.g., by using Intune).
- Only installation from regular installation platforms/app stores is permitted.
- Only licensed or license free applications may be used.
- Keep installed apps up to date, especially in the case of security-relevant updates from the software manufacturer.

- The installation or use of tools or utilities that compromise the system security of mobile IT components (e.g., jailbreaking, root mode) is prohibited.
- The installation or use of apps that jeopardise or may jeopardise the security of the device is prohibited.

Note:

- If you have any questions about mobile device management (e.g., MobileIron), please contact the RWE IT Service Desk.

5.3.5 Data media

The confidentiality of information on mobile data media is jeopardised by loss, theft or disclosure.

- Only use mobile data media (e.g., USB sticks) provided by RWE.
- Only use mobile data media if there is no reasonable alternative ('minimisation').
- When transferring information to mobile data media, you must ensure that no other data is present on the data media.
- Data on mobile data media must be protected against unauthorised access (e.g., by using encryption).
- When receiving/sending mobile data media with integrated password protection, you must transmit the password via a separate communication channel (e.g., via an encrypted e-mail).
- Sensitive information may only be stored on encrypted, mobile data media.
- Secure document exchange (secure data room) must be used when exchanging information with RWE.
- Sensitive information must be deleted securely.

- Without further checking the origins and virus scan, you may not connect mobile data media to operational IT components. If in doubt, contact your RWE IT Service Desk.

Note:

- Mobile data media should only be sent in exceptional cases and only to authorised persons (e.g., members of a project).
- Please contact the RWE IT Service Desk if you have any questions about how to securely delete data.

5.3.6 Data backup

The protection of secured data must be guaranteed. This applies in particular to sensitive information in order to prevent potential damage.

- Store your data on an operational server and drives allocated/shared by your responsible RWE contact. The RWE IT service provider will automatically and professionally secure them.
- You are responsible for backing up locally stored information.
- Data backups on data media with sensitive information must be kept under lock and key.
- Data that is only stored on mobile IT components should be backed up regularly – preferably on a weekly basis. The data backup must be protected from being accessed with a password and encrypted. When backing up data, please observe the legally stipulated retention periods.

- It is not permitted to secure operational and sensitive information on cloud services that have not been licensed and approved by the company. If in doubt, please contact RWE IT Service Desk.

Notes:

- Contact your responsible RWE contact for more information on retention periods and the proper disposal of information.

5.4 Security on business trips

IT components and information are exposed to an increased risk during business trips. It is therefore essential to implement the following measures to ensure increased protection.

5.4.1 During the trip

It is essential to carefully handle mobile IT components and sensitive information on business trips.

- If you work on the go, you must ensure that unauthorised persons cannot 'read' your information (e.g., by putting privacy film on your laptop).
- Always carry mobile IT components, sensitive information and data in your hand luggage.

- Always turn off your laptop completely and secure it physically against theft (e.g., with a Kensington lock on stationary items).
- If possible, store mobile IT components and sensitive information in your hotel room safe.
- Only use encrypted connections to access the RWE network, e.g., the RWE VPN connection with your laptop, because this allows you to work safely via Wi-Fi networks. Do not use public, unsecured Wi-Fi networks.
- If you are asked to hand in your mobile phone, smartphone or tablet during meetings with business partners, switch off your device completely and remove the SIM card before handing it over.
- Sensitive information must also be destroyed securely during business trips. If in doubt, dispose of it at the office in the usual way after the end of the trip.

- You are prohibited from leaving mobile IT components with hotel staff.
- Keep mobile IT components out of sight (e.g., in a hotel room).

Notes:

- If no room safe is available, store your sensitive information in locked luggage.

5.4.2 After the trip

Measures to protect IT components and information must be implemented even after the trip has ended.

- You must report any security-relevant incidents or observations to the RWE IT Service Desk immediately if you were unable to do so during the trip.

- You are not permitted to use mobile IT components if you have reasonable suspicions that they have been tampered with. Please contact the RWE IT Service Desk immediately and without delay.

5.5 Reporting security incidents

The security situation can be better assessed thanks to security incidents being reported and evaluated. This allows necessary adjustments to the rules to be identified and implemented.

- If you discover a security incident (e.g., loss of sensitive data, theft of hardware containing sensitive information, suspicious behaviour of your IT components), or suspect any potential social engineering event, report it immediately to the RWE IT Service Desk and inform your responsible RWE contact.
- Report suspicious e-mails via the Hoxhunt button (if enabled) in Outlook to initiate an examination or write to spam@rwe.com or csirt@rwe.com.

6 Group regulations out of force / concurrently in force

6.1 Group regulations out of force

-/-

6.2 Group regulations concurrently in force

– GDI_008 ‘Cybersecurity’

7 Annexes

Annex 1: Classification of the need for protection of information

Annex 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	– Technical documentation – 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 must be labelled on the cover page with the words 'Internal' or 'For internal use only' at a minimum.	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.