IT POLICY

MYTY

Inhalt

Version 1.0 vom 27.08.2025

1. Introduction

The objective of this policy is to establish uniform regulations for the use of IT systems, IT services, and data, as well as to define relevant behavioral guidelines. The policy ensures compliance with legal requirements, adherence to specified security standards (such as our Minimum Information Security Requirements), and minimizes errors in IT usage. This ensures information security, as well as the confidentiality, availability, and integrity of systems.

This policy governs the use of all data processing devices (including infrastructure, networks, computers, laptops, tablets, smartphones, peripheral devices, etc.) and IT services provided by MYTY Group AG, MYTY Group Germany GmbH, and all affiliated companies within the corporate group (hereinafter referred to as the "Company") or those utilizing the Company's infrastructure.

This policy applies to all employees of the company. This includes all permanent employees, part-time employees, trainees, working students, temporary staff, and others. External individuals working on behalf of the company are also required to comply with this policy. The company will take appropriate measures to ensure that this policy is binding for external parties as well.

Every user of IT systems, IT services, and data is obligated to comply with all applicable laws and internal regulations. The entirety of these regulations is binding.

In general, supplementary regulations may be established as country-specific guidelines. However, these must not override the provisions of this policy. Individual business units of MYTY Group AG, MYTY Group Germany GmbH, and the companies within the corporate group may implement additional, stricter requirements beyond those specified in this policy.

2. User Responsibilities

2.1. Basic usage rules

To ensure information security as well as the confidentiality, availability, and integrity of systems, the following is prohibited:

1) The use of IT systems, IT services, and data is strictly prohibited if it:
    a) Violates any applicable laws or regulations,
    b) Breaches data protection, privacy, copyright, or criminal law provisions,
    c) Is detrimental to the company's business interests,
    d) Involves or communicates offensive, discriminatory, defamatory, threatening, unconstitutional, racist, sexist, obscene, sexually explicit, pornographic, or otherwise objectionable content (harassment and discrimination may occur based on references to gender, nationality, ethnic or national origin (including skin color), age, sexual orientation, marital status, religious belief, or disability),
    e) Contains ideological, religious, or party-political content, or
    f) Is used for personal financial or commercial gain, including advertising.
2) Unauthorized access to computers, smartphones, notebooks, tablets, or other devices, files, data, voicemails, or emails belonging to other individuals.
3) Misrepresentation or impersonation, including providing false or inaccurate identification or pretending to be someone else.
4) Using the company's IT systems, IT services, or data to grant unauthorized persons access to the company's data processing devices or to IT systems, IT services, or data of other companies.
5) Activities that impair the intended operation of IT systems, IT services, or data, or that compromise information security.
6) Public registration of the company's name or brand on a website or any other electronic IT service without prior approval from an authorized body (except for

mentioning the employer in personal profiles on social networks). Only accounts that require the company's name and address for business or technical reasons are permitted.

7) When operating private websites, blogs, forums, chats, or social media profiles, the following risks must be avoided:
    a) Damage to the company's reputation or that of its employees through negative portrayal.
    b) Disclosure of protected or confidential information, which could compromise security or confidentiality.
    c) Violation of security policies or applicable laws, including but not limited to data protection and compliance regulations.

Company-provided end devices must be handled with care, used properly, and maintained in good condition. During transport, devices must be stored in suitable padded bags, backpacks, or equipped with appropriate protective cases. When transporting devices in a vehicle or on public transport, they must be secured to prevent uncontrolled movement due to traffic or sudden stops. Devices must be cleaned regularly using appropriate cleaning materials.

2.2. Corporate use of company end devices and IT Services

1) For data or software purchased, leased, developed, or created by the company, copyright and licensing terms must be observed. Transferring such data or software to third parties is only permissible for legitimate business purposes and in compliance with the applicable licensing terms, provided that the licensing terms explicitly allow such transfer.
2) The independent installation and any modification of system or application software are prohibited. Approved software is generally provided via Mobile Device Management (MDM). Software that cannot be deployed system-wide via MDM will be provided exclusively by the IT department. The use of private or

unlicensed software copies on company computers is strictly prohibited, as is the use of free or trial versions. In case of need, employees must contact the IT department, which will decide on further action. Exceptions require approval by the executive management upon request.

3) In the event of a requirement for new hardware or software, IT must first verify whether alternatives or existing license agreements are available. Costs for required hardware and software may only be incurred after approval in accordance with the currently valid authorization guidelines and must not be covered by private funds.
4) In the event of any malfunction, incident, or other issue that impairs the intended operation of IT systems, IT services, or data, or that poses a risk to information security, the IT department must be notified immediately.
5) Any occurrence of malicious code (such as viruses, trojans, worms, etc.) must be reported immediately to the IT department by phone and email.
6) Company-provided hardware may only be used for official business purposes, except in cases of contract work (e.g., for external employees, external consultants, etc.).
7) Any loss of notebooks, smartphones, storage media, or transponders/keys must be reported immediately to the responsible supervisor and the IT department. The same applies to any suspicion of unauthorized use or manipulation of PCs, notebooks, or smartphones by third parties. IT must, if necessary, immediately block access or deactivate the device. If the device is recovered, it must be examined by IT for manipulation or malicious code (e.g., keyloggers, malware, log files) before being reconnected to the corporate network.
8) All support requests or requirements must be submitted via email to IT or logged in the IT ticketing system. This can be done by the employee themselves or by IT on their behalf.
9) In the event of security incidents involving IT systems, IT services, or data, employees must follow the instructions provided by IT.

10) When leaving the workplace, PCs, notebooks, smartphones, tablets, etc., must be locked to prevent unauthorized access. Automatic locking is configured according to the current settings of the Mobile Device Management (MDM) system.
11) At the end of the workday, IT equipment (except smartphones) must be shut down or at least locked. Exceptions apply to automated processes running beyond working hours or systems providing continuous IT services (e.g., print servers, file servers).
12) When accessing emails or the company network outside of business premises, ensure that personal or confidential data is not automatically saved and cannot be viewed by unauthorized parties (e.g., automatic saving of login credentials in web browsers). Employees must log out of IT services after use.
13) Guests/visitors may only use the provided guest WLAN. They must be informed or confirm that the guest WLAN is to be used exclusively for professional purposes in compliance with the applicable laws of the respective location. Usage may be logged and evaluated to ensure information security. If a guest/visitor requires access to internal IT services and systems, this may only be granted via company-provided devices.
14) The creation of extensive user-developed procedures (e.g., programs, scripts, Excel sheets, Access databases) requires prior approval from the respective supervisor or IT. Additionally, the Data Protection Coordinator or Data Protection Officer must be notified. Procedures must be documented in a way that allows a qualified third party to understand and maintain them within a reasonable timeframe.
15) All devices provided to employees are documented by IT. Each device is recorded with an inventory number and device description in an issue log, which must be signed by the employee.

2.3. Personal use of corporate IT devices and services

1) Company-provided devices (computers, notebooks, tablets, smartphones (including telephony and data usage), IT systems (network including Wi-Fi, servers, peripherals, etc.), and services are primarily intended for business use. Limited personal use is permitted during breaks and outside working hours, provided it does not interfere with business operations and complies with the usage guidelines outlined in Section 2.1. The IT department conducts random checks to ensure compliance with these restrictions. All data traffic is logged by the company for monitoring and security purposes.
2) The use of private devices to access the company's IT systems, IT services, and data is prohibited. Exceptions apply to company IT services accessed via the cloud that do not synchronize data to private end devices and thus ensure that data sovereignty remains with the company (e.g., Microsoft Office 365, Google Workspace, Slack). Connecting private devices to the company's IT infrastructure is also prohibited, except for private end devices that have been explicitly approved by the IT department (approval must be documented in text form) and thus comply with the company's policies. If IT approval is granted, private devices may only connect to the guest/visitor Wi-Fi network.
3) The company does not generally provide or support remote workstations involving the use of private end devices for performing work-related tasks. Therefore, accessing the company's IT services via private devices and/or private infrastructure is prohibited. Exceptions apply to company IT services accessed via the cloud that do not synchronize data to private devices, thereby ensuring that data sovereignty remains with the company (e.g., Microsoft Office 365, Google Workspace, Slack). Any further exceptions require explicit approval by the executive management upon request.
4) When working remotely, employees are required to use only company-provided devices (computers, laptops, tablets, smartphones for both telephony and data

usage). Peripheral devices without data storage capabilities are exempt from this requirement. Data sovereignty must remain with the company at all times. The use of corporate IT services via private devices is prohibited. The use of private infrastructure (e.g., internet access) is permitted. In the event of a violation, the employee consents—by signing this policy—to the complete deletion of data from the private device if necessary. Exceptions apply to company IT services accessed via the cloud that do not synchronize data to private devices, thereby ensuring that data sovereignty remains with the company (e.g., Microsoft Office 365, Google Workspace, Slack). Any further exceptions require approval by the executive management upon written request.

5) Company-owned, licensed, developed, or custom-built software may be used for minor personal purposes during breaks and outside of working hours, provided that such use does not violate licensing agreements, applicable laws, or incur additional usage-based fees or transaction costs.
6) The installation of private or unauthorized software is prohibited.
7) Data purchased, leased, developed, or created by the company must not be used for private purposes.
8) Private data must not be stored on central company storage systems (e.g., SharePoint, OneDrive, Google Drive, network shares, etc.). Private data may only be stored on the provided end devices (without any restriction on the storage capacity required for business purposes). Employees are solely responsible for backing up their private data. The company assumes no liability for the loss of private data. If the company encrypts end devices, private data stored by the employee may also be encrypted. In cases where the company requires access to company-provided end devices, it cannot be ruled out that private data may become known to the company. Before an end device is exchanged, employees have the opportunity to delete their private data. The company may create a backup of the end device before replacement or at another necessary time. Any private data not deleted by the employee will become part of the backup, and the

employee has no claim to the deletion of such backups.

9) Company-provided devices, even if personal use is permitted, remain the property of the company and must be returned upon termination of employment.
10) If a company-provided device is transferred to private ownership based on a separate agreement, the employee consents, by signing this policy, to the complete deletion of all data from the device prior to its handover, if required.
11) Auch bei wiederholter, vorbehaltloser Gewährung der Privatnutzung entsteht kein Rechtsanspruch auf Gewährung für die Zukunft.
12) The company must comply with statutory retention obligations. If private data of the employee is generated alongside business data due to private use, the employee grants consent for the storage of such resulting private personal data. If the employee does not grant this consent, private use is prohibited.
13) Access to the office networks (LAN and Wi-Fi, except for the guest Wi-Fi) as well as remote access via VPN is permitted exclusively through company-provided devices.

2.4. Telephony and mobile data communications

1) The private use of telephony functions and mobile data connections via mobile network operators, as well as company-provided landline telephones/telephony services, is permitted to a minor and reasonable extent, provided that any associated costs are taken into account. Business-related private use (e.g., notifying family or close contacts of delayed return) is generally considered official use. All telephony connections and data traffic are logged by the company.
2) Even if private use is granted repeatedly and without reservation, this does not create any entitlement to such use in the future.
3) The company must comply with statutory retention obligations. If private data of the employee is generated alongside business data due to private use, the employee consents to the storage of such incidental private personal data. If the

employee does not provide consent, private use is prohibited.

2.5. Data storage and transmission

1) All business-relevant data must be stored exclusively on company-provided end devices, central storage systems, or approved external IT services to prevent data loss. Storage on systems explicitly approved by the customer is also permitted, provided that no applicable laws or data protection regulations are violated. It is essential to ensure that only the respective customer's data is stored on the customer's systems. Unless the company specifies an alternative method or technical measure, data transfer must be conducted via a secured connection (VPN). Storing company-created or company-related data on storage systems, cloud services, or external data carriers (e.g., USB drives) that have not been provided or approved by the company is strictly prohibited. Additionally, the transmission of data via cloud services not approved by the company is not allowed. Furthermore, all business-relevant data carriers must be protected against theft, especially during travel.
2) When sharing data with external third parties, ensure that access is restricted to the specific intended recipient only. Data must not be made accessible to anyone with the corresponding sharing link unless explicitly authorized.
3) When working offline (without a network connection), data must be transferred promptly and regularly to the company's storage system. Unless another method or technical measure is specified by the company, the transfer must be carried out via a secure connection (VPN). In the event of loss (misplacement, theft, etc.) or damage to a company device (laptop, computer, smartphone, tablet, storage media), no more than one day's work should be lost. This responsibility lies with each employee.
4) Local storage of data (e.g., on the 'Desktop', in the 'My Documents' folder, etc.) is only permitted if the data is promptly and regularly transferred to the company's

designated storage systems.

5) Redundant data storage on storage systems must be avoided.
6) Mobile storage media (e.g., hard drives in notebooks, external hard drives, USB sticks, etc.) provided by the company must be used in encrypted form only. If an employee notices that a provided storage medium is not encrypted, they are required to encrypt it immediately. For further questions, the employee should contact the IT department without delay.
7) The transfer or synchronization of company or customer data (e.g., between notebooks and smartphones) is only permitted between devices provided by the company. The only exception applies to private devices that have been explicitly approved by the IT department (at least in text form) and are therefore subject to the company's policies. In the event of a violation, the employee consents, by signing this policy, to the complete deletion of data from any non-company-provided device if necessary.
8) Transmission of personal or confidential data (via email, shares, FTP, etc.) over public networks must be conducted exclusively in encrypted form (e.g., using confidential mode in Gmail or via VPN). Additionally, it must be ensured that shares, FTP, and similar methods are only sent to identified individuals and not anonymously, and that links to such data are not publicly accessible.
9) Transmission of special categories of personal data or confidential information (such as salary details, performance appraisals, etc.) via internal networks must be encrypted (e.g., using confidential mode in Google Mail or VPN). Additionally, it must be ensured that shares, FTP, or similar methods are only accessible to identified individuals and are not sent anonymously or made discoverable via public links.
10) Information carriers (e.g., printouts) that are no longer required and contain personal or confidential data must be disposed of in compliance with data protection regulations. This can be done using a paper shredder or designated containers. Obsolete data storage media (e.g., USB drives, CD-ROMs, external hard

drives) must also be handed over to IT for secure and data protection-compliant disposal via the designated containers.

11) Printouts containing personal or confidential information must be collected immediately from unsecured printing devices (e.g., those not protected by password or ID card access).

2.6. Password Management

1) Personal passwords (e.g., logins, internal systems, access to systems or software provided by external vendors) must be protected against unauthorized use (e.g., by using a password manager like 1Password) and must not be shared with anyone.
2) Where passwords are not system-generated, access to systems containing personal or confidential information must be secured with passwords meeting the following criteria: a minimum length of twelve characters, alphanumeric (including both uppercase and lowercase letters and numbers), and containing at least one of the following special characters: # $ & - ! ? % = : ( ).
3) If shared group accounts are absolutely necessary and no technical measures are available to prevent the disclosure of the password to all group members, the following applies:
    a) Logins must be managed using a password management tool (e.g., 1Password). Multi-factor authentication (MFA) must be enabled, and the password must comply with the requirements specified in Section 2.6, Paragraph 2.
    b) Group passwords must be changed immediately if a group member leaves the company or if the password becomes known to unauthorized individuals.
    c) Any system or data changes made using a group account must be logged separately to ensure traceability to an individual physical person.
    d) The same criteria for assigning group passwords apply as for personal

passwords (see Section 2.6, Paragraph 2).

4) The transmission of passwords is prohibited. Passwords must be managed exclusively via a dedicated password management tool (e.g., 1Password).

2.7. Information security

1) Access to company-provided IT services should, wherever possible, be conducted exclusively via encrypted connections (VPN) to ensure that the organization's security systems are fully activated and effective.
2) Users are required to manually lock their workstations (e.g., by pressing Win + L or Ctrl + Command + Q on macOS) when leaving them unattended for short periods. For extended periods of inactivity, users must log off completely
3) Access to computers, laptops, smartphones, tablets, or other devices by unauthorized individuals must be prevented to protect the confidentiality of content, email messages, and voice messages. This can be best achieved by ensuring that devices are not accessed in the direct presence of unauthorized persons or by locking the device when not in use, in accordance with Section 2.
4) To further restrict visibility of device screens—especially during work in public places or while traveling—the use of privacy screen filters is recommended. For smartphones, the message preview on the lock screen must be disabled to ensure that previews are only visible after entering a PIN, Touch ID, Face ID, or other authentication methods.
5) Access rights are granted in accordance with the principle of least privilege ('need-to-know' basis).

2.8. Remote Working

1) When working remotely, employees must use a private and secured internet connection or, alternatively, a personal hotspot (e.g., via smartphone). Accessing corporate systems or data via public hotspots must generally be avoided.

2) It must be ensured that the rooms where mobile work is performed are not accessible to unauthorized third parties for the duration of the mobile work. Appropriate measures must be taken to prevent unauthorized access to work equipment, data, or documents (e.g., locking away paper documents, locking the work computer, etc.).
3) Visual Privacy: Ensure that unauthorized third parties cannot view official documents or data. In particular, measures must be taken to prevent laptop screens or documents from being viewed "in passing" (e.g., by using privacy screens or restricting the visibility of screens).
4) Acoustic Protection: Ensure that official conversations cannot be overheard by unauthorized third parties. In particular, when working remotely, no acoustic assistance systems (e.g., Alexa) should be present.
5) Internet Access Usage: Private or mobile internet access used for remote work must be secured appropriately.
6) Data Backup: Data must always be backed up in accordance with company guidelines. If data is temporarily stored locally, it must be transferred to the company's designated data storage systems at the earliest opportunity.
7) Access Rights: The company or its employees (after prior agreement) must be granted access to remote workspaces. This is particularly necessary to verify compliance with this agreement or to check adherence to data protection regulations (e.g., by the company's data protection officer). Access must be granted during standard business hours (e.g., between 9:00 AM and 6:00 PM). In urgent cases, access must be granted without prior notice. The fundamental rights and freedoms of employees and the protection of their privacy must always be respected.
8) Compliance with Instructions: Employees must comply with the employer's instructions even when working remotely.
9) Remote Work Outside the EU: Employees who intend to work remotely from a non-EU country must obtain prior written approval from the IT and HR

departments. Accessing IT systems and services from abroad is subject to special security requirements: Access to company resources must exclusively occur via a Virtual Private Network (VPN) approved by the IT department, using strong authentication (two-factor authentication). Storing confidential company data on local devices is prohibited; all data processing activities must take place within the secure infrastructure provided by the company.

2.9. Clean desk policy

At the end of each workday, the following rules apply to all workstations within the company: All confidential documents and materials must be removed from desks and securely stored. This also applies to removable media such as USB drives. All IT systems and mass storage devices must be securely locked or stored before leaving the workspace.

3. Internet and Email Usage

3.1. Use of Email Mailboxes

1) E-mails containing personal or confidential information may only be disclosed, shared, or forwarded to authorized individuals (e.g., in accordance with deputy regulations).
2) Forwarding company e-mail addresses or messages to private e-mail accounts is prohibited unless the private use is considered business-related and thus qualifies as company-sanctioned private use.
3) The integration of company e-mail accounts or addresses into e-mail clients not provided by the company is prohibited.
4) Using the company e-mail address to register for privately used accounts or portals is prohibited.
5) Integrating private e-mail accounts or addresses into e-mail clients provided by

the company is prohibited.

6) Access to an employee's e-mail account may be granted by management for valid business reasons, adhering to the four-eyes principle.
7) ncoming e-mails must be carefully checked for integrity, confidentiality, and authenticity of the sender and content. If in doubt, attachments must not be opened, and affected e-mails must not be forwarded without prior consultation with IT.
8) The use of private e-mail accounts and addresses for business purposes is prohibited.

3.2. Internet Usage

When using information retrieved from the internet, caution must be exercised, as the integrity, confidentiality, and authenticity of such information cannot be guaranteed. Therefore, it cannot be ensured that the information in question is accurate, precise, or complete.

3.3. Personal use of the internet

1) The internet access provided by the company is primarily intended for business use. Private use is permitted to a minor extent during breaks and outside working hours, provided it does not impair business operations, and in accordance with the principles outlined in Section 2.1. The same applies to private internet use via company-provided internet-enabled devices outside the company premises. Work-related private use (e.g., notifying family or close contacts of a delayed return home) is generally considered business use.
2) Repeated, unconditional permission for private use does not create a legal entitlement for future use.
3) The company is required to comply with statutory retention obligations. If private data of the employee is included among the business data due to private use, the

employee grants consent to the storage of such personal private data. If the employee does not grant this consent, private use is prohibited.

3.4. Private use of the corporate email account

The use of the company-provided email account, email clients (locally installed, via mobile devices, or web access), or the company email address for private purposes is strictly prohibited, regardless of whether company IT equipment or private devices are used.

3.5. E-mail archiving

1) Due to legal retention requirements and for security reasons, the company uses technology to archive all emails in their original form. This means that all incoming and outgoing emails are stored in the email archive in their original state, regardless of whether they have been processed in the employee's mailbox. Additionally, all incoming emails from external sources to functional mailbox addresses are logged, including sender, recipient, email ID, date, and time.
2) Employees are aware that private emails or emails received unintentionally are also part of the email archive. Archived emails containing personal data cannot be deleted individually, and therefore a right of revocation cannot be granted.

4. Data collection

1) To comply with legal requirements and ensure information security, the company logs all access to IT systems, IT services, and data, stores these logs, and evaluates them as necessary.
2) Personal data collected during the use of IT systems, email, internet, and telephony services is not used for performance or behavioral monitoring. The legal basis for processing personal data to ensure the proper operation of email and

internet services is the company's legitimate interest. The recorded log and connection data are used exclusively for the following purposes: Billing of internet usage, Ensuring system security, Defending against and/or analyzing cybercrime, Managing network load distribution and optimization, Analyzing and correcting technical errors and malfunctions, Monitoring for misuse, and Investigating suspected criminal offenses. With the exception of data subject to archiving as per Section 3.5, the processing of stored personal data is restricted after approximately six months. After this period, the data is retained only as part of long-term archiving.

3) Due to legal obligations, the company is required to retain business records and data for several years. If private employee data is included among business data due to the private use of IT systems, IT services, data, or the internet, this agreement regulates the employee's consent to the storage of such private personal data.
4) Employees must exercise caution when sending emails, text messages, voice messages, or other electronic communications, as incorrect or inappropriate statements can lead to liability for both the company and the individual. In some cases, such statements may even result in criminal liability. Employees should always assume that their emails, SMS, voice messages, or other electronic communications may be accessed, read, or heard by third parties. Regardless of confidentiality or sensitivity, such communications may need to be disclosed due to data protection laws, freedom of information requests, or other legal obligations, court proceedings, or investigations by regulatory authorities. The same level of care should be applied to electronic communication as to written communication, avoiding ambiguity and inaccuracy.

5. Misuse Control

1) All employees have both the right and the obligation to report any suspected or

actual misuse or attempted misuse of IT systems, IT services, and data to the company or their respective supervisor.

2) Personal monitoring of the use of IT systems, IT services, and data will only occur if there is a concrete suspicion of a violation of these regulations. In such cases, the company is entitled to conduct a personal review and evaluation to clarify the suspicion. This may include, but is not limited to, accessing stored data, disclosing the content to the individuals involved in investigating the suspicion, and securing the relevant information. Log data collected will only be evaluated for the purpose of clarifying the specific suspicion.
3) In the event of detected misuse of IT systems, IT services, or data, the company reserves the right to:
    a) Block access to content that is clearly non-business-related and/or poses a security risk,
    b) Revoke or restrict the affected employee's access privileges, and
    c) Initiate and enforce disciplinary measures, including obtaining the employee's statement, in accordance with labor law.

6. Employee offboarding

1) All operational data is subject to statutory retention periods. After an employee leaves the company, their operational data is archived and may, if necessary, be randomly reviewed for legal or regulatory purposes. By acknowledging the Policy on the Use of IT Systems, IT Services, and Data, the employee confirms their consent to this procedure.
2) All company-provided end devices (including PCs, notebooks, smartphones, tablets, accessories, and peripheral devices) must be returned to the respective supervisor, a person designated by the supervisor, or the IT department upon request or when no longer required for business purposes.

3) Data purchased, leased, developed, or created by the company may not be used for private purposes after leaving the company.
4) The employee's accounts for IT systems and IT services are deactivated.

Note: The organization is legally required to periodically verify compliance with this policy through random checks.

7. IT responsibilities

The following activities are exclusively performed by internal or external IT staff. Employees are not permitted to carry out these tasks:

1) Ensuring the availability of local IT systems, IT services, and data (if applicable)
2) Creating data backups of all company data
3) Continuous monitoring and maintenance of regular backup processes
4) Ensuring a suitable storage location for backups (protected from external influences such as fire, water, cold, and theft)
5) Maintenance and configuration of local servers and client systems, including update and patch management (if applicable)
6) Recording and inventory management of deployed client hardware (PCs, laptops, monitors, external storage media)
7) Providing 1st, 2nd, and 3rd level support
8) Reconciling deployed client operating systems with available client operating system licenses and reporting any under- or over-licensing
9) Administration and documentation of each user's access rights to network resources
10) Documentation of access permissions to the server room (if applicable)
11) Ensuring the installation of up-to-date antivirus software on client systems
12) Immediate remediation in the event of malware incidents (e.g., viruses, worms,

Trojans)

13) Ensuring the availability of all local systems (if applicable)
14) Administration and documentation of access rights for all server systems and network drives
15) Centralized license management

8. Violation

Compliance with this policy regarding the use of IT systems, IT services, and data is of critical importance. Failure to adhere to these guidelines may, under certain circumstances, result in severe disciplinary actions, up to and including termination of employment with or without prior warning.

9. Appendix

9.1. Related Documents and Policies

The currently valid versions of the Data Protection Policy and the AI Policy

9.2. Terms and definitions, abbreviations, technical questions

For questions regarding terms, definitions, abbreviations, and other technical issues, please contact your line manager or IT department.