EDV Werke
IT Beratung und Entwicklung

Information Security and Data Protection Policy

EDV Werke AG

Mühlegasse 18

6340 Baar, Switzerland

CHE-480.099.869

Contents

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Purpose of introducing and outline of the policy

This information security and data protection policy is a set of policies regulating information security issues within the organization in various areas. The purpose of the Policy is to ensure protection of data, systems and IT infrastructure against various threats, such as cyber-attack, data leakage, loss of information integrity or threats related to improper data management.

The main objectives of the information security policy include:

1. Protection of data confidentiality: Ensuring that only authorized persons have access to information, and the data are stored and processed in a way that protects their confidentiality.
2. Maintaining data integrity: Preventing unauthorized modification, deletion or destruction of data to maintain its accuracy and immutability.
3. Ensuring data availability: Guarantee that data is available to authorized users at the right time and place, regardless of possible disruptions or attacks.
4. IT infrastructure protection: Ensuring the security of computer systems, networks and devices to prevent attacks and protect the infrastructure from potential threats.
5. Compliance with regulations and standards: Adaptation of activities to applicable legal provisions and norms and standards regarding data protection and information security.
6. User awareness and education: Ensuring that employees are aware of information security risks and have appropriate knowledge and skills in data protection.
7. Incident response: Development of plans and procedures for responding to information security incidents, including rapid identification, analysis and elimination of threats and minimization of damage.
8. Continuous improvement: Constantly monitoring the IT environment, assessing risk, and making improvements and updates to adapt to changing threats and technologies.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Clean desk policy

Purpose of introduction and policy outline

The purpose of this document is to define general principles that will prevent unauthorized access to personal data in the workplace- in particular, unauthorized persons obtaining passwords or physical access to the computer, programs, applications or documents.

Requirements and recommendations

1. Employees are obliged to ensure that any documents or electronic media containing personal data or information that is confidential are not left in a publicly accessible place when:
    a. The employee has finished working at the workstation.
    b. The employee leaves his workstation.
2. Electronic equipment including, among others: laptops, computers should:
    a. Be positioned in such a way that the screen is invisible to persons who are not authorized to process it.
    b. Be locked (screen saver set) when the employee leaves the workstation.
    c. Be completely turned off at the end of the working day.
3. In particular, it is prohibited to save data such as identifiers, logins, passwords on pieces of paper that are hidden under the keyboard, phone flap, glued to the monitor or left in any other way.
4. Keys to cabinets and drawers containing paper documents or media with data, cannot be stored or left in a place where they may be found unauthorized persons to process data.
5. Printed or scanned documents should be removed from the device immediately.
6. Documents intended for destruction should be destroyed immediately in a shredder.

Policy implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Clean screen policy

Purpose of introduction and policy outline

The purpose of the document is to protect data confidentiality and minimize the risk of information leakage by controlling access to computer monitor screens and applying measures to prevent unauthorized access.

Requirements and recommendations

1. Protection against disclosure of information:
    a. Recommendation to place monitors in places that minimize the possibility of potential disclosure of confidential company information to third parties.
    b. Use appropriate blinds, curtains or sunshades to limit external access to monitors.
2. Work Ergonomics:
    a. Requirement to place monitors at an appropriate height and distance from employees' eyes to ensure information privacy and minimize the risk of reading by unauthorized persons.
3. Appropriate Lighting:
    a. Ensuring even lighting in the workplace to minimize eye strain and prevent potential reading of information by unauthorized persons.
    b. Avoiding lighting conditions that are too bright or too dark, which may make it easier or harder to read information on the screen.
4. Login and screen locking:
    a. Requiring employees to secure their computers by locking the screen or logging out of the operating system when they leave their workstation. This helps prevent unauthorized access to confidential data in case the employee is absent.

Policy implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Password policy for IT system users

Purpose of introduction and policy outline

The purpose of this policy is to introduce principles and unified standards specifying the conditions that should be met by passwords used by employees, as well as the management of information constituting the so-called secrets, i.e. access keys to websites, services or hardware configurations.

Recommendations related to user passwords

1. The IT system user password should consist of at least 12 characters, including at least 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character.
2. The organization uses Multi-factor authentication (MFA), which protects information media.
3. The password in its construction cannot consist of information that is predictable, incl:
    a. They cannot contain information relating to the employee, e.g. his personal data,
    b. They should not contain predictable and typical dictionary words.
4. Hasła użytkowników nie mogą być udostępniane dla innych pracowników i osób trzecich.

Managing application "secrets"

1. The Administrator is obliged to appropriately secure data other than user passwords, including:
    a. Application API keys that are used to communicate with internal or external applications.
    b. Access data to databases.
    c. Data used for cryptography.
    d. Access keys, which are the so-called secrets of an application or IT solution.
2. Access to access keys should be limited only to employees indicated by the administrator.
3. The IT Systems Administrator ensures that the President of the Management Board of the organization and persons designated with the authorization of the President of the Management Board can gain access to passwords, access keys and other secrets through an internally defined procedure.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Key policy and room access control

Purpose of introduction and policy outline

The purpose of this document is to introduce an access control mechanism to record the entries and exits of employees from the data administrator's premises. Applies to all employees and third parties located on the data controller's premises.

Requirements and recommendations

1. The President of the Management Board implements appropriate physical protection measures in the rooms where data are processed.
2. The President of the Management Board keeps records of issued means of access to the premises, including, among others:
    a. Keys to the rooms.
3. Termination of the contract with the employee is tantamount to the employee's obligation to return the means of access to the data controller's premises.
4. The administrator records the date of return of the transferred means of access to the administrator's premises.
5. The presence of unauthorized persons in the area of personal data processing is permitted with the consent of the data administrator or in the presence of a person authorized to process data.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Monitoring policy

Purpose of introduction and policy outline

The document specifies the rules related to the use of monitoring techniques, which include monitoring the ICT network and e-mail monitoring, as well as other databases or ICT programs used in the organization. Applies to all employees.

General rules for the use of monitoring techniques

1. Monitoring may only be used to ensure the safety of employees, protect property, maintain the continuity of processes or maintain the secrecy of information, the disclosure of which could expose the employer to harm.
2. Monitoring may not violate personal rights, which include, among others, dignity, confidentiality of correspondence and freedom.
3. Monitoring may be used in relation to:
   a. Employees,
   b. Subcontractors who use the data controller's infrastructure or equipment.
4. Monitoring may not violate the personal rights of third parties.
5. Information about the use of monitoring must be communicated no later than 2 weeks before the monitoring is started in a customary manner, or before the employee is allowed to work.
6. It is prohibited to use business e-mail for private purposes, including redirecting business messages to private electronic accounts, media or disk spaces.
7. The Internal IT department must be informed about the intention to introduce a new form of monitoring or a significant modification of the operation or monitoring infrastructure.
8. It is prohibited to use private hardware for business purposes, including but not limited to accessing, storing, or processing company data. Employees who have been provided with company equipment are strictly forbidden from logging into corporate accounts on private devices or external storage media.
9. The introduction of a new form of monitoring requires a risk analysis and risk assessment.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
3. This policy supersedes previous policies governing the area it addresses.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Policy for granting authorizations to process data

Purpose of introduction and policy outline

The purpose of this policy is to define the principles and criteria for granting authorizations to persons processing important data within the organization, including monitoring the granted processing authorizations.

Authorization to process data

Appropriate management of data processing rights is a key element of our organization in the context of ensuring data protection against unauthorized access and misuse. As part of our policy:

- Data access permissions are granted according to the roles and responsibilities of employees in the organization, as well as partners and suppliers.
- We provide specific internal authorization management procedures that include granting, modifying and removing access to data. These procedures are designed to effectively control access and prevent excessive access to data.
- Decisions regarding granting rights are documented adequately. These criteria take into account business needs and compliance with applicable regulations.
- We implement appropriate technical and organizational security measures to ensure confidentiality, integrity and availability of data. Our procedures ensure that data is processed in accordance with applicable regulations and only by authorized persons.

Policy Implementation

1. The application of this policy begins on the date of its adoption by the authorized body.
2. This policy supersedes previous policies and procedures governing the area it addresses.
3. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, contractors, trainees, interns).
4. The Data Processing Authorization Manual applies to this policy.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Remote work policy

Purpose of introduction and policy outline

The purpose of this document is to define basic principles that aim to raise awareness of working remotely.

Requirements and recommendations

1. All policies and procedures established for work in office premises also apply to remote work.
2. Employees are obliged to ensure that remote data processing takes place with full confidentiality of the processed data by, among others:
    a. Choosing a safe place that will prevent unauthorized persons from viewing device screens (e.g. working in public transport, hotels or other public places such as restaurants).
    b. Securing access to your business data and preventing unauthorized persons from viewing the data, including those living together with you, and against their unauthorized destruction or modification.
    c. Connecting to a secured home WiFi network. It is prohibited to use open WiFi networks, for example hotel WiFi, shopping malls or hot-spots in cafes.
    d. Regularly updating the operating system and activating the firewall.
3. In the event of loss or theft of equipment, documents or other information media, you should immediately report the incident to your direct superior, the Internal IT department and the Compliance department on the day of the event.

Policy Implementation

1. The application of this policy begins on the date of its adoption by senior management.
2. The provisions of this policy apply to all employees, as well as individuals performing work under arrangements other than an employment contract (e.g., B2B contractors, contractors, trainees, interns).
3. This policy supersedes previous policies and procedures governing the area it addresses.
4. The Remote Work Regulations apply to this policy for employees.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Risk analysis policy

Purpose of policy and outline

The purpose of this policy is to ensure compliance with applicable regulations and minimize the risk of security incidents and data breaches through appropriate risk management, risk analysis, and impact assessment.

Risk management

1. The IMS team is responsible for developing and implementing the risk management strategy within the organization.
2. Regular risk assessments related to ICT technologies are conducted, including the identification of critical functions, processes, and assets, as well as the analysis of potential threats and vulnerabilities.
3. As part of incident management, the IMS team is responsible for updating the Incident and Breach Management Policy to ensure effective response to events that require classification, reporting, and management.
4. Operational resilience tests and cybersecurity incident simulations are conducted to evaluate the effectiveness of security measures, identify security gaps, and assess the organization's preparedness for ICT-related incidents.
5. Development of business continuity and disaster recovery plans.
6. Personnel education to raise awareness of threats and responsibilities regarding organizational security.

Risk analysis

1. The IMS Team, with the support of the Data Protection Officer, conducts risk analyses related to personal data processing within their respective departments.
2. Risk assessments should include, among others:
   a. Information assets.
   b. Personal data processing processes.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

c. Service providers in relation to the delegation or potential delegation of personal data processing, where applicable.

d. Potential threats associated with ICT infrastructure and their impact on the operational resilience of the organization.

e. Threats related to access management to systems and data, compliance with legal and industry regulations, financial risk management.

3. Risk analyses or their reviews must be conducted at least once a year.
4. The Data Protection Officer, in collaboration with the IMS Team, verifies the conducted risk analyses and their substantive accuracy regarding personal data.

Data protection Impact assessment

1. The Data Protection Officer is directly responsible for conducting data protection impact assessments and liaising with the data protection authority only when such an obligation arises from regulations.
2. A data protection impact assessment is conducted once for a personal data processing process and also in cases of changes to processing processes or new projects involving personal data processing.
3. Initiated projects may require a data protection impact assessment, but an initial evaluation of whether this will be necessary must be conducted by the IMS Team with the support of the Data Protection Officer.

Policy Implementation

1. This policy takes effect on the date of its adoption by the authorized body.
2. This policy replaces the previous policy concerning the regulated area it addresses.
3. The provisions of this policy are directed at all employees, as well as individuals performing work based on agreements other than an employment contract (e.g., B2B contractors, freelancers, trainees, interns).
4. This policy is subject to the Risk Assessment Manual and the Business Continuity Plan (BCP).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Internal and external audit policy

Purpose of introduction and policy outline

The purpose of this policy is to establish procedures for conducting internal and external audits in connection with improving the data protection and information security system in the organization. Applies to the President of the Management Board, Team Leaders/Managers and designated internal auditors.

Requirements and recommendations

1. Data protection audits will be carried out at least once a year, covering all departments of the organization, unless clearly indicated departments of the organization do not require audits to be conducted with such frequency.
2. During the audit, reviews of data protection documentation and the information assets register or other registers in connection with data protection and information security management will be carried out.
3. Audits are carried out after their approval by the President of the Management Board.
4. The audit plan is established together with Team Leaders/Managers, usually within 1 week of the commencement of the audit, unless the President of the Management Board agrees to a shorter period.
5. In the event of a serious incident or breach of data protection or a suspected threat to the security of data processing, the President of the Management Board may order an ad hoc audit without applying for consent to conduct it.
6. The rights of external auditors are defined in contracts.

Policy implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Policy of using cryptographic mechanisms

Purpose of introduction and policy outline

The purpose of this document is to introduce requirements regarding the use of cryptographic mechanisms to prevent unauthorized access to data by third parties. Applies to the President of the Management Board, Internal IT department (IT Systems Administrator) and all employees.

Requirements and recommendations

The President of the Management Board must ensure appropriate measures to ensure that appropriate cryptographic mechanisms are used throughout the organization.

Cryptographic mechanisms should include, among others:

1. Network connections between IT systems and web applications.
2. Memory in stationary and mobile devices.
3. Memory in portable storage devices, such as USB sticks and portable drives.
4. Electronic correspondence whenever possible.
5. Passwords saved in IT system databases.
6. Connecting users to the data administrator's services (VPN networks).
7. The Internal IT department ensures that all applications using SSL / TLS protocols have certificates issued by a known and trusted provider.
8. The IMS team organizes an annual review of the application of this policy, which is carried out through the Internal IT department.
9. The Internal IT department introduces procedures for managing cryptographic keys.

Policy implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Backup Policy

Purpose of introduction and policy outline

The purpose of this policy is to create standards and indicate responsibility for the process related to making backup copies in the organization in connection with ensuring business continuity and guaranteeing the protection of the rights of data subjects.

Requirements and recommendations for electronic copies

Backups must be made at least once a week, unless a different backup frequency is specified in the information assets register..

Electronic backups must be made, especially for:

1. Relational and non-relational databases.
2. Programs that are necessary to read specific databases containing personal data.
3. System libraries and other IT system dependencies that are necessary to read specific databases containing personal data.

The President of the Management Board must ensure a procedure that will also enable data to be deleted from backup copies. The President of the Management Board should conduct regular tests of the backup restoration procedure in order to verify the correctness of their execution and the duration of the backup restoration process. The President of the Management Board should conduct regular tests of the infrastructure restoration procedure in the event of its complete failure.

Including provisions regarding making backup copies

Provisions in contracts related to data processing should include appropriate guarantees related to the handling of backup copies in order to protect processed personal data and ensure business continuity. Backup copies should be returned or deleted after the expiry of the contract in accordance with the contractual provisions, unless the parties agree on separate procedures in the course of terminating the contract in writing or electronically using a qualified electronic signature.

Policy Implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Authentication policy

Purpose of introduction and policy outline

The purpose of this document is to introduce requirements for IT systems so that the authentication process guarantees an appropriate level of security. Applies to all employees.

Requirements and recommendations

1. The President of the Management Board ensures, as far as possible, that multi-factor authentication is used for IT systems, including, among others:
    a. Authentication using ID and password.
    b. Authentication with the additional use of one-time tokens.
    c. Authentication with the additional use of one-time SMS codes.
    d. Authentication with additional use of hardware authentication mechanisms, e.g. YubiKey, SmartCard.
2. Whenever possible and justified, the Internal IT department introduces mechanisms that enforce the use of multi-factor authentication on users of IT systems.
3. Multi-factor authentication mechanisms should also apply to server infrastructure.
4. Access control systems should also be used for particularly protected rooms.

Policy Implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Policy for concluding contracts with customers and suppliers

Purpose of introduction and policy outline

The purpose of introducing the contractual policy is to ensure consistency and efficiency in the process of concluding data processing contracts between our organization and other entities. This policy aims to establish clear procedures and guidelines that will be used to negotiate, conclude, monitor and manage contracts within our organization. By properly managing information security risk, standardizing processes and raising employee awareness, we want to minimize potential risks while optimizing the process.

1. In the case of concluding or terminating a contract with a Customer or Service Provider where there are doubts in the area of personal data protection, the person responsible for concluding this contract should inform the Compliance Department in order for it to analyze the contract from the point of view of personal data protection and information security.
2. The Compliance Department, with substantive support, analyzes contracts for compliance with applicable data protection regulations.
3. After analysis, the document is sent back to the person who submitted it for verification.
4. All contracts concluded within the organization are concluded via the Auteni platform.

Policy Implementation

1. The application of this policy begins on the date it is adopted by Senior Management.
2. This policy replaces all previous policies and procedures concerning the regulated area.
3. The provisions of this policy are directed at all employees, as well as individuals performing work under agreements other than employment contracts (e.g., B2B contractors, freelancers, interns, trainees).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Incident and breach management policy

Purpose of policy and outline

The purpose of this policy is to establish principles and procedures for managing incidents and security breaches to: a. Ensure business continuity and the protection of data and systems in accordance with the NIS2 Directive (Network and Information Systems Directive 2); b. Minimize operational and cyber risks in compliance with the DORA (Digital Operational Resilience Act) requirements; c. Meet data protection requirements according to GDPR (General Data Protection Regulation). This policy also aims to ensure a prompt response to incidents, reduce their impact, and continually enhance the organization's security standards.

Scope of policy

The policy applies to all incidents related to: a. Information security, including personal data; b. Key services and the organization's critical infrastructure; c. Compliance with regulatory standards (NIS2, DORA, GDPR). The policy covers all employees, IT service providers, business partners, and entities processing data on behalf of the organization.

Key principles

1. Early Detection: Monitoring systems and business processes to identify potential threats.
2. Real-Time Response: Swift and coordinated actions to minimize the impact of incidents.
3. Compliance: Incident reporting in line with DORA, NIS2, and GDPR requirements.
4. Personal Data Security: Safeguarding personal data in compliance with Articles 33 and 34 of GDPR.

Incident reporting

1. In the event of a security incident or data protection breach, you should immediately inform the Compliance Officer by sending a report to privacy@edvwerke.ch.
2. Each event is verified and appropriately classified as a security incident or security breach with the participation of a Compliance Specialist or IT Systems Administrator.
3. In a situation where the breach may threaten the rights and freedoms of the person whose data was breached on behalf of the Company, the Compliance Department is obliged to notify this fact to this person via privacy@edvwerke.ch or in writing (traditional letter).

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Policy implementation

1. This policy takes effect upon adoption by senior management.
2. This policy supersedes any previous policies governing the regulated area it addresses.
3. The provisions of this policy apply to all employees, as well as individuals performing work based on agreements other than an employment contract (e.g., B2B contractors, contractors, trainees, interns).
4. This policy is subject to the Business Continuity Plan (BCP), GDPR Incident and Breach Management Manual, NIS2 Incident Management Manual, and DORA Incident Management Manual.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Data retention policy

Purpose of introduction and policy outline

The purpose of this policy is to define the deadlines for deleting data from information media. The data retention policy applies to all employees processing data and to all information media containing data, in particular:

a. personal data in programs, applications and systems,
b. paper documentation,
c. e-mail messages,
d. recordings,
e. data in control and access systems.

Requirements and recommendations

Personal data should be deleted within the deadlines indicated in the table below, unless they are necessary:

a. to fulfill a legal obligation requiring processing under EU law or the law of a Member State to which the Administrator is subject,
b. for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes insofar as deletion of the data is likely to render impossible or seriously impair the achievement of the purposes of such processing,
c. to establish, pursue or defend claims.

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch

Related documents

Registers

- Incident register
- Register of programs and databases used to process personal data (GLPI System)
- Information Assets Register (GLPI System)
- Register of authorizations to process data of internal employees (HR Administration)
- Register of authorizations for the Partner
- Risk analysis (IMS team)

Other

- Data breach reporting form

List of changes

Document author	Document version	Date updated	Valid from	Notes
Klaudia Kacała	1	26.09.2024	26.09.2024	Development of the document.
Klaudia Kacała Aleksandra Siemaszko Szymon Słupczyński	2	14.02.2025	14.02.2025	Change of annexes from procedures to manuals. Update the document Policy for conducting risk analysis and impact assessment - alignment under NIS2 and DORA. Introduction of NIS2 incident and breach management manual and DORA incident and breach management manual Introduction of the Business Continuity Plan (BCP) as an appendix. Standardise terminology, add table of changes. Adding a provision to the Monitoring Policy - General rules for the use of monotoring item. 7 *"It is prohibited to use private hardware for business purposes, including but not limited to accessing, storing, or processing company data. Employees who have been provided with company equipment are strictly forbidden from logging into corporate accounts on private devices or external storage media."*

14.02.2025..... DocuSigned by: Jakub Wojewski FE2C961927354D1.....

Chairman of the Board – ***Jakub Wojewski***

EDV Werke AG, Mühlegasse 18, 6340 Baar, Schweiz
UID/MWST. CHE-480.099.869 | Handelsregister-Nr.: CH-170.3.043.605-7
www.edvwerke.ch | info@edvwerke.ch