Technical and Organisational Measures

top itservices AG

This data protection concept explains the technical and organisational implementation of data protection measures in companies.

It has been compiled as an information service for interested persons.

25.04.2018
Vers. 1.2

Inhaltsverzeichnis

Technical and Organisational Measures

The following contains a description of the technical and organisational measures that have been taken to ensure data protection and data security. The objective is to especially ensure the confidentiality, integrity and availability of the data and information being processed by the company. The measures comply with the internationally recognised DIN ISO/IEC 27002 standard.

1 Policy

The data protection policy of top itservices AG contains the board's mission statement concerning the handling of personal data by the company. All staff, freelance collaborators and subcontractors are obliged to abide by these basic principles.

The IT security level achieved by the organisational units and the procedures and systems will be monitored through periodic audits and continuous controls.

Daily operations will be monitored in cooperation with the security officer.

The security policy will be reviewed at least once a year insofar as an essential change does not necessitate an earlier review. This will help to ensure the ongoing appropriateness, suitability and efficiency of the regulation.

The security officer is the person in charge of the security policy. He is responsible for developing, reviewing and checking the policy.

2 Organising the information security

Senior staff at top itservices AG is responsible for the complete implementation of the principles of IT security and for fulfilling the assigned IT security tasks in their organisational unit.

Information security roles and responsibilities are defined in the IT security organisation. Conflicting and incompatible tasks and responsibilities have been separated to reduce the possibility of unauthorised or unintentional changes or a misuse of the values (e.g. operating supplies, removable media, notebooks) of our company.

We possess a procedure which establishes when and by whom relevant authorities shall be notified and recognised data protection and information security incidents reported in time.

We are also in regular contact with special interest groups allowing us to remain informed about changes and improvements in the field of data protection and information security.

In projects for which we are responsible data protection and data security is an element during all stages of our project plan.

With the help of our respective guidelines and procedures for using mobile devices, we also ensure that data is protected and secure in these areas.

3 Staff security

Our staff have been carefully selected and scrutinised for their suitability for their positions in our company. We have codified their responsibilities in job descriptions, and we regularly review this compliance with our staff. Before beginning their job all employees sign a confidentiality and data protection agreement which applies beyond the termination of their employment relationship. Our staff are

trained in the fields of data protection and data security, whereby knowledge in this field is brushed up when staff change their function. Our staff are therefore aware of their responsibility in this regard.

In a documented process for the time before, during and after the termination of an employment relationship, we ensure that personal data are protected and data security is ensured. This also includes disciplinary measures in the event of a breach of data protection rules.

4 Administrating the values

We inventory and maintain all values (such as operating supplies, removable media, notebooks) and information carriers that are associated with personal data.

We have appointed persons responsible for protecting these values who are responsible for the life cycle of a value.

Documented rules have been established for a permissible use of these values. Their return is documented.

Our information and data are classified and designated as required by law and their value, their criticality and their sensitivity protected against unauthorised disclosure or alterations.

Corresponding with this classification scheme we have developed and implemented documented procedures for handling our values, in particular also for dealing with our removable media. We possess a documented and regulated procedure for transporting data carriers to protect them from unauthorised access, misuse or falsification.

We safely dispose of data carriers which are no longer needed while using a documented procedure and committed and certified service providers.

5 Access control

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Den Zugang zu Netzwerken und Netzwerkdiensten haben wir geregelt und umgesetzt.

Es ist sichergestellt, dass nur befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird, insbesondere besteht ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern, der die Zuordnung von Zugangsrechten ermöglicht.
Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert.
Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern.
Ist- und Soll-Zustand von Benutzerzugangsrechten werden regelmäßig abgeglichen. Bei Bedarf werden diese entzogen oder angepasst.

Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter.
Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.

6 Cryptography

An adequate and effective use of cryptography ensures the securing of confidentiality, authenticity and integrity of information. This is why we have implemented a regulation concerning the use of cryptographic measures by the company which also includes the administration of cryptographic keys and which meets security requirements.

7 Physical and environmental security

We have taken documented and regulated measures designed to prevent unauthorised persons from accessing the equipment used to process data and use personal data. These measures include but are not limited to the following factors:

- The business premises are situated in different office buildings which are used exclusively.
- The entrances are controlled.
- The doors to security areas are always kept closed. Security is ensured through a token/security key system.
- Visitors and external service providers are admitted individually with name and contact person being documented.
- Fire protection regulations are observed.
- Security zones with access restricted to authorised personnel exist.
- IT rooms are closed separately and can only be opened by authorised staff.
- Utility installations are protected against power failures and disturbances.
- The safety of the cable system is ensured.
- Systems are maintained according to a plan which is put into practice.
- Changes to systems and information and their removal are carried out systematically.
- The security of systems outside of the business premises is accounted for.
- Resources are disposed of or reused according to plan.
- User equipment is secured through a coded system.
- Clean Desk and screen lock guidelines are followed.

8 Operating security

We possess regulated and documented measures to ensure a proper and secure operation of information and data processing equipment. These include control measures for changes to the information processing equipment as well as a control and regular measurement of our capacities and resources to ensure the availability of the required system performance. For example, in this manner the following values among other things are being currently monitored on a regular basis:

- Hard drive status and available memory
- Raid status
- Services and status of all virtual equipment
- Storage occupancy of the storages and central memory

- Use of ether net in Kbit/s and Mbit/s
- Number of RDP sessions of the individual terminal servers
- Throughput and use of the Firewall
- Availability of all servers through VPN
- Availability and throughput of the switches
- Availability of the mail services (internal and external)

We have implemented and documented a protected procedure for data security.

Standard maintenance windows have been defined. Additionally required windows will be announced at least three days in advance.

It is essential that development, test and operating environments are kept separate at our company allowing us to focus on the maintenance of this separation.

To protect against malicious software, recognition, prevention and recovery measures have been taken and are being updated regularly.

We possess a centrally monitored and secured event logging system, and for storing sensitive personal data we have adopted measures to protect the private sphere. All recording facilities and protocol information, including administrators and operator protocols, are protected against manipulation and unauthorised access.

Our clocks are synchronised centrally using a single referential time source.

We use a centralised procedure to control the installation of software on systems at our company.

We possess centrally implemented regulations for limiting software installations.

For audits to our information systems we have established measures designed to keep the disturbances of our business processes at a minimum.

9 Communication security

The security of the personal data and information stored on our networks and network services is absolutely essential. That is why we are using documented measures which administrate, control and secure our networks.

On a needs basis information services, users and information systems are being kept as far as possibly separate from each other.

We possess regulations and procedures for transmitting information and data and transferring agreements regulating the transmission of information to outside authorities.
Our electronic communication is adequately secured. We have implemented measures for securing our communication including securing it from unauthorised access, from changes or from a denial-of-service attack which correspond with the classification scheme taken over from the organisation.

To protect our data, we enter into confidentiality or secrecy agreements that meet our needs and which we review on a regular basis.

10 Acquisition, development and maintenance of systems

We have ensured that data and information security remains an integral part of our systems throughout their whole lifecycle. This also includes the demands place on and the securing of information systems which provide services through public networks. Transactions with application services are secured on a needs basis. We have also established a method for administrating system changes to ensure the integrity of the system and its application as well as of the products from the early design stages through to the subsequent maintenance work. With changes to operating platforms, applications critical to business are checked and tested to ensure that there are no negative effects on the organisational security. We possess a controlled method for analysing, developing and maintaining secure IT systems.

11 Supplier relations

We carefully select our suppliers during the preliminary stages and check their suitability with regard to the safeguarding of data and information security.

Documented arrangements (agreements for commissioned data processing) secure the protection and secrecy of our values and data. Suppliers are being committed to implement technical and organisational measures to ensure their conformity with these arrangements.

A regulated and user-defined access authorisation procedure exists for values and data that the respective suppliers stringently require.

To ensure a secure supply chain, suppliers may only commission sub-suppliers with our approval.

We regularly check the data protection and data security measures of our suppliers in order to maintain the arranged protection level. The assigned authorities are also subject to a continuous documented control.

After terminating the supplier relationship, these suppliers are obliged to return all data and values to us or to destroy them properly. In addition, the duty to observe the secrecy obligation remains indefinitely.

12 Handling information security and data protection incidents

Our company possesses a regulated documented process for handling information security and data protection incidents in order to ensure a consistent and effective strategy in this regard. Staff are called upon to immediately report any data protection and security incidents, and they are also being trained regularly in this aspect.
All incidents are documented, classified and evaluated. A special intervention team has specific instructions on how to deal with such an event.
Together with the board improvement measures resulting from the knowledge gained and the collected evidence relating to an event are regularly discussed and implemented.

13 Information security aspects with Business Continuity Management

The availability of a system allowed within the limits of information security is specifically assessed and documented. We derive the technical and organisational specifications such as redundant systems and

connections or feasible plans from the requirements and implement them accordingly. A comprehensive contingency plan provides the framework for the corresponding instructions for selected documented emergency scenarios. Continually updated training plans for the implemented measures and the documentation of the application of corresponding tests round off the contingency management process. All server and storage systems are equipped with a manufacturer's warranty of at least 36 months, usually however 60 months.

14 Compliance

We have documented all relevant statutory, regulatory, self-imposed and contractual requirements as well as the procedures of our company for complying with these requirements, and these are kept up to date by us.

We have also implemented appropriate procedures with which the compliance with the statutory, regulatory and contractual requirements concerning intellectual property rights and the use of software products protected by copyright is ensured.

Our recordings and personal data are secured on a needs basis according to the statutory, regulatory, contractual and business requirements. Yearly activity reports from the data protection official document the measures that have been taken.

For this purpose we comply with the regulations of cryptographic measures.

To ensure the protection of our information and data a regular independent review of our information security and data protection level, our security and data protection regulations as well as the adherence to technical specifications is carried out.