Technical and organizational measures

The following sets out the technical and organizational measures the Processor is obliged to establish and maintain on an ongoing basis to ensure data protection and data security in compliance with all relevant provisions on data protection. The technical and organizational measures concern the products evasys, evasys and qurricula.

If a software product is hosted by evasys GmbH, measures are in place that are also set out in this document.

Relevant information:

- Support: The Processor performs live support via TeamViewer after receiving an order from the Controller (support request). TeamViewer is used in the support process for the products evasys and evaexam.
- For the product qurricula support is handled using the project management tool Jira.
- Evasys GmbH operates the cloud concept “IaaS” (Infrastructure as a Service).

1. Ensuring confidentiality

1.1. Access control

1.1.1. Controller

All actions taken by the Processor in support can be monitored by the Controller. The actions of the Processor can be tracked in real time on a monitoring screen. In support any necessary passwords are entered by the Controller, who tracks the work on the monitoring screen.

The Controller uses the appropriate infrastructure (hardware/software) and correspondingly secure configuration and assignment of rights, to ensure that when gaining access for support only the computers, network areas and resources mandatory for support can be accessed.

1.1.2. Processor

The computers used for support activities are owned by the Processor and are authorized for purely official use only. Only software for business use is installed.

The operating system on the computers used for support and hosting administration has user management, so access possibilities are limited by means of a role and rights concept and are prevented without valid authentication.

The access possibilities can be differentiated according to data, programs, and type of access.

The rights management of the data storage device is graduated at the levels of the drives, directories, sub-directories, files, and approvals. Rights are assigned restrictively.

The operating system is technologically state of the art. Available security updates for the operating system and the installed security-related software are performed regularly. A check for the availability of security updates and their immediate installation is carried out on a daily basis.

The computers have an up-to-date security software (antivirus software). As soon as the signature updates for the antivirus software are available, they are installed immediately after the client becomes aware of them. The checking activity is documented by the Processor's internal IT support.

The data storage devices are checked regularly (complete scan at least once a week, but permanently in real time via real-time scan) for harmful software using the security software. If an infection is detected, the respective device is only put back into operation when it has been established beyond doubt that the malware has been completely removed. If necessary, the system is reinstalled.

If the device has already been used with the Controller for support or hosting administration before the discovery of malicious software, the Controller will be informed of the incident immediately.

The system is automatically locked if there is inactivity for more than 5 minutes and can only be unlocked by entering the valid password.

All activities for support or hosting administration are carried out exclusively from equipment provided and permanently managed by the Processor.

If it is necessary for the Processor to store personal data gathered during the support process after the support ends, to process the support case, these data will be stored on a separate, dedicated drive. This drive has restrictive access limitations, all writing and deletion procedures are logged.

The data are logged and deleted in accordance with data protection laws immediately after the purpose ceases to exist. For verification purposes, the deletion can be extended to a maximum of 8 weeks after the end of the support case.

Regularly (monthly) a check is made by the head of department to establish whether all data have been deleted in accordance with the rules (at the latest 8 weeks after the end of the support case).

The responsibility for the deletion process lies with the head of support department or their representative. The deletion process itself is performed by a trained employee or carried out automatically.

If data is transferred for support purposes, the transfer pathway is encrypted end-to-end, using the latest technology.

After termination of the support contract, all data of the Controller will be deleted. The data is deleted immediately after the purpose ceases to exist in accordance with the data protection protocol.

Should it be necessary to import data onto a system to recreate and analyse error situations or to carry out a (re)migration, the respective computer is made available exclusively for the duration of this task. After completion of the task, the data can be held for a maximum of 2 weeks. After that,

the data is deleted in accordance with data protection regulations. The deletion is logged in the log kept for this service.

Hosting:

To provide the service, only te network ports required for operation (80, 443, in some cases also 3306, if required) are enabled via VNet configurations within Azure at the network level. In addition, further infrastructure-related network ports are added (e.g. for monitoring purposes or our automation solution).

The connections are secured by a firewall. Administrative access is restricted based on IP filtering, specifically:

IP blocking on network level (TCP), access is only possible from within the evasys network.

Access control via the remote desktop software used (each type of access is logged by nam per user abbreviation).

Server passwords and the password for the administration interface are only known to the Processor and comply with the password policy (please see Password Policy).

The server operating system is technologically state of the art. Available security updates for the operating system and the installed security-related software are performed regularly.

Hosting is provided via Microsoft Azure on a Windows operating system. Microsoft releases update packages on the second Tuesday of each month (Microsoft's "Patch Tuesday").

The update is applied to the evasys production servers on the Saturday after the second Tuesday of each month.

The server systems have an up-to-date security software (antivirus software).

As soon as the signature updates for the antivirus software are available, they are installed immediately after the server becomes aware of them.

The server data storage devices are checked regularly (complete scan at least once a week, but permanently in real time via real-time scan) for harmful software using the security software.

If an infection is detected, the respective device will not be put back into operation until is has been established beyond doubt that the malware has been completely removed. If necessary, the system is reinstalled.

1.2. Access control

1.2.1. Controller

The connection for support is designed so that it can be disconnected by the Controller at any time.

After concluding the support, the Controller ensures that the connection is disconnected.

1.2.2. Processor

The workstations used for support or hosting administration are in an office room that is not accessible by the public. During longer absences, for example for appointments or after work, access is locked. The allocation of keys is subject to clear rules, so that the group of authorized individuals is clearly and unambiguously defined at all times.

If support or hosting administration takes place outside the Processor's office, the company-wide policy applies. Additionally, in the case of support, explicit consent from the Controller is required.

Explanation:

- Documented key allocation to employees.
- Continuous entry checks during business hours.
- Alarm system with alerting of a security firm outside business hours.
- Guests are accompanied and wear identification.

Hosting servers:

Hosting servers are in separate data centres with appropriate security provisions and regulations. For hosting services, evasys GmbH only commissions providers that have ISO 27001 certification. The corresponding proof of certificates will be provided to the Controller for review upon request.

Explanation:

- Electronic access control system with logging.
- High-security fence around the entire data centre.
- Documented key allocation to employees.
- Guests are accompanied and wear identification.
- Data centre manned by staff 24/7.
- Video monitoring of entrances and exits, security checkpoints and server rooms.

1.3. Pseudonymization

1.3.1. Controller

If it is necessary for the processing of a support case to store personal data with the Processor, the Controller must check before each transfer to the Processor whether pseudonymized or anonymized real data or test data can also be used under certain circumstances. This can be done in consultation with the Processor.

In the case of pseudonymization, care must be taken to ensure that the data are transformed in such a way that the Processor cannot identify the individual, even by combining the individual characteristics and incorporating additional sources. Additional sources in this context are publicly accessible sources, in particular data that are published, for example, on the Controller's website or in other publicly accessible databases.

1.3.2. Processor

If the transfer of personal data from the Controller to the Processor is mandatory for the completion of the task – either as an exception or as a rule – points 2.2.1 (measures for transmission control) and 2.3.2 (input control measures) must be fulfilled.

1.4. Encryption

1.4.1. Processor

Mobile computers or devices

If used for support or hosting administration, the data storage devices in the mobile computers are completely encrypted using recognised, strong, cryptographic algorithms, procedures and software and secured with a password (please see Password Policy and the minimum requirements in point 2.2).

Hosting servers:

Encryption at Rest comes into play when storing data on server systems.

1.5. Data storage device control

1.5.1. Processor

Defective or discarded hard drives are overwritten (erased) multiple times usind a defined procedure. The deletion process is logged. The procedure is based on the current technological state of the art.

The hard drives are then destroyed by a certified service provider.

Hosting servers:

After contract termination, hard drives are overwritten (erased) multiple times using a defined procedure. The process is based on the current technological state of the art. The hard drives are reused after inspection. The hosting service provider follows the NIST 800-88 guidelines (erase, delete, and destroy) and keeps records of destruction.

2. Ensuring integrity

2.1. Transfer control

The Controller and the Processor ensure by means of strong encryption (please see 2.2) that no personal data is transferred to external third parties during support or hosting administration.

2.2. Encryption

The connection with the Controller's systems set up for the purpose of the support (online connection), has cryptographically strong encryption.

Currently this means at least
- AES with at least 256-bit encryption length as a block cipher,
- SHA2 as a hash algorithm,
- RSA with a key at least 4096 bits long, and
- TLS in a version currently recognised as secure, as a log or recognised secure equivalent.

The encryption of personal data on mobile data storage devices, in containers (e.g., encrypted files, archives, e-mail, etc.) or the encryption of data storage devices in mobile computers meets at least the following current requirements:

Currently this means at least:
- AES with at least 256-bit encryption length as a block cipher,
- SHA2 as a hash algorithm RSA with a minimum 4096-bit key, and
- TLS in the version currently recognized as secure as the protocol or a recognized equivalent secure protocol.

2.2.1. Controller

The Controller provides suitable access which is sufficiently strongly encrypted and ensures both the authenticity of the communication partner and the integrity of the connection data (for minimum requirements please see 2.2).

This applies to both online connections and the transport of personal data using mobile data storage devices or containers.

For evasys and evaexam applies:

Support is realised as follows:

There is a local firewall on the Controller's personal computer, which activates the static IP addresses of the Processor for port 443 and for the UDP log as needed.

If transport of personal data to the Processor is necessary outside the online connection:

The personal data are strongly encrypted by the Controller before they are sent to the Processor (for the minimum requirements please see 2.2).

When sending data using a data storage device or container, the password complies with the password policy for encrypted data storage devices (please see Password Policy) and is sent to the Processor by a different route than the encrypted data.

Explanation:

If it is necessary to transfer files containing personal data to the Processor during a support case, this transfer is either carried out via Online Support System (OSS) or encrypted with FTP over TLS (key length 4096 bit, SHA256RSA) to the Processor's server specifically intended for this purpose. Filed uploaded to this server are deleted fully automatically after 48 hours in compliance with data protection regulations.

For qurricula applies:

Support requests are submitted in a ticket system by the Controller: (Explanation):

- The Controller is given access to the ticket system when the contract is signed,
- Access is secured according to the above framework,
- The Controller places support requests,
- If it is necessary to transfer files containing personal data to the Processor during a support case, this transfer is either carried out via Online Support System (OSS) or encrypted with FTP over TLS (key length 4096 bit, SHA256RSA) to the Processor's server specifically intended for this purpose. Filed uploaded to this server are deleted fully automatically after 48 hours in compliance with data protection regulations.
- The Controller has control of transfer, provision and deletion in the ticket system at all times.

The access to the systems to be maintained is limited by the Controller to the static IP address by technical measures, e.g. at the firewall.

2.2.2. Processor

If the activity for support is not carried out directly from the company network of the Processor, a VPN connection, or an equivalently secure connection to the company network of the Processor must first be established.

Provided that the technical requirements are in place at the Controller, the connection for support is strongly encrypted from point to point (for minimum requirements please see 2.2), so that between the computer of the Processor on which the support takes place and the endpoint at the Controller, there is no component that can view or manipulate the data stream in plain text.

For evasys and evaexam applies:

The individuals performing support shall be named to the Controller upon the Controller's request.

If support or hosting administration takes place outside the Processor's office, the company-wide policy applies. In addition, in the case of support, the Controller's explicit consent is required.

For qurricula applies:

The support takes place via static IP addresses.

The encryption of personal data on mobile data storage devices, in containers (e.g., encrypted files, archives, e-mail, etc.) or the encryption of data storage devices in mobile computers meets at least the following current requirements:

- AES with at least 256-bit encryption length as a block cipher,
- SHA2 as a hash algorithm RSA with a minimum 4096-bit key,
- RSA with a key length of at least 4096 bits,
- A password according to the encrypted media policy or an RSA key pair with at least 4096 bits. The private key is secured with a password according to the password policy for encrypted media (please see Password Policy).

The individuals performing support shall be named to the Controller upon the Controller's request.

If support or hosting administration takes place outside the Processor's office, the company-wide policy applies. In addition, in the case of support, the Controller's explicit consent is required.

Live support for evasys and evaexam is provided via a direct connection as follows:

If the TeamViewer software is used by the Controller, "peer to peer" accesses can be made without using the IP addresses of the provider of the TeamViewer remote maintenance software. For this purpose, the Controller transmits the static IP address of the computer via which a connection is to be established to the Processor (support). Connections are only established in the "LAN mode" of TeamViewer.

If it is necessary to provide files for download or similar in the context of a support case, these files will be made available end-to-end in encrypted form via the running TeamViewer connection.

Access to the systems to be maintained is restricted by the Controller to the above IP addresses by technical measures, e.g., at the firewall.

Hosting:

All communication is secured via https (TLS 1.2). Maintenance of the virtual machines is also performed via TLS-secured RDP connection. Basically, all communication is secured by current transportation encryption methods.

2.3. Input control

2.3.1. Controller

Support:

The Controller has only opened the programmes that are mandatory to resolve the problem. He tracks the work of the Processor on a monitoring screen and will cut off the connection if necessary.

The access of the Processor to the system of the Controller only takes place after personal occasion-related consent of the Controller.

As a matter of principle, access to personal data is strictly prevented by the Controller unless it is necessary for the fulfilment of the task.

2.3.2. Processor

Computers that have a network connection that has direct access to a public network (internet, company network, or similar.), i.e., are operated without an upstream firewall, have their own firewall. This is mandatory for mobile computers.

The firewall, upstream or on the computer itself, is configured so that only what is explicitly allowed is enabled, and that only connections initiated by the computer itself are allowed.

As a matter of principle, no personal data of the Controller is stored on the computer of the Processor for live support or hosting administration. Should this be mandatory for the fulfilment of the task, the following conditions are met:

- After the end of the support or the hosting administration, all personal data that was processed and stored as part of the activity will be deleted immediately in accordance with data protection laws or handed over to the Controller in accordance with data protection laws.
- If printouts have been made, these will be destroyed immediately after the end of the activity in accordance with data protection regulations. Furthermore, the Processor shall exclude, at least by official instructions, that copies of the printouts have been made or stored on other systems (print server, multifunction device, etc.). If this should nevertheless be the case, these copies will also be destroyed immediately or handed over to the Controller in accordance with data protection regulations.

If the storage of personal data by the Processor is required beyond the online connection:

In the context of support, it may be imperative that personal data must be stored with the Processor beyond the period of the online connection.

This data is stored in a strongly cryptographically secured container (for minimum requirements please see 2.2) or equivalent. The data is deleted immediately in accordance with data protection requirements or handed over to the Controller in accordance with data protection requirements as soon as it is no longer required for processing. The Controller must be notified of the duration of storage and deletion.

The operating system installed on the computers used for support enforces user authentication with username and password (please see Password Policy).

For the support activity, the time, the order, and the individuals involved are documented by the Processor in a conclusive and traceable manner.

Hosting:

The data is entered or recorded by the Controller himself.

3. Ensuring availability, reliability, and resilience

3.1. Login data

Processor

Certificates, SSH keys or similar access data for systems of the Controller are used by the Processor for support activities on the Controller's system. These are stored separately in a secure manner. A strongly encrypted container (for the minimum requirements please see 2.2 and the Password Policy) or an equivalent security measure is used.

The Processor shall ensure through internal regulations that access to the login data is also possible by a named representative in the event of a substitution during absence.

It is at any time technically and/or organizationally traceable on which media the login data for hosting systems are stored, how they are secured and by whom they are used.

3.2. Availability, reliability, and resilience

3.2.1. Hosting servers:

The Processor ensures high availability of the hosting server and the installed software through regulations, as well as fast recoverability in the event of an error.

3.2.2. Backup and recovery concept:

As specified in the hosting contract, the user data is backed up daily for 30 days using Azure Backup. A restore is possible at any time, also e.g. to a temporary additional system. Integrity tests are performed by Azure itself.

Restored data can be made available within 8 hours of evasys GmbH's business hours.

Explanation:

- Backup and recovery concept with daily backup of all relevant data (see above).
- Monitoring of the hosting server.
- Appropriate use of protection programs (virus scanner, firewall).
- Use of hard disk mirroring.
- Use of uninterruptable power supply, emergency standby system.
- Permanently active DDoS protection.
- Defined escalation chain in the event of an error for the fastest possible recovery of a system.

4. Regular monitoring, assessment, and evaluation of the TOMs

4.1. Controller

The Controller shall regularly check whether the technical and organizational measures to be taken by him are implemented and complied with.

4.2. Processor

The Processor shall regularly check independently whether the technical and organizational measures to be taken by him are implemented and complied with.

The Processor ensures that the individuals authorized to process the Controller's personal data are bound by confidentiality and discretion and are prohibited from processing personal data without authorization (data secrecy). Irrespective of any legal obligation, he informs them regularly about data secrecy and data protection instructions.

The Processor's employees are regularly required to comply with the relevant data protection and information security requirements in the home office in accordance with the technological state of the art.

The Processor makes arrangements for the deletion or destruction of personal data stored or printed in the context of support activities.

Explanation:
All sensitive data generated during the support process is stored on a separate dedicated drive. This drive has restrictive access limitations, and all writing and deletion procedures are logged.

A check is made regularly (monthly) to ensure that all data has been deleted in accordance with the rules (no later than 8 weeks after the end of the support case).

Annex 1:

Tabular presentation of the technical and organizational measures of evasys GmbH
Confidentiality (Article 32 para. 1 lit. b) GDPR)

Access control:

No unauthorized access to data processing systems

Type of Measure	Measure	Measure available at evasys GmbH
Technical	Alarm system	x
Technical	Bell system with camera	x
Technical	Light barriers / motion detectors	x
Technical	Manual locking system	x
Organizational	Personal control at the gatekeeper / reception	x
Organizational	Logging of visitors / visitor book	x
Organizational	Regulation for key	x
Technical	Security locks	x
Organizational	Obligation to wear employee or visitor badges	x (visitors)
Technical	Video surveillance of the entrances	x

Access control:

No unauthorized system use

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Careful selection of the IT service provider	x
Technical	Authentication with user password	x
Organizational	Management of user permissions	x
Organizational	Defined password rules	x
Technical	Use of automatic screen savers, spam filters	x
Technical	Use of antivirus software	x
Technical	Firewall deployment	x
Technical	Use of mobile device management	x
Technical	Use of VPN technology	x
Organizational	Creation of user profiles	x
Organizational	Annual review of authorizations	x
Organizational	Careful selection of the remote maintainer	x
Organizational	Careful selection of cleaning personnel (confidentiality obligation)	x
Organizational	Careful selection of security personnel (confidentiality agreement)	x
Technical	Two-factor authentication	x

Access control:

No unauthorized reading, copying, modification or removal within the system

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Reduce the number of administrators to the "bare minimum".	x
Technical	Use of document shredders (see BSI requirements)	x
Organizational	Use of service providers for file and data destruction (with certificate if possible)	x (DIN EN ISO/IEC 27001:2017)
Organizational	Creation of an authorization concept	x
Technical	Minimization of authorizations according to necessity	x
Technical	Proper destruction of data carriers (DIN 66399)	x
Organizational	Password policy incl. length and change	x
Technical	Physical deletion of data carriers before their reuse	x
Technical	Logging the destruction of data	x
Technical	Logging of accesses to applications, especially when entering, changing and deleting data	x
Organizational	Safe storage of data carriers	x
Technical	Encryption of data carriers	x
Technical	Encryption of smartphones	x
Organizational	Management of user rights by system administrators	x
Organizational	Four-eyes principle	x

Data segretation control:

Separate processing of data collected for different purposes

Type of Measure	Measure	Measure available at evasys GmbH
Technical	Anonymization of data sets	x
Technical	For pseudonymized data: Separation of the attribution file and storage on a separate, secured IT system.	x
Organizational	Definition of database rights	x
Organizational	Logical client separation (on the software side)	x
Technical	Separation of productive and test system	x

Pseudonymization:

(Articles 32 para. 1 lit. a GDPR und 25 para. 1 GDPR)

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Instructions / regulations for alienation of data sets as early as possible	x
Organizational	Creation of alienation concepts	x
Organizational	Definition of alienation rules	x
Technical	Alienation of identifiable features by proprietary or third-party software	x

Integrity (Article 32 para. 1 lit. b GDPR) Transfer control:

No unauthorized reading, copying, modification or removal during electronic transmission or transport

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Documentation of the recipients of data and the time spans of the planned transfer or agreed deletion periods	x
Technical	VPN tunnel setup	x
Technical	Email encryption	
Technical	End-to-end encryption	x
Technical	Content encryption	x
Organizational	Careful selection of transport companies	x
Organizational	Disclosure of data in anonymized or pseudonymized form	x

Input control:

Determining whether and by whom personal data have been entered into, modified or removed from data processing systems, e.g.: Logging, document management;

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Traceability of data entry, modification and deletion through individual usernames (not user groups)	x
Technical	Logging of the input, modification and deletion of data	x

Availability and resilience (Article 32 para. 1 lit. b) GDPR)

Availability control and rapid recoverability (Article 32 (1) (c) GDPR)

Protection against accidental or deliberate destruction or loss and precautions to restore the data as quickly as possible

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Alarm message in case of unauthorized access to server rooms	x
Organizational	Keeping data backup in a secure, off-site location	x
Technical	Duplicated IT infrastructure (redundancy)	x
Technical	Established Business Continuity Management (BSI)	x
Organizational	Creation of a backup & recovery concept	x
Organizational	Creation of an emergency plan	x
Organizational	Establishment of reporting channels	x
Technical	Fire and smoke detection systems	x
Technical	Fire extinguishing devices in server rooms	x
Technical	Devices for monitoring temperature and humidity in server rooms	x
Technical	Air conditioning in server rooms	x
Technical	Regular stress tests	x
Organizational	Regular implementation of crisis/emergency trainings	x
Technical	Protective power strips in server rooms	x
Organizational	Server rooms not with water-carrying pipes	x
Organizational	Data recovery testing	x
Technical	Uninterruptible power supply (UPS)	x

Procedures for regular review, assessment and evaluation (Article 32 para. 1 lit. d) GDPR; Article 25 para. 1 GDPR)

Data protection management

Type of Measure	Measure	Measure available at evasys GmbH
Technical	Regular penetration tests	x
Technical	Regular testing of the hardware (lifecycle, performance)	x
Organizational	Appointment of a data protection officer	x
Organizational	Appointment of an IT / information security officer	x
Organizational	Data protection management concept	x
Organizational	Emergency escalation procedures	
Organizational	Evaluation of service providers	x
Technical	Incident-Response-Management	
Organizational	Information / IT security concept	x
Organizational	Regular internal review / update of the measures taken in accordance with the state of the art (by DPO, IT audit, etc.)	x
Organizational	Regular reporting to the management	x

Contract control: Commissioned processing within the meaning of Article 28 GDPR

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Conclusion of contracts for data processing, taking into account all legal requirements in accordance with Art. 28 GDPR	x
Organizational	Selection of the contractor under due diligence aspects (especially with regard to data security)	x
Organizational	Regular review of the contractor with regard to data protection/data security	x
Technical	Verification of all contractually assured technical measures (on site, if necessary)	x
Organizational	Prior examination of the safety measures taken by the contractor and corresponding documentation with verification.	x

Compliance with the rights of data subjects

Type of Measure	Measure	Measure available at evasys GmbH
Organizational	Information about processing of personal data, purposes, categories, storage period, correction, deletion, restriction, objection, right of complaint	x
Organizational	Complaint to competent supervisory authority	x
Organizational	Data portability	x
Organizational	Differentiated consent and objection options	x
Organizational	Establishment of a single point of contact for data subjects	x
Organizational	Restriction of processing	x
Organizational	Data deletion	x
Organizational	Immediate rectification	x
Organizational	Revocation of consent	x

Annex 2

Password Policy

1. The password consists of at least 12 characters; for administrative user accounts or passwords for encrypted data storage devices, containers, or files, at least 20 characters.

2. The password consists of at least three of the four character classes, upper and lower case letters, numbers and special characters (e.g. punctuation marks).

3. The password is not stored in plain text and is not reversibly encrypted. The methods used for this are either those under point 4 or methods of equivalent quality.

4. Currently at least SHA2 or better are used for irreversible storage of the password. Attention is paid to increasing the entropy, either by means of a cryptographic "salt" or a "rehashing" or by means of a method of equivalent quality.

5. The password is chosen and entered independently by the respective user.

6. The password must not be easy to guess. In particular, the following must not be used:

    6.1. Trivial sequences of characters such as "1234", "qwerty", "asdf", etc.,
    6.2. Words, terms, or names from the private or professional environment or parts thereof,
    6.3. Data that can be easily inferred as an outsider, such as date of birth, city, street, etc. to which the user has a connection, no words, no names/abbreviations.

7. The generic change of password is enforced every 90 days even for ordinary users. The new password must differ from all passwords of the last 18 months by at least three digits. This does not apply to encrypted storage devices, containers, or files.

8. If possible or necessary, two-factor authentication by means of OTP or token generators or smart card or biometric method in combination with a password that complies with the above policies may be used. This provides increased security for access control. Biometric identification methods and the OTP or token generators or smart card alone are not sufficient authentication, as they only work via possession.