Acceptable Use Policy for Information and Communication Systems

Purpose

The Acceptable Use Policy forms an integral part of INEB | EKETA's Information Security, Privacy Protection and Business Continuity Policies. It describes the permitted and prohibited uses and activities of users of the Institute's Information Systems, the information stored in the Institute's Information Systems and other critical infrastructure.

The purpose of the Acceptable Use Policy is to ensure that Institute users do not exploit the access granted to them in accordance with the Policy on Logical Access to Information and Communication Systems in order to carry out actions thatany law of the state, lead to the disclosure of confidential information, disrupt the smooth operation of the Institute or, more generally, damage the Institute's reputation. For this reason, upon recruitment, every employee of the Institute signs a Declaration of Acceptance of the Information Security, Privacy Protection and Business Continuity Policies, after these have been explained to them.

In particular, with regard to information, Institute users are required to handle, transmit and store it in accordance with its classification.

The classifications used for information are:

- Public: Documents or information which may be disclosed to third parties without this entailing financial or other consequences for the Institute.
- Internal: Documents or information not intended for distribution or disclosure outside the Institute. In the event that Internal Documents are made public, the consequences will not have a direct financial or legal impact on the Institute but will jeopardise its reputation or credibility.
- Confidential: Documents or information that must not be disclosed or published to third parties or unauthorised persons. The disclosure of Confidential Documents or Information may have direct or indirect financial consequences for the Institute or even hinder the continuation of its activities.

The classification of documents is clearly stated in the header or footer of each document. For any document that does not explicitly state its classification, its use or disclosure shall be subject to the approval of the line manager.

For the classification of emails, the classifications recommended by the platform provider are used. However, the classification of emails should not be left to the capabilities of the mail server and client. The user must classify them themselves, even if this is done independently.

Furthermore, the Institute manages its assets in accordance with their classification.

Scope

The Acceptable Use Policy and its constituent parts, specifically:

- User Rights

- User Obligations
- Consequences
- Rights of the Institute
- Obligations of the Institute
- Storage Media Management Policy
- Portable Data Storage Media Management Policy

(excluding the Partner Security Policy) apply to all users of the Institute.

The Partner Security Policy applies to the Institute's partners, suppliers and subcontractors.

User Rights

User rights refer to the Institute's user groups.

User: A user of the Institute is defined as any employee, partner or supplier who has access to the Institute's Information Systems, in accordance with the Access Control Policy.

Users' rights regarding individual services, subject to the rules communicated to them, are defined as follows:

- Use of email, without sending messages, files or photographs that violate any law of the state, lead to the disclosure of confidential information or, more generally, damage the Institute's reputation. Written guidelines regarding the use of email and the internet have been issued to users and form an integral part of this policy.
- Access to the internet, exclusively to legitimate websites.
- Access to the Institute's internal network, in accordance with their duties.
- Access to the Institute's cloud, in accordance with their duties.
- Access to the Institute's information systems, depending on the nature of their work and the rights granted to them.

User Obligations

Users' obligations are the same regardless of the administrative/research group to which they belong and are as follows:

- To respect and comply with the laws and regulations of the state.
- T o be aware of and comply with the Institute's Information Security and Privacy Protection Policies and Procedures.
- To sign a Declaration of Acceptance of the Institute's Information Security and Privacy Protection Policies on the day of their recruitment.
- Take all appropriate measures to ensure information security (insofar as it concerns them), such as keeping their passwords confidential, locking their computer

when they step away, and changing their password at regular intervals in accordance with the best practices adopted regarding complexity and non-reuse.

- A relevant guideline has been issued regarding security passwords, urging users who have to manage more than one password to use specialised password management software which, in addition to all other conveniences, features a random password generation system incorporating the highest security standards.
- Not to install unauthorised or illegal software on the equipment provided to them by the Institute for the performance of their duties (personal computers / laboratory equipment, etc.).
- To immediately inform the Information Security Manager if they become aware of any security breach in the Institute's Information Systems or procedures that jeopardises its information.
- They must not attempt to gain access to Information Systems or information that is not necessary for the performance of their duties or that is not publicly available.
- It is prohibited to attempt to exploit potential security vulnerabilities in the Institute's Information Systems in order to gain access to information belonging to other Institute users, disrupt the smooth operation of the Information Systems, execute malicious software, or generally compromise the security of the Information Systems.
- Not to disclose to unauthorised persons any confidential or internal information or data that comes to their attention or comes into their possession as a result of the nature of their work.
- Upon leaving the Institute (whether voluntarily or otherwise), they must return all equipment received in good condition, as well as hand over any information or documents belonging to the Institute.
- They must not allow third parties to use the password assigned to them by the Institute in order to gain access to the Institute's applications or other information. Similarly, they must not accept other users' passwords for their own personal use.

Consequences

In the event of users' non-compliance with their obligations, as set out in the Acceptable Use Policy, the Information Security Manager shall take the following actions:

1. A warning is issued to the user by the Information Security Manager (ISM) and the user's Department/Division Manager is informed.
2. In the event of non-compliance by the user or a recurrence of the incident, a recommendation is made to the user's Department/Division Head and the Institute's Senior Management is informed by the ISM.
3. In the event of continued non-compliance, the Senior Management is informed by the YDAP.

The imposition of sanctions is determined by the relevant Head of the user's Department/Division to whom the recommendation is made, in consultation with Senior Management and the Information Security Manager.

When imposing sanctions on an employee, the following are taken into account: the impact of the misconduct, the appropriateness, the specific circumstances in which the misconduct occurred, the employee's general character, as well as their professional reputation as evidenced by their personnel file, and the principle of proportionality is observed.

Rights of the Institute

INEB | EKETA provides users of the Institute with access to the Information Systems, subject to the following:

- The Institute has the right to remove or delete immediately, in part or in full, entries, photographs, data or any other material and content in general, which expresses political views, religious elements, ethnic characteristics, gender discrimination and other personal data that contravene provisions of national and EU legislation or offend public decency.
- The Institute reserves the right, in accordance with its access policies, to grant or revoke access rights to users depending on their professional duties.

Obligations of the Institute

- It must comply with the entire institutional and legal framework relating to Information Security, Business Continuity and the protection of personal data.
- It grants access to its Information Systems only if the user has read and accepted the Acceptable Use and Information Security Policies. This is evidenced by a written declaration bearing the user's original signature.
- They must inform users, partners and patients clearly and comprehensively in the event that they collect or process information falling within the category of personal data and held in their Information Systems or in a paper file.
- It must inform its users, partners and patients of the contact details that may be stored in backups and which are recoverable even after they have been deleted by the user. Users must be aware of the data backup procedure.
- It must make every effort to ensure the proper functioning of Information Systems and to rectify any faults.
- It must maintain, renew, update and expand the Information Security Management, Privacy Protection and Business Continuity Policies.
- It must inform all its staff of this policy and take all necessary steps to train users.
- It must implement information security policies using modern and proven information security technologies and procedures.

Security Policy for Partners – Suppliers – Subcontractors

Purpose

The purpose of the Partner – Supplier – Subcontractor Security Policy is:

- To maintain, between the Institute and its partners/suppliers/subcontractors, an agreed level of service provision (Service Level Agreement) and information security, within the framework of a signed Cooperation Agreement.
- The prevention of potential harmful incidents that may arise from the activities of the Institute's partners / suppliers / subcontractors.
- To safeguard the confidential information and personal data of patients/examinees/research participants and the Institute's employees.

Scope

This policy applies to the Institute's partners, suppliers and subcontractors (hereinafter referred to collectively as 'partners' for the sake of brevity), whether natural or legal persons who have or may gain access to the Information Systems and the information collected and processed by INEB | EKETA.

Compliance with this policy is mandatory and forms an integral part of the collaboration agreement.

Contents

The activities of the Institute's partners, whether they are individuals or companies undertaking various tasks, such as the development, upgrading and maintenance of Information Systems, printing work, etc., as well as service providers, such as telecommunications services, may jeopardise the implementation of the organisation's Information Security Policies.

To ensure that partners comply with the Institute's Information Security Policies, they sign a Confidentiality Agreement and are provided with a copy of this Policy.

INEB | EKETA maintains an up-to-date register listing the partners who have been granted or provided with access to the Institute's information systems in order to offer their services.

Obligations of collaborators

The Institute's partners have the same obligations regarding the security of the Institute's information and information systems, the protection of privacy and business continuity as the Institute's employees.

Specifically in the case of remote access, partners, suppliers and subcontractors must strictly follow the access request procedure, stating the purpose or task involved and the duration required.

The Institute's partners shall allow the organisation, following timely notification and by mutual agreement, to inspect their facilities, policies and procedures, so that the Institute may verify compliance with the terms of the Confidentiality Agreement, the Service Level Agreements (SLAs) and the Cooperation Agreement signed between the two parties (Right to audit).

The audit will be conducted by the Information Security Manager and, possibly, specialist members of his team.

Ensuring information security, privacy protection and business continuity

INEB | EKETA takes all necessary measures to ensure that the activities of its partners do not jeopardise the rights of the system's stakeholders with regard to their health, information security, business continuity and the protection of their personal data.

Protection of Information Systems from Partner Actions

The Institute recognises the risks arising from the activities of its partners and takes all measures to mitigate them.

Obligations of partners

- The Institute's contractors must be familiar with and comply with all the terms and conditions relating to the Institute's Information Security, Privacy Protection and Business Continuity that have been communicated to them. The same rules apply to the staff of partners who carry out work on the Institute's Information and Communication Systems as to the Institute's own staff.
- The Institute's contractors must report to the Institute any incident that may jeopardise its Information or Information Systems.
- The Institute's associates must respect the classification of the information/data to which they have access and manage it in accordance with that classification.
- The Institute's associates are prohibited from disclosing information or other details relating to (a) patients' personal data, (b) details concerning healthcare services provided or to be provided to a person, (c) other personal data of users of the Information Systems.
- The Institute's partners shall permit the Institute, following timely notification and by mutual agreement, to inspect their premises and procedures in order to verify compliance with the terms of the Confidentiality Agreement, the Service Level Agreements (SLAs) and the Cooperation Agreement signed between the two parties (Right to audit).
- Specifically in the case of remote access, partners, suppliers and subcontractors must strictly follow the access request procedure, stating the purpose or task involved and the time period required.

Contracts

All operational requirements for the Information Systems are described in detail in the contracts with partners. The contracts contain the following provisions

- Right to Audit
- Confidentiality
- Non-Disclosure Terms

- Service Level Agreements
- Insurance Cover (where required)

Furthermore, the contracts make specific reference to:

- The requirements and measures taken to ensure information security and business continuity, so as to safeguard the confidentiality, availability and integrity of information when accessed and processed by the Institute's partners, as well as its permanent deletion and destruction upon termination of the collaboration.
- Upon signing the contract, the partner undertakes to implement appropriate measures for information security and to ensure business continuity, as specified in the contract.

In the event that part or all of the development of an information system is outsourced to a partner, the relevant contract must include:

- A description and methodology of the development process
- Definition of roles and responsibilities
- Security specifications for the development environment
- Processes to ensure that the partner meets the Institute's information security requirements, as set out in its Policies and Procedures.

Project contracts relating to the operation of the Institute's Information Systems include terms that ensure, both contractually and technically, compliance with the Institute's Information Security Policies and Procedures. The contracts make specific reference to the Protection of Personal Data.

Project contracts relating to the operation of the above Systems include clauses in the event of non-compliance with the Information Security Policies and Procedures.

Access to the personal data of patients/examinees/research participants at the Institute is subject to the applicable Data Protection legislation.

Staff members who gain access to Information or Information and Communication Systems and data relating to patients' communications are not permitted to disclose any information or details that come to their attention or into their possession, as a result of the nature of their work.

The Information Security Manager reviews and advises on the adequacy of the contract terms relating to information security, of Information Systems, as well as on the partner's ability to meet the security and business continuity requirements set by the Institute.

INEB | EKETA appoints a specific individual who is responsible for supervising the relevant partner.

The terms relating to compliance with Information Security Policies are also included in the project calls for proposals.

For staff of partners who have access to the Institute's IT facilities (e.g. Computer Room), laboratory equipment and information systems, a permit is required and temporary access is granted (via RFID tag, with log files) by the Institute's Information Security Officer.

External maintenance or repair teams working on IT premises and infrastructure are accompanied at all times by Institute staff.

A partner may not grant rights of use or access to the Institute's equipment to third parties without the express permission of the Institute's Management.

The Institute's partnerships are reviewed on an annual basis to enable their evaluation and improvement. Senior Management and Heads of Divisions/Departments monitor the progress of contracts with the Institute's partners on an annual basis.

Potential changes to the services provided by partners, or the review and improvement of existing information security policies and related procedures and controls, are examined in the light of the criticality of the business information and processes concerned and the re-assessment of the risks.

The Institute's designated staff shall activate the Security Incident Management Policy for any breach of the contractual terms regarding information security and the confidentiality terms referred to in the preceding paragraphs.

Storage Media Management Policy

Purpose

The management, storage, withdrawal or destruction of storage media must be carried out in such a way as to ensure the confidentiality, integrity and availability of the data hosted on them, in accordance with the Information Security Management Policies, Privacy Protection and Business Continuity of the Institute

INEB | EKETA holds and manages confidential data in the context of carrying out its research projects and providing its services. This data, which may potentially be stored on various storage media, must be protected against unauthorised disclosure, destruction or misuse. The Institute uses security mechanisms that provide an appropriate level of protection for the storage media.

Scope

The Storage Media Management Policy applies to all media used for the storage of the Institute's data and information and applies to all users of the Institute.

Contents

Procedures and Guidelines

1) Storage Media Management:
   (1) Users must take all reasonable measures to protect the storage media entrusted to them, whether from unauthorised access or theft, or from accidental destruction.
   (2) Appropriate physical and environmental safeguards must be provided for storage media placed in a storage area.
   (3) Management of storage media containing confidential data:
      - Storage media containing confidential data must be accessible only to authorised users. Where this cannot be ensured, they must be encrypted using appropriate methods in line with the current state of the art.
      - Storage media containing confidential data, if removed from the machine on which they are installed, must be appropriately labelled with their classification level. The labelling must include all specific handling instructions.
      - Storage media containing confidential data must be adequately protected when not in use (e.g. kept in a locked drawer, cupboard or security box).
      - Storage media containing confidential information should be kept out of sight when visitors are present.
2) Destruction of Storage Media:
   (1) Users must be aware that deleting data locally from storage media does not completely or permanently remove it from the medium. Deleted files are vulnerable to unauthorised recovery if they are not properly disposed of or destroyed. For this reason, the destruction of storage media is carried out by the IT Manager through physical destruction.

(2) Storage media containing confidential data are destroyed by physical destruction when they are no longer used for the storage of confidential data.
(3) For any IT equipment managed by the IT Manager that is transferred, donated or otherwise decommissioned, the storage media associated with that equipment are subject to a physical destruction process.

Roles and Responsibilities

Information Owners are responsible for the correct classification of information and its handling in accordance with its classification. The holder of classified information must manage it in accordance with the classification assigned to it by the information owner.

Holders of storage media must handle and destroy them in accordance with the Institute's policies and procedures.

1) **Systems Administrators** are responsible for:
   (1) Assisting Information Owners with the proper handling of information and storage media, in accordance with corporate policies and procedures.
   (2) Implementing policies and procedures for all storage media assigned to them.
   (3) To notify the Information Security Officer immediately in the event of the loss, destruction or theft of any storage medium entrusted to them.
2) **Users** are responsible for:
   (1) Protecting the storage media in their possession.
   (2) Notifying the Information Security Officer in the event of the loss, destruction or theft of any storage medium entrusted to them.
   (3) Not storing classified information on portable storage media that has not been previously encrypted.
3) Managers**/Heads of Divisions/Departments** must:

   Ensure that their staff are aware of the correct procedures for handling and disposing of storage media, in accordance with the Institute's policies and procedures.

4) The **Information Security Officer** is responsible for developing policies and procedures for the management of storage media, for training and keeping users informed of these, as well as for conducting checks on their implementation.

Policy on the Management of Portable (Removable) Data Storage Media

Purpose

The purpose of the Policy on the Management of Portable Information Storage Media is to define and implement appropriate measures regarding the use, handling and disposal of portable storage media in order to prevent the disclosure of information to unauthorised persons.

Scope

The Policy on the Management of Portable Data Storage Devices applies to all users of the Institute.

Contents

INEB | EKETA permits the use of unencrypted portable data storage devices exclusively for the transfer of presentations and information of a public nature.

Should there be a need to transfer information of a different classification to a portable storage device, a request must be made to the Information Security Manager, who, provided they approve the request, provide the applicant with an encrypted external hard drive or USB stick.

In any other case, the use of portable storage media for the transfer of information is strictly prohibited.

Any portable storage device that has been rendered unusable for any reason must be handed over to the IT Manager, who will ensure its physical destruction and recycling. INEB | EKETA enters into a relevant agreement with a recycling company, where appropriate.

Portable storage devices containing confidential data must also be protected against unauthorised access, misuse or tampering during transport.

INEB | EKETA:

- Uses reliable carriers or courier companies.
- Uses appropriate packaging, in accordance with the manufacturers' instructions, to protect the contents from any physical damage that may occur during transport.

Staff responsible for the transport of portable storage media:

- He/she must ensure that the vehicles being transported are not left unattended at any time.
- They must report to the Institute any unusual events or incidents relating to the security of the storage media being transported.

Policy on the use of INEB's communication/team organisation and task management platform

1. Purpose

The purpose of this policy is to ensure the safe and effective use of communication and task management platforms, such as Slack, Trello and similar services, by all INEB members. This policy aims to safeguard sensitive information, ensure compliance with regulatory requirements and promote effective communication and collaboration within the Institute.

2. Scope

This policy applies to all staff, research staff, students and any other person granted access to the Institute's communication and task management platforms. It covers the use of these platforms both on the Institute's premises and remotely.

3. Policy Statement

The Institute is committed to providing a safe and productive environment for all its members. The use of communication and task management platforms is encouraged to facilitate collaboration, information exchange and project management. However, it is imperative that these tools are used responsibly and in accordance with the following guidelines to protect the Institute's information and resources.

4. Guidelines for use

4.1. Account security

Users must keep their account credentials confidential and are prohibited from sharing their login details with others.

Two-factor authentication must be enabled for all accounts where available, to provide an additional layer of security.

Users who have access to such services, as well as their associated permissions, must be recorded.

4.2. Data handling and confidentiality

Sensitive or confidential information should only be shared via private channels or direct messages and only with individuals who have a legitimate need to know.

Users must comply with all applicable data protection and privacy laws when handling personal or sensitive information.

4.3. Acceptable use

The platforms should be used exclusively for activities related to the Institute and not for personal communications.

Users must refrain from posting content that is offensive, biased or otherwise inappropriate.

4.4. Compliance and Reporting

Any suspicious activity, data breaches or policy violations must be reported immediately to the Institute's IT Security Team.

Users are expected to comply with all software licence agreements and terms of service for the platforms used.

4.5. Training and Awareness

All users are required to complete an initial training course on the safe and effective use of the communication and task management platforms. Refresher training sessions will be held annually or as required.

4.6. Monitoring and enforcement

The Institute reserves the right to monitor the use of the platform to ensure compliance with this policy. Any breaches may result in disciplinary action, up to and including termination of access, employment or enrolment.

5. Implementation

The IT Department is responsible for implementing and enforcing this policy. This includes providing the necessary training, monitoring the use of the platform and taking corrective action when breaches occur.

6. Review and revision

This policy will be reviewed annually or more frequently, as required, to reflect changes in regulatory requirements, technological developments or operational needs. Amendments to this policy will be communicated to all relevant parties in a timely manner.

7. Acknowledgement

By accessing and using the Institute's communication and task management platforms, users acknowledge that they have read, understood and agreed to comply with this policy.

Data protection (compliance with GDPR & ISO 27701)

1. Purpose

This policy sets out the principles and guidelines for the responsible and lawful use of the Institute's information systems, networks and resources, ensuring compliance with the GDPR and ISO 27701 regarding the protection of personal data. Its purpose is to mitigate the risks associated with unauthorised access, data breaches and misuse of personal data, whilst supporting the Institute's commitment to privacy, security and regulatory compliance.

2. Scope

This policy applies to all students, research staff, employees, external partners and third parties who access or use the Institute's IT infrastructure, data repositories, cloud services or any device (including personal devices under the BYOD scheme) connected to the Institute's network. It covers all forms of personal data processing, including collection, storage, transmission and disclosure, whether via devices provided by the Institute or via personal devices. All information systems, digital communications, data storage solutions and access points – whether on-premises or cloud-based – must comply with GDPR and ISO 27701 standards for privacy, security and data governance. Any processing of personal data must be explicitly authorised, monitored and documented to ensure compliance with legal and regulatory requirements.

3. Policy Statement

Users must ensure that they do not process, store or transmit PII unless they have received explicit authorisation and it is necessary for academic, research or administrative purposes. The use of personal data must comply with the principles of data minimisation, and users must employ appropriate technical and organisational measures (e.g. encryption, access controls, secure authentication, etc.). Unauthorised access, modification, sharing or storage of personal data outside approved and secure environments is strictly prohibited. All users must immediately report any suspected data breaches, unauthorised access or security incidents.

Users must adhere to the following principles when accessing or processing personal data:

Lawfulness, fairness and transparency: The processing of personal data must be carried out only for lawful, legitimate and explicitly defined purposes.

Data minimisation: Only the minimum necessary personal data should be collected, processed or stored, and access should be restricted to authorised personnel.

Security and confidentiality: All personal data must be encrypted, subject to access controls, and protected against unauthorised disclosure, alteration or loss. When

remote access to personal data, multi-factor authentication (MFA) and secure transmission protocols must be used.

Retention and disposal: Personal data must be retained only for the documented and legally specified period and securely deleted when no longer required.

Incident reporting: Any suspected or confirmed breach involving PII must be reported immediately in accordance with the Institute's incident response protocol.

4. Instructions for use

- Access controls: Access to PII is granted on a need-to-know basis, with role-based access controls (RBAC) and multi-factor authentication (MFA) applied where required.
- Data transmission and storage: Personal data must be transmitted securely (e.g. encrypted email, VPN) and stored only in approved storage locations. Cloud services must be checked for GDPR compliance prior to use.
- Data retention and disposal: Personal data must be retained only for the documented period necessary for its intended purpose. When disposing of data, secure deletion methods must be used to prevent unauthorised retrieval.
- Monitoring & auditing: The Institute reserves the right to monitor, audit and log activities relating to the access and processing of personal data to ensure compliance. Users must cooperate with security checks and investigations where required.
- Use of personal devices (BYOD): If a personal device is used to access personal data, explicit written authorisation must be obtained and users must comply with the BYOD policy, including the implementation of the required security measures.
- Prohibited activities: Users must not share, store or transmit personal data outside authorised systems, use personal email to exchange PD, or bypass security controls.
- Monitoring and compliance: All system activities relating to personal data are subject to monitoring, logging and audits to ensure compliance. Breaches of this policy may result in disciplinary action and legal consequences.
- User responsibilities: Every user who handles personal data must complete the mandatory data protection training and acknowledge their role in protecting sensitive information.
- By accessing the Institute's IT resources, users confirm their understanding and acceptance of these data protection obligations in accordance with the GDPR and ISO 27701.

Physical Data Transfer Policy - (compliance with ISO 27001:2022, GDPR & ISO 27701)

1. Purpose

This policy sets out the security measures and compliance requirements for the physical transfer of data, whether containing simple data or personally identifiable data, ensuring alignment with the ISO 27001:2022, GDPR and ISO 27701 standards. It aims to prevent unauthorised access, data breaches, loss or corruption during the physical transfer of data via removable media, printed documents, external hard drives or other physical storage devices.

2. Scope and Application

This policy applies to all teaching staff, staff, students, contractors and third parties who transfer data physically using any medium, including, but not limited to, USB drives, external hard drives, CDs/DVDs, paper files, portable computing devices (laptops, tablets) and paper documents. It covers both internal transfers within the Institute and external transfers to third parties, suppliers or regulatory bodies.

3. Policy Statement

The physical transfer of plain text data must only take place when absolutely necessary and only via secure, approved methods. Unencrypted or insecure physical transfers are strictly prohibited. Personal data must not be copied or transferred unless there is explicit authorisation, with documented justification, a retention period and approval from the designated Data Protection Officer (DPO). Any physical transfer of data must be recorded, monitored and tracked to maintain accountability and prevent data loss or unauthorised disclosure.

4. Instructions for use

- Data classification and approval:
  - Prior to any physical transfer, data must be classified according to its sensitivity and the transfer must be justified.
  - The transfer of personal data or sensitive data requires prior written authorisation from the relevant department or the Data Protection Officer (DPO).
  - External transfers to third parties must comply with the GDPR rules on data transfer, including the signing of appropriate data processing agreements (DPAs).
- Approved storage and transport media:
  - Only encrypted storage media approved by the Institute (e.g. encrypted USB sticks, external hard drives with hardware encryption) may be used for the transport of sensitive data.
  - Where printed documents are transported, they must be stored in locked, tamper-proof containers and handled only by authorised personnel.
  - The transfer of physical data outside the Institute's premises must be documented and monitored, ensuring a controlled retention record.

- Encryption and security measures:
  - All sensitive data or personal data must be encrypted prior to physical transfer.
  - Strong encryption methods (AES-256 or higher) must be used for removable storage devices.
  - Passwords for encrypted files or devices must be sent separately via a secure channel (e.g. encrypted email, secure messaging platform).
- Physical security and transport:
  - Physical storage devices must not be left unattended in public places, vehicles or unsecured areas.
  - When transporting sensitive data via courier or postal services, tamper-proof packaging must be used and the parcel must be sent via a tracked and secure delivery service.
  - Only authorised personnel may handle physical data transfers and must sign a declaration of responsibility.
- Data retention and disposal:
  - Physical data must be stored only for as long as necessary, in accordance with documented retention policies.
  - Any obsolete or redundant physical data must be securely disposed of by destruction, incineration or certified data destruction methods for storage media.
  - A distribution log must be kept for compliance checks.
- Incident reporting:
  - Any loss, theft or unauthorised access to physically transported data must be reported immediately to the Data Protection Officer (DPO) and the Head of the Data Protection Unit.
  - The Institute will conduct an investigation and, if necessary, report the incident to the competent Data Protection Authority in accordance with the requirements of the GDPR.