Information Security Policy

Document Type: Standalone Institutional Policy
Institution: European Academy of Advanced Studies (EAAS)
Applies To: Students, faculty, administrative staff, management, contractors, vendors, and authorised third-party service providers
Policy Owner: Prof. Dr. Wolfgang Georg Arlt FRGS FRAS- Dean, Quality Assurance Cell
Effective Period: 2026–2027
Review Cycle: Annual review or earlier where required by regulatory, operational, or technological change

1. Purpose and Scope

The purpose of this Information Security Policy is to define the principles, responsibilities, and controls used by EAAS to protect institutional information, student records, staff records, learning data, assessment data, communication systems, and digital platforms.

EAAS operates as a fully online higher education institution and uses digital systems to support teaching, learning, assessment, student administration, quality assurance, communication, and institutional governance. The institution uses systems such as Moodle, BigBlueButton, Turnitin, cloud-based document storage and email communications.

This policy applies to:

- Student personal data and academic records
- Staff and faculty records
- Moodle and Learning Management System data
- Assignment submissions and assessment records
- Turnitin originality reports
- Internal quality assurance records
- Institutional policies, procedures, and governance records
- Email and communication records
- Financial, administrative, and operational information
- Data held by authorised vendors and third-party systems

EAAS is committed to handling information in a safe, lawful, confidential, and responsible manner, in line with the General Data Protection Regulation, Maltese legal requirements, MFHEA expectations, and institutional quality assurance standards.

2. Roles and Responsibilities

2.1 Management Board

The Management Board has overall responsibility for institutional governance and ensures that appropriate information security controls are implemented and monitored. Responsibilities include:

- Approving institutional policies related to information security and data protection
- Ensuring compliance with legal and regulatory requirements
- Allocating resources for secure digital infrastructure
- Reviewing reports relating to risks, incidents, audits, and improvement actions

2.2 Rector and Head of Institution

The Rector has executive responsibility for ensuring that information security is implemented across academic and administrative operations.
Responsibilities include:

- Ensuring that staff and students comply with institutional information security rules
- Supporting the implementation of secure teaching, learning, and administrative systems
- Ensuring that information security risks are escalated where necessary
- Promoting a culture of data protection, accountability, and responsible digital conduct

2.3 Quality Assurance and Compliance Unit

The Quality Assurance and Compliance Unit is responsible for monitoring compliance with institutional policies, including information security, data protection, and information management procedures.
Responsibilities include:

- Conducting internal reviews and compliance checks
- Maintaining policy documentation
- Supporting staff awareness and training
- Monitoring evidence of compliance for accreditation and regulatory review
- Reviewing incidents and recommending corrective actions

2.4 IT and Digital Systems Administrator

The IT and digital systems administrator is responsible for the technical security of institutional digital platforms.
Responsibilities include:

- Managing access rights and user permissions
- Maintaining Moodle, communication systems, cloud storage, and other approved platforms
- Implementing system updates and security patches
- Monitoring system availability and performance
- Supporting backup, recovery, and incident response procedures
- Ensuring that only authorised users have access to institutional systems

2.5 Academic Staff

Academic staff are responsible for protecting student data, assessment records, feedback, and learning materials.
Responsibilities include:

- Using only approved institutional systems for teaching and assessment
- Protecting student submissions, grades, feedback, and academic records
- Avoiding unauthorised sharing of student information
- Reporting suspected data breaches or system misuse
- Ensuring secure use of Moodle, BigBlueButton, Turnitin, and related systems

2.6 Administrative Staff

Administrative staff are responsible for protecting student records, admissions documents, communication records, and institutional data.
Responsibilities include:

- Maintaining confidentiality of student and staff information
- Following access control and password rules
- Using approved storage and communication channels
- Reporting suspected security incidents
- Handling records in accordance with data protection requirements

2.7 Students

Students are responsible for using institutional systems securely and ethically.
Responsibilities include:

- Keeping their login credentials confidential
- Using Moodle, email, and other platforms responsibly
- Not attempting to access unauthorised systems or records
- Not sharing institutional materials without permission
- Reporting suspicious activity or account compromise

2.8 Vendors and Third-Party Service Providers

Vendors and third-party providers must comply with institutional security expectations and applicable data protection laws.
Responsibilities include:

- Processing institutional data only for agreed purposes
- Applying appropriate technical and organisational security measures
- Maintaining confidentiality of institutional and personal data
- Notifying EAAS of security incidents affecting institutional data
- Supporting audits, data protection reviews, and contract compliance checks where required

3. Access Control Rules

EAAS applies role-based access control to ensure that users only access information required for their role.
Access control principles include:

- Access is granted only to authorised users.
- Access is based on institutional role, function, and operational need.
- Student access is limited to their own learning materials, submissions, grades, and feedback.
- Faculty access is limited to assigned modules, student submissions, assessment data, and relevant academic records.
- Administrative access is limited to relevant student, staff, admissions, finance, or support records.
- System administrator access is restricted to authorised technical personnel.
- Access rights are reviewed periodically.
- Access is removed or amended when a staff member, student, contractor, or vendor changes role or leaves the institution.
- Shared accounts are not permitted unless formally approved for a specific operational reason.
- Unauthorised access, attempted access, or sharing of access credentials is treated as a security breach and may lead to disciplinary action.

4. Password and Authentication Requirements

All users must protect their accounts through secure password practices.
Password requirements include:

- Passwords must be unique and not reused across personal and institutional accounts.
- Passwords must not be shared with other users.
- Passwords must not be written down in unsecured locations.
- Passwords must be changed immediately if compromise is suspected.
- Users must not save passwords on shared or public devices.
- Default passwords must be changed before systems are used.
- Administrative accounts must use stronger authentication controls than standard user accounts.
- Passwords should contain a combination of uppercase letters, lowercase letters, numbers, and symbols.
- Weak or easily guessed passwords, such as names, birthdays, or simple number sequences, must not be used.

Where technically available, systems should enforce minimum password strength, failed-login limits, and account lockout controls.

5. Multi-Factor Authentication

Multi-factor authentication should be enabled where available and appropriate, especially for systems containing sensitive or confidential information.
MFA should be prioritised for:

- Institutional email accounts
- Moodle administrator accounts
- Cloud storage administrator accounts
- Student information systems
- Finance and administrative systems
- Vendor management portals
- Systems containing student records or assessment data
- Any account with privileged access rights

Where MFA is not technically available, alternative controls should be used, such as strong passwords, restricted access permissions, regular access review, and monitoring of suspicious login activity.

6. Email and Communication Security

EAAS uses email and approved communication platforms for academic and administrative communication. Users must ensure that institutional communication is secure, professional, and compliant with data protection requirements.
Rules include:

- Institutional email should be used for official academic and administrative communication.
- Sensitive personal data must not be sent to unauthorised recipients.
- Users must check recipient addresses carefully before sending confidential information.
- Personal student information should not be sent through unsecured personal email accounts.
- Attachments containing sensitive data should be password-protected or shared through approved secure systems where possible.
- Staff and students must not open suspicious links or attachments.
- Phishing attempts must be reported immediately.
- Confidential institutional discussions should not be conducted through unauthorised messaging platforms.
- Online meetings must be managed securely, including appropriate use of meeting links, passwords, waiting rooms, and access controls where available.

7. LMS and Student Information System Security

EAAS uses Moodle and other approved digital systems to support online learning, assessment, student administration, and academic records.
Security controls include:

- Moodle access is provided only to authorised students, academic staff, and administrators.
- Student submissions are stored within approved institutional systems.
- Assessment submissions are checked through Turnitin-enabled Moodle submission points where applicable.
- Grades and feedback are accessible only to authorised users.
- Course access is restricted to enrolled students and assigned staff.
- Faculty must not download or store student assessment data on unsecured personal devices.
- Moodle administrator rights are restricted to authorised personnel only.
- Course materials, recorded sessions, and assessment information must not be shared outside authorised platforms without approval.
- Student records must be handled in accordance with GDPR and institutional data protection requirements.
- Any suspected unauthorised access to Moodle or student information systems must be reported immediately.

8. Data Classification

EAAS classifies institutional data according to sensitivity and required level of protection.

8.1 Public Data

Information approved for public release.
Examples:

- Website information
- Published policies
- Public programme information
- Marketing materials
- Public contact details

8.2 Internal Data

Information intended for internal institutional use.
Examples:

- Internal meeting records
- Operational procedures
- Internal planning documents
- Staff communications
- Internal quality assurance documents

8.3 Confidential Data

Information requiring restricted access.
Examples:

- Student records
- Assessment submissions
- Grades and feedback
- Staff records

- Admissions records
- Financial records
- Contracts
- Vendor agreements
- Internal audit reports

8.4 Sensitive Personal Data

Information requiring the highest level of protection under data protection law.
Examples:

- Identification documents
- Health-related information
- Disability or special needs information
- Disciplinary records
- Data breach records
- Any special category personal data under GDPR

Users must handle data according to its classification. Confidential and sensitive personal data must only be accessed, used, shared, stored, and retained for legitimate institutional purposes.

9. Device Security

All devices used to access institutional systems must be protected against unauthorised access, loss, theft, and malware.
Device security rules include:

- Devices must be protected by passwords, PINs, biometrics, or equivalent access controls.
- Devices used for institutional work must not be left unlocked and unattended.
- Staff should avoid accessing confidential data on public or shared computers.
- Users must log out of Moodle, email, cloud storage, and other systems after use.
- Personal devices used for institutional work must have updated operating systems and security software.
- Lost or stolen devices containing institutional information must be reported immediately.
- Confidential data should not be stored permanently on personal devices unless authorised.
- USB drives and removable media should be avoided for confidential institutional data unless encrypted and approved.
- Devices used by administrators should apply additional safeguards due to elevated access privileges.

10. Cloud Storage Security

EAAS may use approved cloud-based systems for documentation, learning resources, records management, and institutional administration.
Cloud storage rules include:

- Only approved institutional cloud platforms may be used for official records.
- Access to folders and files must be restricted according to user role.
- Confidential documents must not be shared using public links.
- External sharing must be approved and limited to legitimate institutional purposes.
- Access permissions must be reviewed periodically.
- Documents must be removed or archived when no longer required.
- Sensitive records must not be uploaded to unauthorised personal cloud accounts.
- Vendor terms, data protection safeguards, and storage locations should be reviewed where relevant.
- Cloud services should support encryption, access control, audit logs, and secure backup where available.

11. Backup and Recovery Rules

EAAS maintains backup and recovery arrangements to protect institutional continuity and reduce the risk of data loss.
Backup and recovery rules include:

- Critical institutional data must be backed up regularly.
- Backup arrangements must cover academic, administrative, LMS, and institutional records where applicable.
- Backups must be stored securely and protected from unauthorised access.
- Backup access must be restricted to authorised technical or administrative personnel.
- Recovery procedures must be tested periodically where feasible.
- Backup copies must be protected against accidental deletion, corruption, malware, and unauthorised modification.
- Recovery priorities must support continuity of teaching, assessment, student services, and institutional administration.
- Backup arrangements should be aligned with the institution's business continuity planning.

12. Malware and Antivirus Protection

EAAS requires appropriate protection against malware, viruses, ransomware, spyware, and other malicious software.
Rules include:

- Devices used for institutional work should have active antivirus or endpoint protection.
- Users must not download or install unauthorised software on institutional systems.
- Suspicious links, attachments, or files must not be opened.
- Malware alerts must be reported immediately to the responsible administrator.
- Users must not disable antivirus, firewall, or endpoint protection tools.

- Files from unknown or suspicious sources must not be uploaded to institutional systems.
- Any device suspected of infection must be disconnected from institutional systems until checked.

13. Software Update and Patching Rules

EAAS recognises that timely software updates are essential to protect systems against known vulnerabilities.
Update and patching rules include:

- Operating systems must be kept up to date.
- Moodle, plugins, themes, and related LMS components must be updated where necessary and compatible.
- Security patches must be applied promptly.
- Browser updates must be installed to ensure secure access to online systems.
- Antivirus and endpoint protection tools must be updated regularly.
- Unsupported or outdated software should not be used for institutional work.
- Updates should be tested where necessary to avoid disruption to teaching, assessment, or records management.
- Critical vulnerabilities must be prioritised for urgent remediation.

14. Incident Reporting Obligations

All staff, students, contractors, and vendors must report suspected information security incidents immediately.
Examples of reportable incidents include:

- Loss or theft of a device containing institutional data
- Unauthorised access to Moodle, email, or student records
- Accidental disclosure of personal or confidential data
- Sending student information to the wrong recipient
- Suspected phishing or email compromise
- Malware or ransomware infection
- Compromised password or account
- Unauthorised sharing of assessment materials
- Unavailability or disruption of critical systems
- Any suspected breach of GDPR or institutional data protection rules

Incident reporting procedure:

1. The user must report the incident immediately to the responsible institutional contact, IT administrator, or Quality Assurance and Compliance Unit.
2. The incident must be recorded with relevant details, including date, time, system affected, data involved, and immediate action taken.
3. The institution must assess the severity and potential impact.
4. Corrective action must be taken to contain and resolve the incident.

5. Where required by law, the incident must be escalated under GDPR breach notification procedures.
6. Lessons learned must be reviewed and used to strengthen controls.

15. Staff Training Requirements

EAAS provides staff awareness and training to support responsible information handling and secure use of digital systems.
Training requirements include:

- Data protection and GDPR awareness
- Secure use of Moodle and online learning systems
- Secure handling of student records and assessment data
- Password and authentication good practice
- Phishing and email security awareness
- Incident reporting procedures
- Secure use of cloud storage
- Academic integrity and protection of assessment information
- Responsible use of AI and digital tools where applicable
- Confidentiality obligations for academic and administrative staff

New staff should receive information security guidance as part of induction. Existing staff should receive refresher training periodically or when major systems, policies, or risks change.

16. Vendor and Third-Party System Security

EAAS uses approved third-party systems and vendors to support online education, assessment, communication, and institutional administration.
Vendor security requirements include:

- Vendors must be reviewed before use where they process institutional or personal data.
- Contracts or service agreements must define data protection and confidentiality obligations.
- Vendors must comply with GDPR where personal data is processed.
- Data processing agreements must be in place where required.
- Vendors must provide appropriate technical and organisational security measures.
- Access granted to vendors must be limited to what is necessary.
- Vendors must notify EAAS of security incidents affecting institutional data.
- Vendors must not use EAAS data for unauthorised purposes.
- Where vendors process student data, students should be informed through relevant privacy notices or institutional documentation.
- Vendor performance, risk, and compliance should be reviewed periodically.

Examples of third-party systems may include Moodle hosting, Turnitin, BigBlueButton, cloud storage services, email systems, payment systems, and other approved educational technology providers.

17. Monitoring and Audit Arrangements

EAAS monitors information security compliance through governance, quality assurance, technical review, and internal audit procedures.
Monitoring and audit arrangements include:

- Periodic review of user access rights
- Review of administrator accounts and privileged access
- Monitoring of Moodle and LMS security settings
- Review of data protection and information management practices
- Checking compliance with backup and recovery procedures
- Review of incident reports and corrective actions
- Internal quality assurance audits
- Review of vendor and third-party system arrangements
- Review of policy implementation by the Quality Assurance and Compliance Unit
- Reporting significant risks or incidents to institutional management

Monitoring must be proportionate, lawful, and limited to legitimate institutional purposes. Monitoring activities must respect privacy and data protection requirements.

18. Policy Review Cycle

This policy must be reviewed at least once per year.
The policy may also be reviewed earlier where there is:

- A major change to institutional systems
- A new LMS, cloud service, or student information system
- A significant data protection or cybersecurity incident
- A change in GDPR, Maltese law, MFHEA requirements, or other regulatory expectations
- A new vendor or third-party service processing institutional data
- A change in institutional structure, programme delivery, or assessment model
- Findings from internal audits or external reviews

The Quality Assurance and Compliance Unit is responsible for coordinating the review. The updated policy must be approved by institutional management and communicated to relevant staff, students, and stakeholders.

19. Compliance and Breach of Policy

Failure to comply with this policy may result in corrective, disciplinary, contractual, or legal action, depending on the seriousness of the breach.
Examples of non-compliance include:

- Sharing passwords or login credentials
- Accessing records without authorisation
- Disclosing confidential student or staff information
- Using unauthorised cloud storage or communication channels

- Ignoring security updates or malware warnings
- Failing to report a suspected incident
- Misusing institutional systems
- Sharing assessment materials without permission
- Breaching GDPR or institutional confidentiality obligations

All suspected breaches must be reviewed fairly and in line with institutional procedures.

20. Approval and Ownership

Policy Owner: Prof. Dr. Wolfgang Georg Arlt FRGS FRAS- Dean, Quality Assurance Cell
Responsible Authority: Dr. Jay Krishna Thakur- Rector and Head of the Institution
Approved By: Management Board
Applies From: 2026–2027 Academic Year
Next Review: 2028