



REGULATIONS / POLICY LIBRARY

Digital Learning and Information Security Standard

DIG-002 | Digital Services

VERSION 1.0 · 18 OCTOBER 2026

INSTITUTIONAL REGULATIONS & POLICIES | IEU

Digital Learning and Information Security Standard

DOCUMENT CONTROL / DIG-002

Document ID	DIG-002
Document family	Digital Services
Document custodian	Information Security / Learning Platforms Lead
Version	1.0
Edition date	18 October 2026
Review cycle	Annually and following material change

1 Purpose and applicability

Applies to accounts, systems, digital content and administrative access. The provisions govern the activities within the defined IEU service scope; applicable programme-specific contracts and verified rules of a separate awarding institution govern award requirements wherever relevant.

2 Policy requirements

- 01 Role-based permissions and multi-factor authentication protect sensitive institutional systems.
- 02 Student and staff accounts must not be shared and lost credentials must be reported promptly.
- 03 Learning resources are distributed through approved platforms with appropriate accessibility and rights controls.
- 04 Incidents are recorded, contained, escalated and reviewed using an internal response process.
- 05 Backups and recovery capability are tested according to an owned schedule.
- 06 Vendor relationships require proportional security and privacy due diligence.

3 Operational procedure

Trigger: New account, role change, vendor onboarding or security incident

- 01 Provision minimal necessary access, require MFA where feasible and deactivate access on role exit.
- 02 Record learning-platform system owners, content permissions and backup arrangements.
- 03 Contain and escalate suspected incidents; preserve evidence and notify relevant authorized contacts.
- 04 Test recovery and document remedial actions following incidents and control reviews.

4 Responsibilities and evidence

Accountable process owner. Information Security / Learning Platforms Lead maintains implementation, staff guidance, case processing and reporting. Academic decisions requiring external award authority must be referred according to the verified programme arrangement.

Minimum evidence. Access list; vendor due diligence; incident register; backup test; recovery plan.

Record protection. Keep case files, decisions and correspondence in access-controlled systems; apply an approved retention schedule and document transfers to relevant partners. Do not publish personal or confidential records.

5 Exceptions, concerns and review

Exceptions. Material deviations require a written rationale, authorization by a role with the appropriate delegation, and a record of any impact on students or staff. No local exception may override mandatory law or a controlling awarding-body requirement.

Challenge and escalation. Explain the applicable complaints, academic appeals or rights-request route to affected persons. Refer safety concerns, integrity incidents, data incidents, conflicts of interest or disputed award claims to the designated specialist authority.

Monitoring. Review privileged accounts, access exceptions and recovery test outcomes.

6 Linked institutional controls

Related controls, where relevant: Academic Regulations (ACD-001); Academic Integrity (ACD-003); Student Complaints (STU-004); Academic Appeals (STU-005); Quality Assurance (QUA-001); Privacy and Student Records (DIG-001); Academic Partnerships and Award Information (PAR-001).

7 Document information and periodic review

Document series	IEU Regulations & Policies
Institution	International European University (IEU)
Applicability	See section 1 and programme-specific terms
Student enquiries	Use the IEU contact and support routes
Document maintenance	Controlled by the responsible function