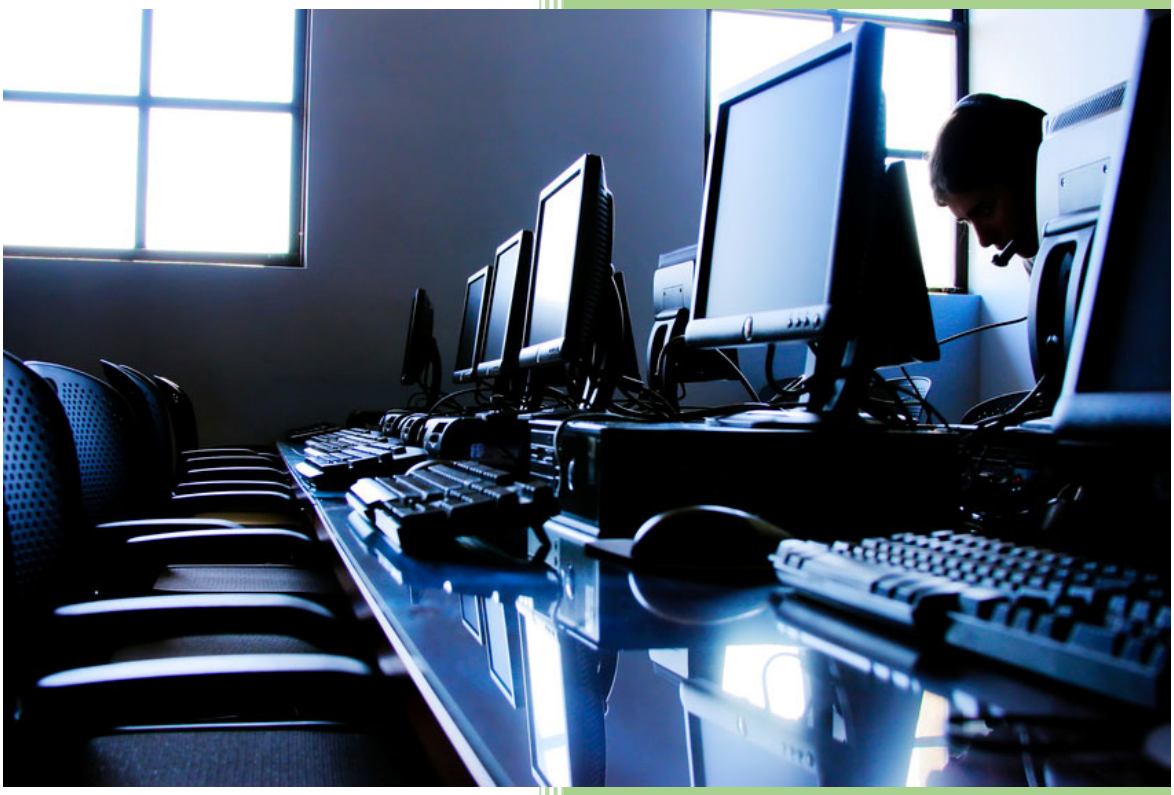
Information Security Management

Document Reference and Version No	Information Security v3
Purpose	This document sets out the Institute's commitment + guidelines in relation to the management and security of Institute held/controlled data.
Commencement Date	April 2021
Date of Next Review	May 2024
Who needs to know about this document	All Staff and external parties accessing the Institute's data.
Revision History	Minor Revision of previous guidelines.
Policy Author	Head of Information Services
Policy Owner	Head of Information Services
Approval by Sec/Fin Controller	April 2021

Information Security Management



Information Services Division

Dun Laoghaire Institute of Art Design and Technology

Contents

1.0 Overview

The ICT Acceptable/Appropriate Usage Policy (A/AUP) endeavours to protect all IADT held data and in order to fulfil IADT's mission of teaching, research and public service, the Institute is committed to providing a secure yet open network that protects the integrity and confidentiality of information while maintaining its accessibility.

Institute held/controlled data and systems are resources and assets owned by and entrusted to the IADT. This document sets out the Institute's commitment and guidelines in relation to the management of the security of these resources.

Note: all information, documents, and data created by an IADT Staff member on behalf of IADT or on IADT ICT Resources, or by any other staff member, are considered Institute property and should be treated as such unless proven to be under the ownership of a third party.

A staff member who is retiring or leaving the Institute must surrender any IADT held data including any cloud based data (MS Teams, SharePoint, OneDrive etc.) and delete any electronic copies they may have on non-owned IT systems and shred any hard copies.

2.0 Scope

This policy applies to all IADT electronic administrative systems and data no matter where they are physically hosted.

The Institute's administrative systems and data are managed, used and developed by several elements of the organisation. These guidelines sets out specific roles associated with the management of information security at IADT.

3.0 Statement + Guidelines for Information Management

The Institute generates, manages and is entrusted with private, confidential and sensitive information. The Institute is committed to protecting the confidentiality of all our information and ensuring that information is accurate, complete and available for appropriate uses.

Each member of the IADT's campus community is responsible for the security and protection of electronic information resources over which he or she has control or access to.

Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

To achieve this, we set out the following security principles:

a) **Appropriate Access**- Access to administrative data and systems shall be provided to those authorised as necessary to facilitate the conduct of Institution activities.

b) **Protection of integrity**- Information resources shall be managed to ensure that they remain accurate, trustworthy and reliable by ensuring they are protected from theft, misuse, corruption and loss.

c) **User Identity Management**- Users identity shall be tightly managed and controlled, access privileges across all systems shall be regularly audited and users access disabled where appropriate. Users should not expect any access on leaving the Institute for any reason including career break or extended unpaid leave.

d) **Risk based protection**- Data and systems shall be protected in a manner appropriate to the risks to the resources and the Institute's needs.

e) **Compliance**- Information resources shall be managed to ensure compliance with external regulation, governance and statutory requirements.

f) **Continuous review** –Protection mechanisms and processes shall be continuously reviewed to ensure that they are effective, relevant and appropriate to meet the needs of IADT.

3.1 Roles + Responsibilities

To achieve the above, the roles + responsibilities on each user can be multifaceted, but we **all** have responsibilities when it comes to information security.

Responsibilities range in scope from security controls administration for a large system to the protection of one's own access password. A particular individual often has more than one role.

Administrative Officials (individuals with administrative responsibility for Institutional organisational units or individuals having functional ownership of data) must:

- identify the electronic information resources within areas under their control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided to the campus as needed;
- establish acceptable levels of security risk for resources by assessing factors such as:
    - how sensitive the data is, such as research data or information protected by law or policy,
    - the level of criticality or overall importance to the continuing operation of the Institute as a whole, individual departments, research projects, or other essential activities;
    - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
    - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
    - limits of available technology, programmatic needs, cost, and staff support;
- ensure that requisite security measures are implemented for the resources;

Providers (individuals who design, manage, and operate campus electronic information resources) must:

- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;

Users (individuals who access and use campus electronic information resources) must:

- become knowledgeable about relevant security requirements and guidelines;
- protect the resources under their control, such as access passwords, computers, and data they download;
- should encrypt and password protect files that they share with others with-in the Institute and must password protected and encrypted if been shared outside the Institute.

Insufficient security measures at any level may cause resources to be damaged, stolen, or become a liability to the Institute. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, computer(s) and users posing a threat will be blocked from network access.

3.2 Key Security Elements

System owners + managers are required to ensure that information systems are managed in accordance with the security needs of the information resources they control or access

Logical Security:

Computers must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. For example, installations that allow unrestricted access to resources must be configured with extra care to minimize security risks.

Adequate authentication and authorisation functions must be provided, commensurate with appropriate use and the acceptable level of risk.

Attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus or off-campus resources, including computers maintained for a small group or for an individual's own use.

Physical Security:

Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or data centre where server machines are located, to simple measures taken to protect a User's display screen.

3.3 Privacy and Confidentiality

Applications must be designed and computers must be used so as to protect the privacy and confidentiality of the various types of electronic data they process, in accordance with applicable laws and policies.

Users who are authorised to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. For example, when sensitive data is transferred from a well-secured centralised system to a user's location (office, home etc.) adequate security measures must be in place at the destination computer to protect this "downstream data". Where possible the data should be kept on an IADT owned and managed device.

Information services technical staff assigned to ensure the proper functioning and security of Institute electronic information resources and services are not permitted to search the contents of electronic communications or related transactional information except as provided for in the Institute's Acceptable Appropriate Usage Policy. For example, any scanning of network traffic to detect intrusive

activities must follow established Institute guidelines to ensure compliance with laws and policies protecting the privacy of the information.

3.4 Compliance

Institute functional areas, faculties, departments, offices, or groups should establish security guidelines, standards, or procedures that refine the provisions of these guidelines for specific activities under their control, in conformance with these guidelines, the A/AUP and other applicable policies and laws.

Policies that apply to all campus electronic information resource security include, but are not limited to, the A/AUP and the Data Roles and Responsibilities, Data Protection, GDPR and document management policies. Irish and EU laws prohibit theft or abuse of computers and other electronic resources.

The following activities are specifically prohibited under these guidelines:

- interfering with, tampering with, or disrupting resources;
- intentionally transmitting any computer viruses, worms, ransomware or other malicious software;
- attempting to access, accessing, or exploiting resources you are not authorised to access;
- knowingly enabling inappropriate levels of access or exploitation of resources by others;
- downloading sensitive or confidential electronic information/data to computers that are not adequately configured to protect it from unauthorised access;
- disclosing any electronic information/data you do not have a right to disclose.

In addition to any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal.

4.0 Breaches of Security

Information Services monitor network activity. Any individual suspecting that there has been, or is likely to be, a breach of information systems security or suspect any suspicious activity should inform the System Manager and the Head of Information Services immediately, they will advise the Institute on what action should be taken. Most often, some of the biggest data breaches come from an internal source, even if it was a mistake.

The IADT President or his/her delegated agent has the authority to invoke the appropriate Institute disciplinary procedures to protect the Institute against breaches of security.

In the event of a suspected or actual breach of security, the Head of Information Services or his/her delegated agent may, after consultation with the relevant manager make inaccessible/remove any unsafe user accounts, data and/or programs on the system from the network.

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the Data Protection Acts (Irish + EU), GDPR and could lead to civil or criminal proceedings. It is vital, therefore, that users of the Institutes Information Systems must comply, not only with this policy, but also with the Institute's Data Protection policy.

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor to comply could lead to the cancellation of a contract.

5.0 Further Information

If you have queries in relation to this policy, please contact:

Head of Information Services

Dun Laoghaire Institute of Art Design and Technology

Tel: 012394777

Email: ict_manager@iadt.ie