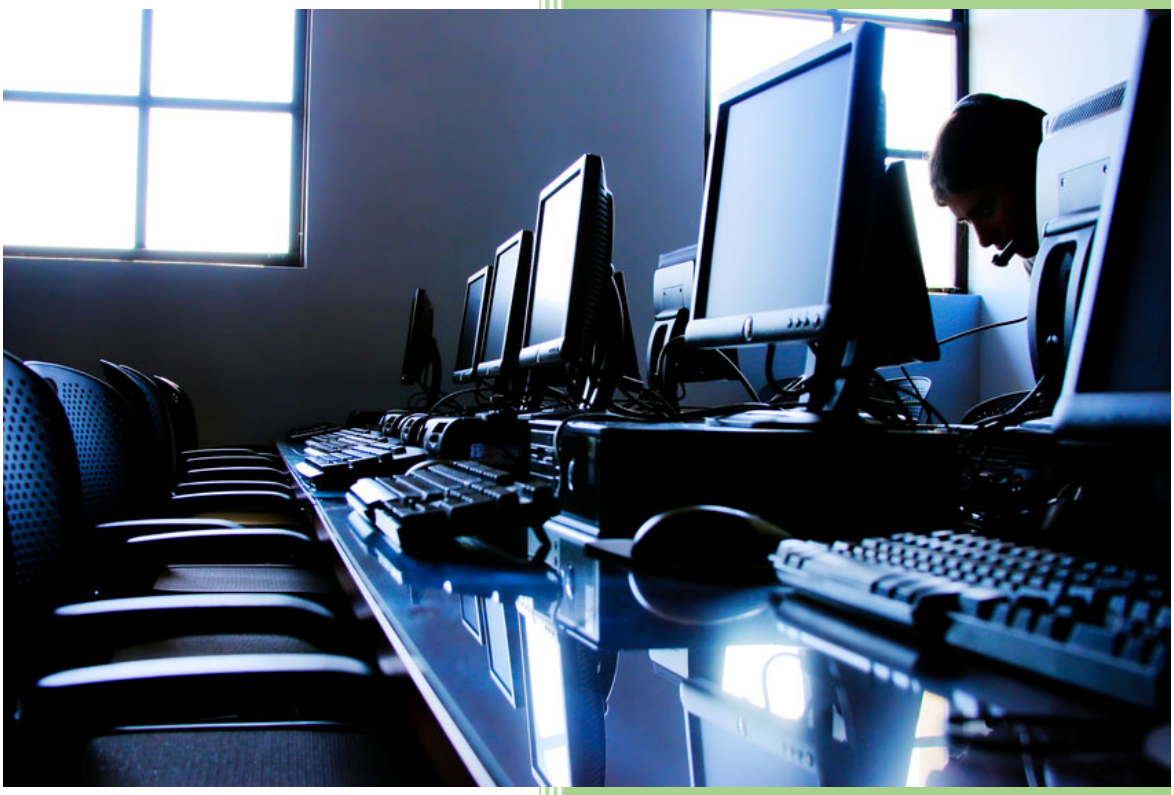
Network Security Policy

Document Reference and Version No	Network Security v2
Purpose	To ensure the continuous service, security + integrity of the IADT's ICT Network
Commencement Date	April 2021
Date of Next Review	September 2024
Who needs to know about this document	All Staff, Students and external parties accessing the Institute's networks
Revision History	Minor updates from v1
Policy Author	Head of Information Services
Policy Owner	Head of Information Services
Approval by Sec/Fin Controller	April 2021

ICT Network Security Policy



Information Services Division

Dun Laoghaire Institute of Art Design and Technology

Contents

1.0 Overview

The ICT Acceptable/Appropriate Usage Policy (A/AUP) specifies that effective security is a team effort involving the participation and support of every User who deals with information and/or information systems (section 4.2).

Information Systems play a major role in supporting the day-to-day activities of the Institute. These systems include but are not limited to all infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store Information owned by the Institute.

The network infrastructure is a key component to the success + usage of all the Institute's information systems and without it, most functions across the campus would cease. Thus the security of Network is a key component to the overall running of Institute activities.

2.0 Scope

This policy applies to all IADT's networks and connected networks and to all equipment connected to those networks physically or via wireless.

Should any networks be created independently of the campus networks, they will have to comply with this policy if they are connected to the Internet.

The policy applies to all IADT-owned ICT equipment including servers, desktops, laptops, tablets and other mobile devices, network-related equipment, as well as personally-owned equipment used by staff or students in conjunction with their work or study on IADT campus.

Note that access to and the use of IADT–related electronic information and data are covered by A/AUP, Information Security Management Guidelines and the Data Roles + Responsibilities Policy.

3.0 Policy

Every student and staff member in IADT is provided with access to the IADT networks and various services provided through these networks. They are required to familiarise themselves with the relevant policies, procedures and standards and to comply with these at all times. The up-to-date versions of the policies are available on the Information Services website (www.iadt.ie/is) and anyone requiring further information, clarification or advice should contact the Information Services support desk in the first instance (support@iadt.ie).

Information Services is responsible for the development, management and maintenance of the IADT networks and no equipment or sub-networks may be connected to the IADT network unless authorised by Information Services.

Each piece of equipment connected to the network must have as an identifiable 'owner', a staff member who will be responsible for ensuring that the connected equipment complies with the relevant policies and regulations. In cases where someone other than a member of staff is connecting equipment, they must first have the written permission of the relevant head of department, faculty or function who will take responsibility for the connection and for informing Information Services when that user no longer requires the connection. In the case of events such as conferences, the local IADT organiser will be responsible for connections made by any of the non-IADT attendees. Where an IADT staff member is taking responsibility for non-IADT users on the network, they are obliged to inform the users of their obligations under the Acceptable/Appropriate Use Policy.

Information Services has the authority to remove from the network any equipment for which no owner can be identified.

Information Services has the authority to remove from the network any equipment which is interfering with the network service or is deemed likely to compromise the security of the network. While every effort will be made to contact the owner of the equipment in advance, maintaining the service must take precedence.

Anyone connecting equipment to the network is responsible for ensuring that the equipment is configured correctly, that the operating systems and software applications are up-to-date as regards patch management etc. and that the equipment has adequate protection against viruses and other malware. If there is any suspicion that the equipment may be infected or compromised in any way it should not be connected.

Information Services acts as single point of contact between IADT and the National Research and Education Network HEAnet. Access through the network perimeter firewall is managed and operated by Information Services. Individuals located on the main Institute network may make direct application for access through the firewall for certain services through the Head of Information Services.

Any servers hosting production services for the Institute must be housed in a suitable environment with regard to security, electrical power, air cooling etc. The owner of the server must ensure that all software licenses are up-to-date and that maintenance support is available for both the hardware and software. Provision must be made for adequate backup and documented operating procedures must be available.

It is the responsibility of the System Manager of each service to ensure that an adequate business continuity plan is in place in the event that the service is affected by the non-availability of the relevant servers, network or other elements of the IT infrastructure.

Authentication is required for each connection to the network. Authentication is normally via a password or PIN. It is the responsibility of each user to ensure that their password or PIN is not disclosed to anyone. In the rare event that a member of the Information Services staff requests a user's password from them to rectify a problem with their system, the user should change their password immediately afterwards. Users should never send their passwords or other identity information via email, text, messaging system, post etc. passwords should only be shared through a phone call or conference call through MS Teams or other approved services.

Any breaches of security should be reported immediately to the Information Services support desk and the Head of Information Services.

This network policy is intended to ensure that an effective, secure and available network infrastructure for the benefit of all users is always available. Where necessary, support will be provided by Information Services to assist users in complying with the policy

4.0 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