



Waterford Institute of Technology
INSTITIÚID TEICNEOLAÍOCHTA PHORT LÁIRGE

Computer and Network Security Policy

Document Reference :	CS/GB/25102011 Version 1.0
Purpose :	The purpose of this policy is to detail acceptable usage and responsibilities regarding computer use and network security at Waterford Institute of Technology.
Commencement Date :	25 th October 2011
Date of Next Review :	This document is reviewed annually.
Who Needs to Know About this Document :	General Public, HETAC, WIT - Governing Body, Academic Council, Executive Board, Heads of School, Heads of Dept., All Staff, Student Union, Students.
Revision History :	New Document, approved by Governing Body 25 th October 2011.
Policy Author :	IT Manager
Policy Owner :	Governing Body

Contents

1	Introduction.....	3
1.1	Irish law.....	3
1.2	WIT Policies.....	3
1.3	Definitions.....	4
2	Computer Acceptable Usage Policy (AUP).....	4
2.1	Guiding Principals.....	4
2.2	Rules.....	4
3	System and Network Security Policy.....	6
4	Password Policy.....	7
5	Data Protection – clear screen and desk policy.....	8
5.1	Introduction.....	8
5.2	Policy Recommendations.....	8
	Appendix 1.....	10

1 Introduction

Waterford Institute of Technology (WIT) is committed to providing computing resources including e-mail and internet access, for staff and student use to promote the aims of the Institute and to facilitate education, research and administration. This document constitutes WIT's policies and procedures for the management of computer and network security issues. These policies reflect the ethical principles of the Institute community and outline the responsibilities of those using computer and network services.

In general, the computer resources of the Institute may not be used for illegal acts, for activities in breach of other WIT policies, for activities in breach of software or electronic library licenses, or for personal commercial activity unless specifically authorised. Only WIT staff and registered students or other approved users may make use of WIT computer resources.

All individuals using any of the Institute's computer or network services are required to abide by the terms of these policies.

There are a number of external factors which influence any policy such as this one which include the following:

1.1 Irish law

Users must respect the laws of Ireland and specifically, but not exclusively, be aware of responsibilities under:

- Copyright Act (1963) and as amended
www.irishstatutebook.ie/1963/en/act/pub/0010/sec0056.html.
- Data Protection Act (1988)
www.irishstatutebook.ie/1988/en/act/pub/0025/index.html
- Prohibition of incitement to hatred Act (1989)
www.irishstatutebook.ie/1989/en/act/pub/0019/index.html
- Criminal Damage Act (1991)
www.irishstatutebook.ie/1991/en/act/pub/0031/index.html
- Freedom of Information Act (1997)
www.irishstatutebook.ie/1997/en/act/pub/0013/index.html
- Child Trafficking and Pornography Act (1998)
www.irishstatutebook.ie/1998/en/act/pub/0022/index.html

1.2 WIT Policies

In addition, there are other Institute policies already in place which must be adhered to. These include:

WIT Student Code of Conduct: www.wit.ie/Policies/Student_Rights_Responsibilities.pdf

WIT Dignity and Respect Policy: www.wit.ie/Policies/Dignity_and_Respect_Policy.pdf

1.3 Definitions

Authorised User: Current members of the staff of WIT (whether on a permanent, temporary, contract or visiting basis), external suppliers to WIT and individuals who are currently studying at WIT who are permitted to access the WIT local area network (LAN)

User: A user is a person who uses a computer or network service provided by WIT.

2 Computer Acceptable Usage Policy (AUP)

2.1 Guiding Principals

The rules which follow have been formulated with these goals in mind:

- a) Ensure security, reliability and integrity of the Institute's computer resources, and the computer resources of others.
- b) Avoid situations that may cause the Institute to incur civil liability.
- c) Maintain the image and reputation of the Institute.
- d) Preserve the value of computer resources as a conduit for free expression.
- e) Encourage the responsible use of computer resources, discouraging practices, which degrade the usability of these resources.

2.2 Rules

- a) Users may be provided with accounts and passwords to permit access to the Institute computers and other network resources. Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions that the other party takes with the password.
- b) Access to any WIT system or data is on a minimum needs basis by default and must be approved by a relevant head of function.
- c) Access rights will be reviewed at least once every 12-months and HR will inform Computer Services in a timely manner when employees leave WIT.
- d) All student accounts will expire within 12-months of being issued and only re-enabled once students have re-registered with the Institute for further study.
- e) All staff accounts will be set to expire on the termination date listed on account setup forms. For permanent staff or staff on contracts of indefinite duration, no expiry will be set on accounts. Accounts will fall due for expiry on termination of employment with the Institute.
- f) Once a password has been issued full responsibility for that account and associated password passes to the user.
- g) Users must make use of WIT computer resources in a reasonable fashion. Users must not undertake or facilitate any activity that could jeopardise in any way, the integrity, reliability and performance of these resources. Wilful damage or attempted damage to computer resources will result in disciplinary action which may include prosecution under appropriate legislation. Likewise, deliberately wasteful use of resources and time could lead to a withdrawal of services or disciplinary action.

- h) Users must take reasonable care to ensure that you do not transmit viruses or other malicious computer code to other users or external entities.
- i) It is not acceptable to hack or attempt to hack into accounts or computer resources for which you not entitled to use. Only systems or network administrators can authorise accounts, users may not authorise other users to use accounts.
- j) It is not acceptable to view, download, transmit or store any illegal, offensive, indecent images or material. Nor is it acceptable to attempt to access any files, data or records for which you are not authorised. You may not use WIT computer resources to transmit anything that is illegal, libellous or defamatory or is damaging to another system. Neither may you deliberately misrepresent your views as those of WIT or any other person or organisation.
- k) Software copyrights and licence conditions must be observed. Only licensed files or software may be downloaded from the Internet.
- l) All software installed and used on WIT computer resources, including stand-alone computers, must be appropriately licensed. Where site licenses permit off-campus use and/or personal use, users must adhere to the terms and conditions of such licenses.
- m) Increasing amounts of data and information are stored on electronic media on WIT computer resources. If you have access to, or are responsible for such data, you must ensure that the integrity, accessibility, accuracy and confidentiality of such data are maintained. If you keep personal data (e.g. exam results) on others you must comply with the provisions of the Data Protection Act 1988. You must also be aware that The Freedom of Information Act applies to records held in electronic format.
- n) Users should not leave computers logged in and unattended. You will be held personally liable for use of computers, and for documents and images stored or downloaded from the Internet or other sources, while the computer was left logged in and unattended.
- o) Failure to abide by these policies may result in being denied access to computer resources or disciplinary action where appropriate.
- p) WIT reserves the right to retain logs of computer and network activity on all WIT services and to access these logs for investigative purposes.

3 System and Network Security Policy

The WIT computer network consists of an interconnection of approximately 6,000 networked devices. These include computers, printers, data projectors, door entry and other networking equipment. The Institute depends heavily upon its IT network for research, teaching and administrative activities. It is essential that the stability, integrity and security of the Institute IT network be safeguarded. This policy defines the Institute regulations regarding access to the Institute network. All Users must comply with the following policy statements:

- a) Computer Services at WIT are responsible for the administration of Institute backbone network and primary software domains. The administration of this network including network connections, services, addressing and design is the responsibility of the IT Manager and delegated agents. The IT Manager reserves the right to delegate agents as required.
- b) Access to the WIT network and facilities is restricted to fully authorised Institute users. Users are required to login to an authorised domain using a secure login-name/password combination. Additional authentication mechanisms may be required for other systems as appropriate.
- c) Once a password has been issued full responsibility for that account and associated password passes to the user.
- d) Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions that the other party takes with the password.
- e) Users may not attempt to circumvent user authentication or security of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for the User, logging into a server or account the User is not expressly authorised to access, or probing the security of other networks.
- f) Users may not attempt to interfere with any service to any user, host, or network ("denial of service attacks"). This includes, but is not limited to; "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
- g) Users who violate systems or network security may incur criminal or civil liability. WIT will co-operate appropriately with investigations of violations of systems or network security at other sites, including co-operating with law enforcement authorities in the investigation of suspected criminal violations.
- h) In the event of unacceptable network events occurring on the network, the IT Manager and delegated agents have the right to gain access to and inspect the configuration of devices or equipment on the network and to remove any devices or equipment that they believe could be the source of the problem. Where root access has not been provided to do this, the IT Manager may instruct that passwords are provided or reserves the right to decode passwords to gain access to suspect equipment.
- i) Users should be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon.
- j) Failed access attempts are logged and reviewed. Logs to be kept for a period of 12 months.

4 Password Policy

Username and passwords are utilised in WIT to facilitate access to Institute IT resources. They also protect Institute data from access from unauthorised individuals both internally and externally. This policy applies to all WIT Staff, Students, or third parties who are issued with usernames and passwords for any Institute IT system or device. This policy is the minimum policy which applies to all username and password pairs on all devices, systems and applications that are part of the WIT network and which provide access to Institute owned information. Other password policies may be applied to applications requiring a greater level of security and accountability.

- a) Once a password has been issued full responsibility for that account and associated password passes to the user.
- b) Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions that the other party takes with the password.
- c) Passwords must not be written down and left in a place where unauthorised persons might discover them.
- d) All Users must choose passwords that cannot be easily guessed. For example, a car license plate number, a spouse's name, or an address must not be used. This also means that passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, and slang must not be used.
- e) Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must not employ passwords like "JANUARY" in January, "FEBRUARY" in February, etc.
- f) Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.
- g) Passwords should be changed periodically. Network managers, system administrators or application administrators should select an appropriate time frame for changing passwords taking into account the data or system to be protected and the knock on effects of changing thousands of passwords. For this reason all staff passwords must expire every 90 days and all student passwords must expire within a maximum of 12 months.
- h) To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After a defined number of unsuccessful attempts to enter a password (usually between 3 and 8 per hour), the involved user account must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three (3) minutes, or (c) if dial-up or other external network connections are involved, disconnected.
- i) A password history must be maintained for all domain levels. This history file should be used to prevent users from reusing passwords. The history file should minimally contain the last 7 passwords for each username.

- j) Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover them.
- k) All vendor-supplied default passwords e.g. default passwords supplied with routers, switches or software such as operating systems and databases must be changed before any computer or communications system is used.
- l) Passwords must be a minimum of 9 characters in length.

5 Data Protection – clear screen and desk policy

5.1 Introduction

This policy document is written to provide guidance to all WIT employees in the protection of private information. WIT is obliged under the Data Protection Acts to ensure that personal or private data is protected from misuse. The legislation applies to personal data held in both manual and electronic format. Unauthorised access of an unattended workstation or laptop can result in harmful or fraudulent entries, e.g. modification of data, fraudulent e-mail use, etc. Access to an unattended workstation or laptop could result in damage to the equipment, deletion of data and / or the modification of system / configuration files.

Information can be stored in many forms; piece of paper or a Post-It® note, digital forms such as data stored on a hard-drive, or USB pen or Institute information accessible from computer workstations or laptops. If your screen or laptop is readable when you are absent from your desk or work area, this may result in sensitive information being read and 'leaked' to unauthorised persons. If people can see when a sensitive system is being accessed, it facilitates either pre-meditated or opportunistic attempts to read and copy the data when the PC or laptop is left unattended; even for a short period. Similarly, you should ensure that any private, sensitive or confidential documentation is kept securely and out of sight should colleagues or students be in attendance at your workspace

This policy directs all users of screens / terminals to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentiality. As 'Data Controllers' and 'Data Processors', of personal data, we have key responsibilities and should ensure compliance with these obligations. The end user is the person with the responsibility to ensure the security of data. End users must be especially vigilant when accessing confidential data off campus.

5.2 Policy Recommendations

- a) All users are expected to protect the information for which they are responsible.
- b) Never share your password with anyone.
- c) Lock away all sensitive and valuable documents (paper, DVD, CD, USB pens etc.) in cabinets or desk drawers (as appropriate) when the desk is unattended for an extended period - for example when away for meetings, at lunch times, or overnight.
- d) Ensure that any potentially sensitive, personal or private correspondence is not exposed to the wider public.

- e) Log off computers and windows terminals when unattended by pressing ctrl alt del. At cease of work close down all the applications and log off/shutdown the PC.
- f) Use password protected screensavers with a 10-minute lockout policy. The policy activates a password protected screensaver whenever a workstation is not used for 10 minutes. When a user returns to their computer after that time, they must enter the PC password in order to unlock it. To do this, go to: Start, Control Panel, Display and select Screen Saver. Make sure to tick the “On resume, password protect” option – see Appendix 1.
- g) To quickly activate the workstation lockout facility press CTRL+ALT+DEL and click Lock this computer. However, a windows key combination is even simpler. Press Windows Key + L and your computer.
- h) Remember that it is a fundamental principle that knowledge or possession of sensitive information is to be strictly limited to those Users that have a need to know and have appropriate privileges.
- i) Be aware of positioning your screen so that sensitive information cannot be read by others.
- j) These recommendations also apply to laptops.
- k) Make yourself aware of the WIT Data Protection Policy at:
<http://www.wit.ie/InformationCompliance/DataProtection/>
- l) For further information on Data Protection or if you have any specific queries, please contact the information Compliance officer at foi@wit.ie or visit www.dataprotection.ie

Appendix 1

Setting up password protected screensaver.

