

Advanced User Guide

Internal IT Security Policy and Procedures

This guide is one of a series of "How To" Guides" produced by Enterprise Ireland to meet the needs of Irish companies, particularly our client base, the majority of whom are small to medium enterprises (SMEs) in manufacturing or internationally traded services.

They are designed for non-IT professionals charged with developing and/or implementing eBusiness/IT strategy in their companies. Hopefully they may also be of use to IT professionals.

These guides are only one of a range of eBusiness resources provided by Enterprise Ireland. Most of the other resources, can be accessed through our eBusiness webpages

www.openup.ie

Here you can access more guides and cases about eBusiness and related topics, details of solution providers, access to our free eBusiness e-zine and discussion forum, eBusiness events guide and links to interesting reports etc.

The funding for these guides was provided to Enterprise Ireland by "The Information Society Fund" which was established by Government to progress the objectives of the Government's Action Plan for the Information Society.

INTRODUCTION

The purpose of this document is to provide you with sample policies and procedures, which may be included on formal internal security documentation. Our sample is a combined security policy and security procedures document. However, there is an increasing tendency to have separate documents for "Security Policy", "Security Procedures" and "Security Standards". We should also emphasise that this sample is designed to illustrate the type of issues that need to be addressed rather than necessarily an example of the best way for your company to address them.

Each company should develop their own, more detailed policies, procedures and standards documents, to support their specific business situations and requirements, using independent professional advice where appropriate.

Once your Security policy document has been developed it should be provided to all of your company's computer users and to anyone else accessing your company's computer systems. You may wish to have all agree that they will observe the policy. This can be done by having them sign a piece of paper or by clicking an "Accept" button when they login. A typical wording for the latter is given in Appendix 3.

The document is laid out as follows:

- The main section deals with security policy issues that are relevant to all staff and to third parties accessing your IT network.
- The first appendix contains a summary of current legislation that relates to the use of IT systems.
- The second appendix outlines potential IT set-ups in place relating to security, which are usually primarily the concern of the IT Department.
- The third appendix contains notices that could be displayed on external mail leaving your company or on logon to the network, for example.

Sample Policy Document

Please Note

Non-compliance may lead to disciplinary action being taken.

"Company Name" IT SECURITY POLICY

1 NETWORK ACCESS

1.1 User Identification and Passwords

- * Each user is allocated an individual user name and password. Logon passwords must not be written down or disclosed to another individual. The owner of a particular user name will be held responsible for all actions performed using this user name.
- * Requests for new computer accounts and for termination of existing computer accounts must be formally authorised to the IT Help Desk/relevant IT resource by the relevant manager. Requests for additional access to specific business applications, e.g. Financial Accounts must be authorised in writing to the IT Dept/resource by the relevant application owner.
- * Staff must notify the IT Help Desk/relevant IT resource when moving to a new position or location within "Company Name". This ensures that the necessary setups to provide fast access to the most appropriate mail and file servers can be put in place. Staff are not permitted to take IT equipment such as PCs or notebook computers when moving to another position within "Company Name".

- * Line management must notify IT of staff changes that might affect security. An example of this would be an individual who has access to restricted confidential client information and moves to another role where this access is not required.
- * All user accounts have the following password settings:
 - Minimum password length of 8 characters;
 - A combination of alpha, numeric and punctuation should be used;
 - Users are forced to change their passwords every (insert number) days;
 - Users cannot repeat passwords;
 - Accounts are locked after (insert number) incorrect login attempts.
- * Passwords must not be easily guessed (i.e. names, months of the year, days of the week, usernames, etc. must not be used as passwords).

1.2 Access to "Company Name" Information

- * All information held on the networks including email, file systems and databases are the property of "Company Name" and staff should have no expectation of privacy for this data.
- * Although it is not the general practice of "Company Name" to monitor stored files, email messages and Internet access for their general content, "Company Name" reserves the right to do so for the protection of staff, for system performance, maintenance, auditing, security or investigative functions (including evidence of unlawful activity or breaches to "Company Name" policy) and to protect itself from potential corporate liability.
- * Requests to access the computer account of a member of staff who is absent from the office must be directed to the IT Help Desk/relevant IT resource in writing by the "Relevant Manager". The access is given effect by changing the user's password and allowing the "Relevant Manager" or a colleague to access the account directly. Where this access is granted it must be used for enquiry purposes only.
- * Staff must not issue any information to third parties unless they have authorisation to do so.
- * Users are only permitted to access electronic information and data that they require to perform their duties.
- * If confidential information is lost, either through loss of a notebook computer, backup media or other security breach, the IT Help Desk/relevant IT resource must be notified immediately.
- * All computers must be switched off at the end of the day. This action erases residual information contained in the computer's memory and assists with overnight anti-virus software updates.

1.3 Data Protection Act

- * The Data Protection Act (1988) imposes responsibilities on users regarding the processing of personal data. Personal data refers to data relating to a living individual who can be identified either from the data, or from the data in conjunction with other information held by an organisation. It is the responsibility of all "Company Name" staff to ensure that the principles of the Act are complied with.

A summary of other relevant Irish legislation is included in Appendix 1.

1.4 Personal use of computer systems

- * While "Company Name's" PCs and notebook computers are provided for business use, it is acceptable to use them for a limited amount of personal use. This limited personal use of PCs is permitted provided such use does not a) interfere with the user's job commitments; or b) have a detrimental effect on the computer or network's performance.
- * Staff must not use "Company Name's" systems or the Internet for commercial activities that are not related to the business of "Company Name".

2 PC and NOTEBOOK SECURITY

2.1 General

- * PCs and notebook computers must not be left unattended for long periods while signed-on e.g. during lunch, coffee breaks etc. Users must either logoff or activate a password-controlled screensaver if they are leaving their PC. The screensaver should be set to activate by default after 10 minutes of inactivity.
- * IT equipment must not be removed from "Company Name's" premises unless written approval has been received from the IT Department/relevant IT resource. An exception is made for authorised off-site back-ups providing they are adequately protected against unauthorised access. All notebooks must be signed for before being removed from "Company Name" premises.

2.2 Software

- * Software must not be copied, removed or transferred to any third party or non-organisational equipment such as home PCs without written authorisation from the IT Department.
- * Only software that has been authorised by the IT Department may be used on PCs and notebook computers connected to the "Company Name" IT network.
- * Downloading of any executable files (.exe) or software from the Internet is forbidden without written authorisation from the IT Department/relevant IT resource. Staff may be given this authorisation based on their specific job requirements.
- * Regular reviews of desktop software are undertaken and the presence of unauthorised software will be investigated. "Company Name" reserves the right to remove any files or data from IT systems including any information it views as offensive or illegal.

2.3 Confidentiality

- * Confidential data held on computer media (e.g. floppy disk) must be stored securely when not in use.
- * PCs and notebooks for disposal must have the hard disk 'wiped clean' before they are distributed outside "Company Name"

2.4 Notebooks and Palmtops

- * All reasonable precautions must be taken to protect equipment against damage, loss and theft. The equipment must not be left unattended in any public place. Damage, loss or theft must be immediately reported to the relevant IT resource
- * "Company Name's" notebook computers are protected by the following arrangements (insert details). These must not be disabled.
- * Anti-virus software is installed on all notebook computers.
- * Data must be backed-up to the network on a regular basis and notebook users must ensure that the data on their notebook computers is adequately backed up.
- * Palmtop computers must be set with a switch on pin number and must not be used to store sensitive information.
- * All notebooks must be locked to a physically secure object when in use using the Kensington lock provided. Notebooks must be stored securely when not in use. Staff must not leave a notebook computer unattended at any time when not secured.

2.5 Computer Viruses

- * Corruption of PC's or notebook's data or software by malicious software (e.g. a computer virus or a worm) must be reported to the IT Help Desk/relevant IT resource.
- * Users are not permitted to disable or remove antivirus software under any circumstances.
- * Unauthorised screen savers are not permitted, as they are a potential source of computer virus. If in doubt, please contact the IT Help Desk/relevant IT resource for advice.

3 INTERNET AND EMAIL

3.1 General

- * All staff have a responsibility to use the Internet in a professional, ethical and lawful manner. Users must regard Internet access as a privilege, which can be revoked.
- * Users should exercise caution when making payments over the Internet, as the security of credit card details cannot be guaranteed. "Company Name" will accept no liability for losses arising through the transmission of personal or financial information (e.g. Credit Card numbers) over the Internet.
- * Users must not use "Company Name's" Internet facilities to download, display, generate and/or pass on to others material whether in text, pictures or any other form, which would be regarded as offensive. It is important to note that what constitutes offensive material is not one for the sender to determine - it is the effect on anyone viewing the material that is considered important. In law, possession of some material is deemed to be a serious criminal offence, whether in the workplace or otherwise.
- * All access to the Internet from "Company Name's" network will be via an approved channel that will be secured by a firewall.
- * Users must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, failing to exit from websites, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.
- * Users must not use the same passwords for login to Internet websites as they do internally for "Company Name" systems.
- * "Company Name" reserves the right to review, audit, intercept, access and disclose all access to the Internet. This includes emails sent and received in addition to websites visited and files downloaded from the Internet.

3.2 Email

- * Email users must exercise caution with any external attachments other than those received from a trusted source, as these attachments may contain a computer virus.
- * Users must not represent themselves as another individual in electronic communications.
- * Email users must be aware of the risks associated using email to send confidential or commercially sensitive information.
- * Users must ensure that documents attached to emails are not copyright protected.
- * Email messages must be appropriate and professional.
- * As email is a form of publishing and covered by relevant publishing Acts, libellous and defamatory material is not permitted.

- * Users should be aware of their obligations under the Data Protection Act and must not use email for transmitting data of a personal nature related to a third party.
- * If any person receives email, which they deem to be inappropriate, offensive or illegal, they must inform their "Relevant Manager". Immediate reporting of incidents facilitates more successful identification of the source and other details.
- * All emails that are sent externally must carry a standard "Company Name" disclaimer. Users must not attach their own disclaimers to emails.

4 UNSOLICITED COMMUNICATIONS

(Where software is in place, use these clauses as appropriate)

4.1 Email

- * Software is in place to monitor incoming and outgoing external email messages. Messages that contain text which indicate that they may have come from an unsolicited source are 'quarantined' by the software and an automatic email is sent to the "Company Name" sender or recipient to inform them that a message has been stopped. Please contact the IT Help Desk/relevant IT resource if you receive a quarantine message.

5 TELECOMMUNICATIONS

5.1 Remote access

- * Remote Access can be defined as "Access to "Company Name's" IT resources or data from a location external to "Company Name"". This access may be by a third party or an employee who is located off-site.
- * All notebook computer users must ensure they have remote access software to connect securely to the "Company Name" IT systems.
- * For cost and other security reasons remote connections must be closed as soon as a search is completed.
- * Telephone numbers that are used to access "company Name" computers must not be listed in public telephone directories and must not be disclosed to unauthorised personnel.

6 THIRD PARTY ACCESS

- * Third Party Access can be defined as "The granting of access to "Company Name's" IT resources or data to an individual who is not an employee of "Company Name"".

Examples of third parties include:

- Software vendor who is providing technical support;
 - Contractor or consultant;
 - Service provider; and
 - An individual providing outsourced services to "Company Name" requiring access to applications or data.
- * Third Party Access can only be provided after the Third Party has signed a confidentiality agreement that must be included in their formal contract with "Company Name". "Company Name" staff must never permit another individual to utilise their user name to access the "Company Name" network.
 - * Further requirements for granting Third Party Access are:
 - Risk analysis process;
 - Approval by Data Owner;
 - Approval by the Head of IT/relevant IT resource;
 - * Third party access will only be permitted to facilities and data which are required to perform specific agreed tasks as identified by "Company Name".

7 SOFTWARE LICENCES

7.1 Copyright

- * Copyright stipulations governing vendor-supplied software must be observed at all times.
- * The IT Department/relevant IT resource is responsible for maintaining records of software licences. Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions.
- * All software developed within "Company Name" is the property of "Company Name" and must not be copied or distributed without prior written authorisation from the IT Department.

8 DATA BACKUPS

- * The IT Department must take regular (define as appropriate for your company e.g. daily) backups of the main servers for which they are responsible for managing.
- * Users must always save data and files on the network as opposed to the local hard disk. This ensures that regular backups are taken and are available for recovery purposes. Users should be aware that data saved on the local hard disk is not backed up by the IT Department/relevant IT resource.

Appendix 1 - Legislation

The following is a list of Irish legal acts that relate to the use of IT systems:

- * Child Trafficking and Pornography Act 1998
- * Copyright Act 2000
- * Criminal Damage Act 1991
- * Data Protection Act 1988 & Amendment 2002

This list should not be seen as all-inclusive.

It is the responsibility of "Company Name" staff to make themselves aware of their obligations under Irish law as it relates to the use of IT.

The following is an overview of these Acts, but do bear in mind that the legislation is changing. If you are in any doubt about the specifics of these or other related Acts further information can be found on the Government website at www.irlgov.ie

Child Trafficking and Pornography Act 1998

The making, storage or distribution of child pornography is an offence. In the terms of this Act a child is an individual or the depiction of an individual under the age of 17 years. This includes actual children, cartoon images of children or a combination of either i.e. amending or superimposing a graphic over an image.

If you receive or view any image(s) or media (picture, graphic, booklet, audio tape, video etc.) which depicts a child engaged in or witnessing a sexual explicit act you must report it to the Gardai as this act has a mandatory reporting requirement. There are no exceptions to the reporting requirement. In addition, you must contact the Human Resources Department who will provide assistance in this matter.

Copyright Act 2000

The copying of software or documents, which are copyrighted, is an offence. "Company Name" has a policy whereby only licensed media is used within the organisation. If you require additional software contact the IT Department who will ensure that the relevant licensing agreements are complied with.

Criminal Damage Act 1991

Damage to or threatened damage to data or IT infrastructure is an offence. While in your possession you must take the necessary precautions to protect data and equipment provided to you.

Data Protection Act 1988 & Amendment 2002

The Data Protection Act (DPA) was initially enacted to protect personal information that was held on electronic media. Personal information is data that can be directly related to a living individual. In 2002 the scope of the Act was broadened to cover paper-based information and also to expand the information that is covered under the Act. For example an email address is now considered to be a personally identifiable piece of information and is therefore covered under the Act.

If you have access to personal information you must ensure that it was obtained fairly, is accurate, protected against unauthorised disclosure, used only for the purpose(s) for which it was collected and is held no longer than is necessary for that purpose(s).

Refer to www.dataprivacy.ie

Appendix 2 - IT Dept/personnel SECURITY RESPONSIBILITIES

This section contains policy guidelines, which are the responsibility of the IT Department/relevant resource.

USER IDENTIFICATION AND PASSWORDS

- * All unused usernames must be deleted following an initial period when they are disabled. Line managers must inform the IT Help Desk/relevant IT resource when staff leave "Company Name" to ensure that their usernames are promptly removed.
- * Staff transferring sections within "Company Name" must have their access privileges reviewed and altered based on their new responsibilities, following notification to the IT Help Desk/relevant IT resource by the person moving location.
- * Usernames must conform to the standard "Company Name" naming convention. The convention must be used consistently across all applications and platforms.
- * When the IT Help Desk/relevant IT resource are unsure of the identity of the user requesting a password change, then authorisation must be received from relevant manager before the request is actioned.
- * All "Company Name's" hardware and software must have the vendor-supplied default passwords changed on installation. This applies to test as well as live environments.

ACCESS TO DATA

Emergency file updates

- * Where emergency changes are made to production files or software, these changes must be authorised by line management. The resulting audit trail must be retained.

Auditing and Monitoring

- * All application systems that handle sensitive "Company Name" information must generate logs that show additions, modifications, and deletions to such sensitive information.
- * Operating systems handling sensitive, valuable, or critical information must securely log all significant IT security relevant events.
- * Security reports and audit trails must be reviewed on a regular basis and all violations accounted for.

- * All login screens must include a warning against unauthorised use of "Company Name's" computer systems and a notification of "Company Name's" right to monitor user activity.

Logical access controls

- * The use of privileged accounts (e.g. administrator) must be restricted to authorised personnel only. The passwords must be held securely and their use will be recorded and checked on a regular basis.
- * When end-users have logged in, they should be restricted to menus that show the options that they have been authorised to select. End-users must not be allowed to invoke operating system level commands.

PC and NOTEBOOK SECURITY

Computer Viruses

- * Virus checking must be performed by the IT Department on all software prior to installation or distribution within "Company Name"
- * Virus checking software must be installed on all "Company Name's" PCs and notebook computers and must be automatically executed at system start-up.
- * PCs and notebooks must be updated with virus signature files on a (insert relevant timescale for your company e.g. daily/weekly etc basis.
- * Servers must be updated with virus signature files on a (insert relevant timescale for your company e.g. daily/weekly etc basis.)

TELECOMMUNICATIONS

Remote Access

- * All inbound and outbound communications to Company Name's" private network must be routed through the Demilitarised Zone (DMZ).
- * Where dial-up communications are used, "Company Name's" identity i.e. name or logo must not be revealed until all security validations have been successfully established.

SOFTWARE

Change Control

- * All alterations to system and application software must follow strict change control procedures to ensure the integrity of "Company Name" 's computer systems. For major changes this should include:
 - Authorisation of request for change;
 - Risk assessment of change;
 - User Acceptance Testing;
 - Relevant management sign-off;
 - IT Security sign-off;
 - Roll-back procedures in the event that the change failed; and
 - Documentation of the above.
- * Software development and testing must be carried out on a separate server from the live environment.
- * Adequate controls should be in place over any test data that is used in the testing process, as this data quite often is a mirror of live data.

PHYSICAL SECURITY

The following standards must be applied to (Insert relevant locations for your company)". e.g.

Computer Room Access

- * Access to the Computer Operations rooms must be restricted to authorised personnel only.
- * Third parties who have been granted access to the Computer Operations rooms must be accompanied at all times by authorised personnel.
- * Access to the Computer Operations rooms must be controlled by a physical access control mechanism such as an electronic or combination lock.

Fire detection/prevention

- * The Computer Rooms must be fitted with smoke/fire detectors and fire extinguishing equipment, which should be set to automatic operation when the computer room is left unattended for long periods.
- * Fire detection and prevention equipment must be tested at least twice a year.

UPS/Backup Generator

- * Each production server must have a UPS installed to protect against power surges.
- * The UPS and generator must be tested every x months.

Control of Computer Media and Documentation

- * Computer media e.g. tapes and documentation must be stored securely, e.g. in locked cabinets, when not in use.
- * Magnetic media that is no longer required and which may contain confidential data must be disposed of securely, i.e. all data must be erased or the media must be rendered inoperable.
- * Back-ups of sensitive, critical, and valuable information must be stored in an access-controlled site.

Business Continuity Planning

- * The IT Department/relevant IT resource is responsible for business continuity planning for IT systems. The business continuity plan must be fully documented, maintained and tested on a regular basis.
- * The IT Department/relevant IT resource must make (insert frequency e.g. daily) backups of the main servers for which they are responsible for managing. These backups must be stored off-site for ease of access or should the computer room become inaccessible. The media should be tested for recovery purposes on a regular basis.

Appendix 3 - SECURITY NOTICES

1. External Email Disclaimer

This email may contain information, which is confidential and/or privileged. The information is intended solely for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents is prohibited. If you have received this electronic transmission in error, please notify the sender by telephone or return email and delete the material from your computer.

"Company Name"
Tel: +353
Web: www.companyname.com

This email message has been scanned for viruses.

2. Logon Notice

Unauthorised access to "Company Name's" computer systems is prohibited.

You are reminded that your PC user name and password are for your use only and it is your duty to ensure that they are never made available to others. Actions carried out on "Company Name's" systems will be deemed to be the responsibility of the user name holder. "Company Name" reserves the right to monitor user activity.

"Company Name's" IT security policy covers issues relating to use of the Internet, email, confidentiality of information, personal use of the systems, Irish legislation, physical security of IT assets and software licensing.

By logging on you are accepting that you understand and will adhere to the IT Security Policy while logged on to the "Company Name" network.

Please contact the IT Department/relevant IT resource if you have any queries regarding this policy.

Irish Office Network

Office Telephone

Fax

Address

Enterprise Ireland

Cork	+(353 21) 800 200	+(353 21) 800 201	Rossa Avenue, Bishopstown, Cork.
Donegal	+(353 74) 69800	+(353 74) 69801	Portland House, Port Road, Letterkenny, Co. Donegal.
Dublin	+(353 1) 857 0000/808 2000	+(353 1) 808 2020	Glasnevin, Dublin 9.
	+(353 1) 857 0000/206 6000	+(353 1) 206 6400	Merrion Hall, Strand Road, Sandymount, Dublin 4.
	+(353 1) 857 0000/808 2000	+(353 1) 808 2802	Wilton Park House, Wilton Place, Dublin 2.
	+(353 1) 609 2150	+(353 1) 609 2151	35-39 Shelbourne Road, Dublin 4.
Galway	+(353 91) 735 900	+(353 91) 735 901/2	Mervue Business Park, Galway.
Kerry	+(353 64) 34133	(353 64) 34135	57 High Street, Killarney, Co. Kerry.
Louth	+(353 42) 935 4400	+(353 42) 935 4401	Finnabair Industrial Park, Dundalk, Co. Louth.
Sligo	+(353 71) 59700	+(353 71) 59701	Finisklin Industrial Estate, Sligo.
Waterford	+(353 51) 333500	+(353 51) 333501	Industrial Estate, Cork Road, Waterford.
Westmeath	+(353 902) 87100	+(353 902) 87101	Auburn, Dublin Road, Athlone, Co. Westmeath.

All Enterprise Ireland staff can be contacted at:
first.name.surname@enterprise-ireland.com

www.openup.ie



The programmes of Enterprise Ireland
are co-funded by the European
Regional Development fund.