



An
Phríomh-Oifig
Staidrimh

Central
Statistics
Office

TECHNOLOGY INFORMATION SECURITY POLICIES

CENTRAL STATISTICS OFFICE, SKEHARD ROAD, CORK T12 X00E, IRELAND

Contents

1	Secure Development Policy	4
2	Information Transfer Policy	6
3	Change Management Policy	8
4	Back up Policy	9
5	Disposal and Destruction Policy.....	10
6	Clean Desk and Clear Screen Policy	15
7	Password Policy.....	15
8	Access Control Policy	17
9	Information Classification Policy.....	17
10	Acceptable Use Policy	18
11	Bring your own device policy	27
12	Event Audit and Log review	28
13	Penetration testing methodology.....	30
14	Physical Security.....	32
15	Protect Data in Transit	32
16	Protect Stored Data	35
17	Security Awareness and Procedures.....	35
18	Network security.....	37
19	Anti-virus policy	38
20	Patch Management Policy	38
21	Vulnerability Management Policy.....	42
22	Software Installation:.....	43
23	Cryptography Policy	45
24	Wireless Policy	56
25	Segregation in Networks Policy	57
26	Equipment (IT) Maintenance Policy.....	58
27	Management of Portable Electronic media & USB Access.	59
28	Unattended User Equipment.	63
29	Legislative Requirements which may impact Cryptography.....	64

THIS DOCUMENT IS TO BE READ IN CONJUNCTION WITH THE DATA MANAGEMENT POLICY

1 Secure Development Policy

The purpose of this policy is to define the rules for secure development of software and systems. This policy is applicable to the maintenance and development of all services, architecture, software and systems that are part of the Information Security Management System (ISMS).

This policy applies to all management and operations personnel, suppliers or third parties who work on development or maintenance at the Central Statistics Office.

Secure Development & Maintenance

2.1 Risk Assessment for the Development Process

In addition to the risk assessment performed at a divisional level, the Technology Project Manager must periodically conduct risk assessment of the following:

- The risks related to unauthorised access to the development environment
- The risks related to unauthorised changes to the development environment
- Technical vulnerabilities of the IT systems used in the organisation
- The risk a new technology might bring if used in the organisation

The Technology Project Manager documents these risks in the relevant project documents [Applications Division - Technology Project templates](#).

Security requirements

When acquiring new information systems or developing or changing existing ones, the Technology Project Manager must document security requirements in the relevant project documents [Applications Division - Technology Project templates](#).

Security Requirements related to public networks

The Technology Project Manager is responsible for defining security controls related to information in application services passing over public networks:

- The description of authentication systems to be used.
- The description of how confidentiality and integrity of information is to be ensured.
- The description of non-repudiation of actions will be ensured.

The Technology Project Manager is responsible for defining controls for online transactions, which must include the following:

- How misrouting will be prevented
- How incomplete data transmission will be prevented
- How unauthorised message alteration will be prevented
- How unauthorised message duplication will be prevented
- How unauthorised data disclosure will be prevented.

Checking and validating the implementation of security requirements.

The Technology Project Manager is responsible for defining the methodology, responsibilities and the timing of checking whether all of the Security Requirements of the Security Requirements Specification have been met, and whether the system is acceptable for production. Monthly progress reports detail the current status of each project [Applications Division - April 2019 Progress Reports - Corporate Projects](#) The Technology Division Work Support System is updated on a weekly basis [Eoin McCuirc - Weekly Report\(s\) Reminder](#) recording the time spent on each project. Monthly management meetings are held to review progress with the Head of Division [Eoin McCuirc - FYI - "ITCS Monthly Mgt Meeting - April 2019 - Agenda" in Applications Division....](#)

Repository

Development servers can be found on the Test and Development Network (a separate domain).

Version Control

Version control is maintained by SVN, part of the Software Development Process Flow [Applications Division - Technology Project templates](#) .

Change Control

Changes in development and during the maintenance of systems must be done according to the Software Development Process Flow [Applications Division - Technology Project templates](#) as part of the system development project planning process.

Protection of Test Data

Confidential data as well as data that can be related to individual persons must not be used as test data. Exceptions may be approved by the Technology Project Manager who must define how such test data are protected.

Required Security Training

The Technology Project Manager defines the level of security skills and knowledge required for the development process and the proposed approach (Agile). The Technology Project Manager includes appropriate trainings as part of the Performance Management and Development System(PMDS). Technology Division Applications maintains a repository including a web library and coding standards <https://incubator.cso.ie/weblibrary/index.html#>

2 Information Transfer Policy

The purpose of this policy is to ensure the security of information and software when they are exchanged within or outside the organisation. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all the information and communication within the scope of the ISMS.

This policy applies to all staff at the Central Statistics Office.

This should be read in conjunction with “Section 6.5 – Data Handling Procedures” of the Data Management Policy.

Transfer of Information.

Electronic Communication Channels

The Data Management Policy determines the communication channels that may be used for each type of information and possible restrictions regarding permissions to use the communication channels, i.e. defines which activities are forbidden.

In addition to controls prescribed by the Data Management Policy, the IT Security Officer may prescribe additional controls for each type of data and communication channels based on risk assessment.

Relations with external parties

External parties include various service providers, companies for hardware and software maintenance, companies handling media transactions or data processing, public bodies, information users etc.

Before exchanging information and / or software with any external party, an agreement must be signed, which is the responsibility of the relevant Principal Officer or the Information Security Manager. The agreement may be in paper or electronic form (e.g. Agreeing to terms and conditions) and must contain clauses in line with the risk assessment, including at least the following:

- Method of the identification of the other party,
- Authorisations to access information
- Ensuring non-repudiation
- Technical standards for data transfer
- Incident response
- Labelling and handling sensitive information
- Secrecy
- Copyright

Agreements with external parties must be drawn up according to the Supplier Security Policy.

File Transfer Options:

CSO uses SFTP for the secure transfer of files. SFTP (SSH File Transfer Protocol) creates a secure tunnel through which the data is transferred. For additional security data files should still be

encrypted. We have two SFTP servers - one on the internal Government Network (for use when receiving files from public sector) and one on the public internet.

We recommend this service for those occasions when you have to send/receive large encrypted files which might otherwise have been burned to CD or which would fall foul of email size restrictions.



Filezilla transfer instructions for Staff.docx

(SFTP Server Details ==>[Notes Link](#) - private doc)

Backup Tape movement

The location of each backup tape is recorded in a document on the file server. When a tape is being transferred between sites its location is changed to 'in transit' until it arrives at its destination. Once it arrives its location is again updated to the destination location. The actual transfer happens via An Post EMS in a specially designed tape case with a numbered security seal.

3 Change Management Policy

The purpose of this policy is to define how changes to information systems are controlled. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all the information and communication within the scope of the ISMS.

This policy applies to all management and operations personnel (Officer of Statistics) at the Central Statistics Office.



Change
Management Policy.

4 Back up Policy

The purpose of this policy is to ensure that Backup copies are created defined intervals and regularly tested. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all the information and communication within the scope of the ISMS.

The Back Up Policy is detailed in Section 7.5 of the Data Management Policy.

Backup copies and the process of their restoration must be tested at least once every twelve months by implementing the data restore process and checking that all data has been successfully recovered.

5 Disposal and Destruction Policy

The purpose of this policy is to ensure that information stored on equipment and media is safely destroyed or erased. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all the information and communication within the scope of the ISMS.

This policy applies to all management and operations personnel (Officers of Statistics) at the Central Statistics Office.

Disposal and Destruction of Equipment and Media

All data and licensed software stored on mobile storage media (USB Flash Drive, CD, DVD, memory card... etc.) and on all equipment containing storage media (e.g. laptops, mobile phones etc.), must be erased or the medium destroyed before it is disposed of or reused.

The person responsible for erasing data or destroying media must inform the owner of the asset in question about erasing / destroying data and the asset owner must update the inventory of assets.

Equipment

The IT Service Manager or their delegate is responsible for checking and erasing data from equipment, unless the information security classification policy prescribes differently. Paper documents are destroyed in paper shredders.

Records of Erasure / Destruction must be kept for all data classified as "Confidential". Records must include the following information; information about the media, Erasure / Destruction date, method of Erasure / Destruction person who carried out the process.

All information classified as "Confidential" must be Erased / Destroyed in the presence of the persons authorised to access the information in question of the IT Service Manager or their delegate.

Office Notice 10/2016

An Phríomh-Oifig Staidrimh

Central Statistics Office

CSO Policy on Retention and Secure Disposal of Statistical Data, and Storage Media.

(Note: This Office Notice updates and replaces Office Notice 12/2013 [Notes Link](#) to extend the policy to a broader range of statistical records and electronic media. Survey owners and any staff who are custodians of electronic media need to know and implement this policy. The policy applies to statistical returns - paper and electronic - and to all electronic storage media, including backup tapes, laptops, mobile phones and storage cards.)

1. This policy outlines a standard approach to the retention and secure disposal of statistical data (paper and electronic) and electronic storage media across the Office.
2. The Statistics Act, 1993 requires us to protect the confidentiality of returns to the CSO. For this purpose, we need to have a policy on how long we retain survey / statistical returns and electronic media and how we dispose of them securely. (The disposal periods set out in this notice do not apply to Census of Population records which are retained under Section 35 of the Act.)
3. This policy reflects guidelines from the Office of the Data Protection Commissioner on the secure management of data (*see guidance note appended*).

4. Statistical Data

At every data stage of the GSBPM (Collect, Process, Analyse, Disseminate), a data lifecycle must be implemented including the secure deletion of data when no longer required for statistical purposes. In the interests of enhancing the security of CSO data and safeguarding the confidentiality of our respondents, maximum data retention periods must be determined and documented for each phase of the GSBPM.

4.1 Data at Collection Stage

The following are the maximum retention periods for survey forms, scanned images scanning export files and electronic data sources. After this time paper forms should be securely disposed of and electronic files deleted.

--

Survey or Data Frequency	Paper Forms, Scanned & eForms image files.	Scanning & eForms export files	Electronic Data Sources ~ : Secure Deposit Box, Household Surveys, (CAPI / CATI), ADC,
Monthly	15 periods	15 periods	1 month
Quarterly	5 periods	5 periods	1 month
Annual	5 periods	2 periods	1 month
Biennial	3 periods	2 periods	1 month
5 Yearly	1 period (Scanned image only)	1 period	1 month

Survey owners should specify a data retention policy for each survey input, subject to the maximum periods set out above.

In exceptional cases survey owners may retain returns beyond the specified periods (e.g. returns for a base year might be required for rebasing). All such cases must be documented and notified to the Data Office. The Data Office may seek approval from the CDSC in relation to such cases.

~ *Electronic Data Sources*: Once data has been imported/loaded to a secure central database location or processing system the data transmission files should be deleted. One month is the maximum allowable for this. In addition, ADC management procedures to remove identification data should apply to all data received via the Administrative Data Centre (ADC) portal. Corresponding procedures should be applied to household survey data, to remove identification variables.

As a policy any data lodgement older than one month will be automatically removed from the Secure Deposit Box. A record of the lodgement will be retained as a reference but all attached data files will be deleted.

4.2 Data at Process, Analyse or Final/Disseminate Stage

The retention periods and deletion policies for **Process, Analyse and Final/Disseminate data** should be determined by Data Owners (Heads of Division) taking account of the needs of each survey. The final dataset used for dissemination must be lodged to the Corporate Data Vault. More specific corporate rules on retention and deletion periods will be provided by the Confidential and Data Security Committee (CDSC).

5. Electronic Media

5.1 To reduce the risks associated with the storage of confidential data or official CSO information on electronic media devices the following retention and disposal arrangements are to apply:

Category	Retention Period	Destruction Method (in all cases to be arranged by IT Service Desk)
----------	------------------	--

Backup tapes***	7 years	Secure destruction method
Laptops / desktops / tablets	Until end of life	Hard disk drive to be securely destroyed
Servers	5-7 years	Internal disks to be securely destroyed
All other storage media: Mobile phones, SD cards, USB sticks, CDs, Diskettes, etc.	<ul style="list-style-type: none"> Retention period dependent on lifetime of device; devices no longer in use should be returned to ITSD for destruction. These are not to be used for storage of statistical microdata. 	Secure destruction method
Printers	Until end of life	Hard disk drive to be securely destroyed

The policy of destruction of backup tapes after 7 years will be implemented by ITSD in conjunction with an archiving policy, currently being developed. Measures to ensure that historic backups remain readable by current technology will be applied every 4 years.

5.2 As a once-off step, legacy mainframe reel-to-reel tapes which are currently held in secure off-site storage in Cork will be securely destroyed. The age and condition of these tapes is such that it is technically unlikely that any meaningful data can be read from them. Their existence however presents an element of risk and as such they should be securely destroyed.

6. Survey owners should put procedures in place to ensure ongoing compliance with this policy. Requests to delete electronic files may be logged to the IT Service Desk if necessary. IT Service Desk should also be contacted about the disposal of electronic media devices. Any such media which is deemed end-of-life or which is no longer required should be returned to IT Service Desk who will arrange for its secure destruction and disposal. Disposal of paper returns should be organised with Office Services Unit and must comply with the procedures set out in Office Notice 09/2009 - CSO Policy on the Disposal of Confidential Paper Records [Notes Link](#)

Joe Treacy
Director
Data Protection Officer

Physical Server Destruction Policy

Background: Server reaches End of Life and / or Warranty Expires.

1. Call for Server removal / destruction is logged to the Service Desk
2. Server to be wiped / formatted by rebuilding with Server Installation Disk
3. Any Licencing Issues (with existing software folders etc.) to be deleted if required.
4. All Network cables to be removed from the Server and the Comms Room
5. All KVM Cables to be removed from the Server and the Comms Room
6. All Power cables to be removed from the Server and the Comms Room
7. All Physical Server Disks to be removed from server & disposed of in the media bin provided
8. Server Box to be checked for any identifying labels etc. and removed if present
9. Call logged on Facilities Management Service Desk for Removal of Server Box
10. Server box to be physically removed to Disposals Room (Ground Floor – GE 15)
11. Destruction of Server to be recorded and verified on agreed CMDB
12. IP Address released to Available IP Address List for reuse

Service Licences records to be updated accordingly

Guidance Note for Data Controllers on Purpose, Limitation and Retention of Personal Data

Section 2(1)(c) of the Data Protection Acts 1988 & 2003 which requires data controllers to comply with the following provisions concerning personal data kept by them:

-
- the data shall have been obtained for one or more specified, explicit and lawful purpose(s),
- the data shall not be further processed in a manner incompatible with that purpose or those purposes,
- the data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and
- the data shall not be kept for longer than is necessary for that purpose or those purposes.
-

6 Clean Desk and Clear Screen Policy

The purpose of this policy is to define the rules to prevent unauthorised access to information in workplaces, as well as to shared facilities and equipment. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all the information and communication within the scope of the ISMS.

This policy applies to all staff of the Central Statistics Office.

Please see Section XX of the Data Management Policy

Clear Screen Policy

There is a clear screen policy in effect in the CSO. This policy directs all users to lock their PCs when leaving their desks for a short period or to log off when leaving for an extended period.

In the event of a user not locking their PC, the pc automatically locks after 10 mins. The user will be notified, and security awareness training will be re-given where necessary

7 Password Policy

The purpose of this policy is to define the rules to ensure secure password management and secure use of passwords. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all the information and communication within the scope of the ISMS.

This policy applies to all staff of the Central Statistics Office.

The password policy is detailed in Section 7.2 of the Data Management Policy with the following amendments:

Users are prompted to update their password on expiry. Users are forced by Active Directory Group policy to choose a quality password in accordance with the password management policy.

Enforce Password History = 24

Maximum Password Age = 42

Vendor accounts must only be enabled to facilitate the completion of specific tasks. These accounts must be disabled once the project/work item has been completed by the vendor/service supplier.

It is sometimes necessary to create service accounts in order to facilitate the running of certain software/applications. When an account of this nature is necessary the password must be known only to the relevant IT team and will be entered as requested by a member of that team.

8 Access Control Policy

The purpose of this policy is to define the rules to for access to various systems, equipment, facilities and information based on business and security requirements for access. This policy is applicable to the entire Information Security Management System (ISMS) scope. i.e. to all systems, equipment, facilities and information within the scope of the ISMS.

This policy applies to all staff of the Central Statistics Office.

The Access Control Policy is detailed in Section 7.1 of the Data Management Policy

9 Information Classification Policy

The Information Classification Policy is detailed in Section 5 and Annexe A of the Data Management Policy.

Office Notice 15/2015

An Phríomh-Oifig Staidrimh

Central Statistics Office

Information and Communication Technologies (ICT) Acceptable Use Policy

Part 1 - Introduction and scope

Introduction

This notice sets out the Office policy for appropriate use of ICT facilities in the CSO. It updates and replaces Office Notice 21/2008.[Notes Link](#)

The use of CSO ICT facilities should always be in accordance with this policy and should respect the requirements of all related Civil Service policies. ICT facilities should also be used in compliance with the obligations on statistical confidentiality set out in the Statistics Act.

Need for Rules on Acceptable Usage

The purpose of this policy is to protect the good name of the Office, the security and integrity of its ICT facilities and its electronically stored information, and to prevent misuse of the CSO ICT facilities. ICT facilities present risks including security risks, potential misuse of ICT facilities, lost staff productivity, and potential liability for employers and staff. The Office and staff have mutual responsibilities in relation to ICT security and the appropriate use of ICT facilities. This policy aims to address the risks and the related responsibilities; and to facilitate the provision of an enabling and respectful work environment.

Acceptable use of information assets

Definitions

Information system – includes all servers and clients, network infrastructure, system and application software, data and other computer subsystems and components which are owned or used by the organisation or which are under the responsibility of the organisation. The use of an information system also includes the use of all internal or external services, such as internet access, email, etc.

Information assets – in the context of this policy the term – “information assets” is applied to information systems and other information/equipment including paper documents, mobile phones, portable computers, data storage media etc.

Acceptable use

Information assets may only be used for CSO business needs with the purpose of executing organisation related tasks.

Responsibility for assets

Each information asset has an owner designated in the asset register (inventory of assets). The asset owner is responsible for the confidentiality, integrity and availability of information in the asset in question.

Data management and security

Security of data is paramount within the CSO and confidential data must not leave the CSO by any means except for transfers permitted under the Statistics Act 1993.

Privacy is not guaranteed

Staff should also be aware that information stored or transmitted electronically, such as e-mail, system access logs, and network records, may be considered accessible under Freedom of Information legislation or may be subject to discovery in legal proceedings. Information stored on or transmitted to or from CSO ICT facilities may also be accessed by the Office for the purposes set out in this policy.

Scope of this policy

In the context of this notice, ICT facilities include computer hardware and software; mobile ICT devices and items such as laptops, smartphones and tablets; and any other devices or systems which make use of information and communication technologies. This policy will apply equally to ICT facilities not listed herein or which are introduced at any future date. The use of ICT facilities includes the storage, transmission and communication of any electronic material.

This policy therefore applies to all material stored on CSO ICT facilities and to materials transmitted to or from those facilities. Specific examples of items covered include the use of e-mail, use of the internet and storage of material in electronic format. The policy applies whether the material in question is for personal use or for CSO business purposes. CSO ICT facilities are provided primarily to carry out the work of the CSO. The policy includes rules on the extent to which personal use of ICT facilities is permitted (see Section 2.5).

The policy applies in all places where and at all times when CSO ICT facilities are used. It applies in the case of mobile or tele-working and it also applies to any ICT facilities or material on equipment not belonging to the CSO which are brought into a CSO workplace or which are used in connection with the work of the CSO.

This policy is addressed to all staff of the CSO. It is the responsibility of every member of staff in the CSO to understand and follow the rules set out in this policy. All staff will be required to acknowledge that they have read and accepted this policy. Acceptance of the policy will be a precondition for access to CSO ICT facilities; and staff will regularly be reminded of this policy (see Section 4.4).

Any breach of the rules may result in withdrawal of access to ICT facilities and may also be liable to disciplinary action (see Part 4).

HR Division and IT Service Delivery (ITSD) will implement central aspects of this policy, which will include the use of software to monitor all material stored on or transmitted to or from CSO ICT facilities. All such material will be subject to monitoring at any time, to ensure compliance with this policy and to detect and prevent breaches.

Local managers are responsible for ensuring that the policy is known and implemented throughout the Office. Managers may request ICT usage reports, in respect of their staff, from ITSD. Managers or staff members who become aware of a breach of this policy should notify their supervisor, or contact Personnel or ITSD, as appropriate.

External service providers will also be made aware of this policy and required to indicate their acceptance of it, to the extent that their work involves access to CSO ICT facilities. The CSO Section contracting an external service provider will be responsible for implementing this aspect of the policy.

Part 2 - Rules for Appropriate Use

2.1 Legitimate use of ICT facilities: General rules

The CSO ICT facilities, including e-mail and internet access, may be used only for legitimate business purposes related to your work in the CSO (*other than limited personal use consistent with Section 2.5 below*).

2.2 Except as allowed under Section 2.5 below, **you may not use or attempt to use the CSO ICT facilities for:**

communicating information that is confidential under the Statistics Act, 1993. The divulging of such information is strictly prohibited under the terms of Part V of the Act and is punishable by law.

breaching the CSO's personnel and other rules or breaching the Civil Service Code of Standards and Behaviour Notes Link

accessing blogs or social networking groups e.g. Facebook, Google+,

accessing streaming media sites e.g. YouTube, broadcasters for non-work-related purposes

accessing cloud-based file sharing / repository sites such as Dropbox for non-work-related purposes

using cloud-based development services or systems unless prior sanction has been received from IT

communicating or using any personal information in breach of the Data Protection Act

unlawful activities

electronic sabotage

sending copyrighted material in violation of copyright laws or license agreements

non-official commercial purposes

political purposes, campaigning or advocacy on behalf of organisations or causes

accessing or communicating sexually explicit, offensive, discriminatory or libellous material

harassing, bullying or threatening a colleague or any other person or organisation

personal activities that incur additional costs to the CSO or interfere with staff work performance

profit-making activities

sending anonymous e-mail or other messages or sending messages using another person's account

or imitating another person's identity

any activity which could cause offence or is inappropriate to the workplace

any activity which could adversely impinge on the work productivity of the CSO, overload the IT

network, give rise to legal liabilities for the Office, or bring discredit to the Office forwarding (or

mass-mailing) non-work related material.

The above list is indicative and not exhaustive.

2.3 Courtesy in the use of email and other ICT communications

In general, e-mail and other messages should be courteous, professional and business-like. This applies to external and internal e-mails; and to messages posted on all Lotus Notes Databases. Try to make your contributions as positive and relevant as possible, and keep them polite. Avoid making subjective remarks regarding individuals, teasing, ironic or sarcastic statements, or immoderate language.

2.4 Internet access: General terms of use

The facility to access the internet is provided to staff who need it for official purposes. The internet may be used only for legitimate business purposes related to your work in the CSO (other than limited personal use consistent with Section 2.5 below). This includes work-related duties such as accessing the websites of other national statistical institutes, professional training and education, technical research, services connected to work-related travel, reference material, etc.

2.5. Use of ICT facilities for personal purposes

The CSO ICT facilities are provided primarily for official business purposes. However, their limited use for personal purposes is permitted on condition that it conforms with this policy. Staff are reminded that, as with other Office resources such as telephones, personal use of ICT facilities (such as email or the internet) is a concession. Such use should not impinge adversely on the workplace either in terms of individual work and output, or in terms of ICT system performance.

2.5.1 Internet: News groups, mailing lists or Bulletin Boards

Subscriptions to internet news groups, internet mailing lists, social networking sites or blogging etc unless they are clearly work-related, are not permitted. Posting messages to external groups or bulletin boards other than for work-related reasons is not permitted.

2.5.2 Internet: Remote computers

Some internet services allow users to gain direct access to computers located at remote sites. For CSO work, examples may include systems for transmission of results to Eurostat and accessing EU meeting documentation via CircaBC. You must abide by posted security and usage policies on such sites and any related instructions for their use given by ITSD.

2.5.3 Advertising of goods or services

The limited personal use of ICT facilities includes permission for staff to place small personal advertisements for goods or services on the internal Bulletin Board. Such advertisements and the goods or services offered must comply with law. The CSO offers no warranty or endorsement in relation to goods or services advertised or sold in this way. This privilege may not be used for commercial (i.e. as a trade or profession) sale or promotion of goods or services.

2.5.4 Social or Charitable Activities

The limited personal use of ICT facilities also includes permission to provide information on social and charitable activities. Such activities must comply with law and the Office reserves the right to restrict or limit the use of this exemption.

2.6 Software updating

Only staff from ITSD or authorised by ITSD may install software on the ICT facilities; and only software from the standard CSO toolkit or non-standard Software that has been approved by the Desktop manager and properly tested may be used. Unlicensed (or pirated) software may not in any circumstance be installed or used.

2.7 Security and monitoring controls

Staff may not circumvent, or attempt to circumvent, the security controls and monitoring measures implemented by the Office.

2.8 Passwords

Individual passwords for CSO accounts and systems should never be given to other persons. You may not allow any other person to use ICT facilities and privileges assigned to you.

2.9 Corporate Mobile Devices

If you have a mobile device provided by the Office you must ensure that you adhere to all security procedures advised at the time of issue and do not install any software which is unsuitable or involves illegal activity.

Part 3 - Practical measures to underpin compliance with this policy

This section sets out practical measures taken by the CSO to ensure the optimum running of CSO ICT facilities and compliance with this policy. It includes practical rules and advice which staff are required to follow under this policy.

3.1 ICT security software

ITSD deploys ICT security software across the CSO computer networks and some other ICT facilities. The software packages check for viruses and other malware in incoming and outbound communications; and they similarly scan all files on the CSO network and on desktop or laptop computers attached to the network.

If the virus scanning software on your desktop or laptop computer gives a warning message that a virus or other problem has been detected, please contact ITSD. Do not ignore the problem and do not attempt to solve it yourself.

Software to filter external e-mails for SPAM is provided by an external company. Thousands of unwanted messages are blocked by this system before they reach the CSO; others are quarantined. The system enables staff to check the sender and subject of quarantined messages. Staff may release quarantined messages provided they are satisfied that the message is legitimate. Staff should not release a message if it appears to contain inappropriate contents or appears to contain a hoax, fraud or scam.

Within CSO, attachments to incoming e-mails are also checked for compliance with security and appropriate use requirements (see Section 3.4).

Monitoring and screening software is also applied to internet access. The software restricts access to some categories of sites, to prevent inappropriate use. For some other site categories, access is allowed only outside core working hours, to minimise the impact of personal use on the network. If a legitimate work-related site is blocked by the software, staff may contact ITSD to request that the site be unblocked.

The CSO logs all accesses by its staff to internet sites and an analysis of the log file (which may identify individual usage details) may be made available on the CSO internal computer network. Similarly, a volume analysis of external e-mail traffic (which may also identify individual users) is compiled and made available on the CSO internal network on an ongoing basis to monitor compliance with this policy.

Additional software is being deployed, under the terms of this Office Notice, to check regularly for compliance with this policy and to prevent and detect breaches. This software will be run on an ongoing basis and all material stored on or transmitted to or from CSO ICT facilities will be subject to inspection by the software.

ITSD may deploy such further additional software or methods as are necessary in the light of future ICT risk management needs and technologies.

3.2 Restrictions in size of e-mail messages shipped during the day

In order to preserve bandwidth both on our link with the internet and between CSO locations certain restrictions apply in relation to the size of e-mail messages sent and received:

Size in excess of 100Mb : Not permitted. Sending will fail and a failure report will be returned to you. Staff must not test this out.

Size between 10Mb and 100Mb: Message is held in storage and only shipped between 6 pm and 8 am.

Less than 10Mb: Message will ship as normal.

If you have a business need to send or receive large e-mail or other communications, please discuss this with ITSD to find the best available solution.

3.3 Junk mail, inappropriate mail and hoax messages

The volume and the sophistication of junk mail or SPAM generated worldwide continue to increase. While all SPAM is annoying, the increasing incidence of sexually explicit SPAM is particularly disturbing. CSO takes this issue very seriously. The steps taken by ITSD to block SPAM are described in section 3.1.

In addition to the steps taken by ITSD, staff are advised to do the following to reduce risks:

- Be wary of subscribing to services unless you are confident that they are bona fide and will not subject you to junk mail or sell your email address to others.
- Do not reply to a junk mail message at all ! i.e. Do not reply to junk mail saying you wish to unsubscribe -- this confirms that your email address is correct and may actually have the effect of adding your address to other spammers' lists.
- Don't display your email address in public more than necessary, at least not in a form that's easy prey for scavenger programs that spammers run to "harvest" email addresses from websites, lists of member addresses, newsgroups, etc. Ensure in particular that your email address is not given on the CSO website or on other possible sites such as Eurostat. (It is accepted that it is occasionally necessary to publicise an email address, for example in a tender being posted online.) This remark applies to all constituent pages and content of the website, even extending to attachments in MS Word and Adobe Acrobat (pdf) format. All reasonable effort should be taken to ensure that Section or group email addresses are similarly protected.
- If it is clear from the sender and the subject line that a new mail you received is SPAM, delete it without opening it.
- If you receive an email that contains sexually explicit material or other offensive material, words or phrases, log a call with ITSD so that it can be assessed with a view to blocking similar messages. You should not forward any such e-mail to any other person.
- If you get repeated SPAM from the same source, contact the ITSD HelpDesk to put a block on the sending email address.
- Contact ITSD, via the HelpDesk or otherwise, if you have problems or need assistance in relation to junk mail.

In order to avoid the spread of either malicious or hoax messages the following advice should be strictly observed by all CSO staff members.

You should not forward any virus warnings of any kind to anyone other than nominated staff in ITSD. The vast majority of virus warnings are in fact hoaxes. You should delete them, or, if you believe a warning to be genuine, forward it only to ITSD. It is the job of ITSD to issue virus warnings if required, and therefore no action should be taken on the basis of a warning that comes from any other source.

Similarly, you should not forward any chain or pyramid letters which you receive by e-mail. Such messages generally promise wealth or other rewards if you forward them to several of your friends. Forwarding the message will rapidly clog up in-boxes, so don't do so.

3.4 Email attachments

Many potential problems are associated with email attachments: they can harbour viruses or other means of damaging ICT facilities; they can contain inappropriate content; they can contain very large files, such as video clips, that affect the efficiency of the computer system.

Attachments (Word, Excel, PDF etc.) should not be opened unless you are confident that they came from a legitimate source. If you are in any doubt, you should not open the attachment. If appropriate, contact the sender to verify that the attachment has been sent and to ascertain its suitability and relevance.

If upon opening a file in an Office application such as Word or Excel, you are informed that it contains macros, you should not choose the "Enable macros" option unless you are confident that the file has come from a trusted and known source.

The following procedures are carried out by ITSD Division as a matter of policy with respect to e-mail attachments:

- All incoming email messages are automatically checked for classified attachments (i.e. attachments subject to parking because they may pose a risk to ICT security or to compliance with the appropriate use policy).
- Classified attachments are automatically parked.
- The sender of a classified attachment receives a short automatically generated message from postmaster@cso.ie stating that the attachment was removed.
- The intended recipient of a classified attachment receives a short automatically generated email message stating that an attachment was removed. The filename of the attachment is included in the message.
- If the intended recipient seeks the release of an attachment, he or she should log a call with the service desk and provide details of the sender and datestamp.
- The Postmaster (meaning the person in ITSD attending to the postmaster@cso.ie account at that particular time) will release the attachment. Generally, this will be done within one working hour of receiving the request.
- However, the Postmaster has the right, at his or her discretion:
 - a) to examine the contents of any classified attachment for which a release is sought;
 - b) to refuse to release an attachment that is considered to be a possible breach of rules on policy, security, or appropriate content;
 - c) to consult with his or her superior before a decision is made.
- Unclaimed messages are automatically deleted after 30 days.

3.5 Official communications in unattended e-mail accounts

In the event of a prolonged unplanned absence or other exceptional circumstances, access to a staff member's personal email account may be granted to their manager (or to a colleague if the manager(s) is not available) for official business purposes only, on the authority of at least Head of Division or higher grade as appropriate. Official business purposes in this context means work related material only. A prolonged unplanned absence in this context would usually be an unexplained absence of more than one week. In the event of any such request ITSD will prepare a

report on the numbers, of requests for access under this paragraph and the number of requests granted.

3.6 Standard disclaimer on external email messages

A standard disclaimer notice is automatically added to all e-mail leaving the CSO. This disclaimer includes statements concerning CSO external communications and policies.

Part 4 - Monitoring and Compliance

4.1 Monitoring of compliance with this policy

The implementation of this policy will be supported by specialised monitoring software. Personnel, with the support of ITSD, may directly examine material identified, either directly or indirectly, by the software as needing closer examination regarding compliance with the policy, and related material.

Information stored or transmitted electronically will only be directly examined for the purposes of compliance with this policy if there are reasonable grounds to believe that such information may involve a policy violation or security risk, or if it is necessary for system maintenance purposes. All direct examinations by CSO staff of information stored or transmitted electronically will be logged for subsequent audit and access purposes.

Where necessary, the Office may disclose information relating to breaches of this policy to relevant external authorities.

4.2 Compliance control of postings on CSO Databases

Corporate Support may, either directly or by instructing ITSD, and at their absolute discretion, make any of the following changes to any document whose location or content they consider possibly inappropriate or potentially offensive or otherwise not in compliance with this policy: edit the document in any way; move it to a more appropriate database; recategorise it; delete it. Furthermore, they may make any such changes to relevant response documents, irrespective of whether the response documents respect the rules set out in this policy or not. A record will be kept by Corporate Support of all decisions taken to change documents pursuant to this paragraph and this record will be made available to Personnel.

4.3 Dealing with breaches of the ICT Acceptable Use Policy

Staff who breach this Acceptable Use Policy may have access to ICT facilities or privileges (e.g. e-mail, internet, etc) withdrawn or curtailed and may also be liable to disciplinary action as outlined under the Civil Service Disciplinary Code DF Circular 14/2006 ([Notes Link](#)).

4.4 Acknowledgement of this policy

This policy updates and replaces Office Notice 21/2008. All staff of CSO will be required to accept the contents of this policy and the implications of non-compliance. Acknowledgment should be made by clicking on the button below. For staff with no access to Lotus Notes the acknowledgement slip below should be completed and returned to HRM section.

Circulation

Please bring this Office Notice to the attention of all officers serving in your Section without delay, including eligible officers who are currently on any form of leave not exceeding 12 weeks duration. HRM section will circulate this Office Notice to any officers on leave exceeding 12 weeks duration. Please contact HRM Section if you have any queries in relation to the circulation of this Office Notice.

Marie Creedon,
HR and Finance Manager.
7th October 2015

Acknowledgement

I acknowledge that I have read Office Notice 15/2015 and accept that my use of CSO ICT facilities is governed by this policy.

Officer's Name (Block Capitals): _____

Signed: _____

Date: _____

11 Bring your own device policy

Only devices issued and supplied by the CSO are allowed access the Corporate Network – this applies to PCs, mobiles, tablets.

See Section 7.8 of the Data Management Policy for further information.

12 Event Audit and Log review

This procedure covers all logs generated for systems within the data environment, based on the flow of information product data over the CSO network, including the following components:

- Operating System Logs (Event Logs and su logs).
 - Database Audit Logs.
 - Firewalls & Network Switch Logs.
 - Antivirus Logs.
 - File integrity monitoring system logs.
- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis)
 - The following personnel are the only people permitted to access log files (Domain Admins, Firewall Admins, A/V Admins, SIEM Admins).
 - The following Operating System Events are configured for logging:
 - a. these logs are left at the default OS setting and are overwritten as prescribed under that setting.
 - The following Database System Events are configured for logging, and are monitored by the network monitoring system (CSO to define software and hostname):
 - Audit Logging does not take place.

System and Application logs must at a minimum be set for the default period and monitoring parameters.

AD Auditor software is running on the domain and monitors all AD activity

A powershell script running on a Domain Controller monitors Admin Groups and provides real-time alerts to the AD team if/when any changes are made to same.

- The following Firewall Events are configured for logging, and are monitored by the SIEM managed by SmartTech:
 - a. ACL violations.
 - b. Invalid user authentication attempts.
 - c. Logon and actions taken by any individual using privileged accounts.
 - d. UTM events including blocked and allowed traffic, application control.
 - e. VPN ipsec events
 - f. Endpoint events (FortiClient connections)
- The following Switch Events are logged:
 - these logs are left at the default OS setting and are overwritten as prescribed under that setting
- The following File Integrity Events are to be configured for logging:
 - The One Identity System collects file activity data on Windows file systems. It is currently capable of collecting data on 1 VNX File system
- Real-time copying of logs to a system outside the control of Sys Admins has not been

introduced as a combination of AD Auditor and One Identity activity logging is seen as an adequate deterrent to malfeasance.

- Clock Synchronisation
Our Primary Domain Controller's time is synced with the NTP server (ntp-galway.heal.net)
All other servers times are synced with the PDC.

13 Penetration testing methodology

There are risks inherent in conducting penetration testing over the information systems of the CSO.

When introducing a new system/application IT staff should ensure access is limited to that requested by the business. This should be tested using test accounts prior to release of the new system/application. This should be done regardless of any external penetration testing.

The exact format of the tests will vary but will be agreed with the testing authority and take account of the following requirements.

Additionally, it should be noted for each mitigation measures that will be taken. Examples might be:

Example 1#

Risk: Denial of Service in systems or network devices because of the network scans.

Mitigation measure 1: network scans must be performed in a controlled manner. The start and end of the scan must be notified to responsible personnel to allow monitoring during testing. For any sign of trouble will abort the scan in progress.

Mitigation measure 2: scanning tools must be configured to guarantee that the volume of sent packets or sessions established per minute does not cause a problem for network elements. In this sense, we must perform the first scans in a very controlled way and a use minimum configuration that may be expanded when is evident that the configuration is not dangerous for network devices or servers in the organisation.

- Key staff involved in the project by the organisation may include the following:

Technical Project Manager,
Information Technology Security Officer (ITSO),
Business application owner,

- External intrusion tests will be performed remotely from the supplier's premises. Internal intrusion tests will be conducted in the CSO Cork office. Audit team must to have access to the Organisation's network. It must manage access permissions to the building early enough to ensure that the audit team can access without problems during planning period.
- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organisation, the incident should be brought immediately to the attention of the IT Security Officer and Service Desk Manager responsible for incident management.
- As good practice the scope of the test should include, at least the following:
 - All systems and applications that are part of the perimeter of the production data environment.

Example:

- a) Systems included in the scope

System 1: IP: System: System Description

System 2: IP: System: System Description

Wifi network CSO

.....

b) Applications included in the scope

Application 1: URL: Description of the application

.....

c) Systems excluded from the scope

System 5: IP: System: System Description

System 6: IP: System: System Description

.....

d) Applications excluded from the scope

Application 3: URL: Description of the application

.....

Technical tests must follow the OSSTMM methodology. Tests must be conducted at network, system and application level and must ensure that at least identifies any vulnerabilities documented by OWASP and SANS, as well as those identified in relevant project test plans:

1. Injections: Code, SQL, OS commands, LDAP , XPath , etc.
 2. Buffer overflows.
 3. Insecure storage of cryptographic keys
 4. Insecure Communications
 5. Improper error handling
 6. Cross -site scripting (XSS)
 7. Control of inappropriate access.
 8. Cross - site request forgery (CSRF).
 9. Broken authentication and incorrectly session management.
 10. Any other vulnerability considered High Risk by the organisation.
- For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.
 - As a result of tests performed should generate a document containing at least the following sections:
 - Introduction
 - Executive Summary
 - Methodology
 - Identified vulnerabilities
 - Recommendations for correcting vulnerabilities
 - Conclusions
 - Evidence

14 Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- All employees at the CSO are officially officers of statistics and as such bound to secrecy.
- Employees are responsible for exercising good judgement regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes anonymised data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- Only authorised devices are permitted consistent with the Access Policy and Acceptable Use policy. Authorised devices are listed on QF- Information Asset Register.
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- Personnel using the devices should be trained and aware of handling the devices
- Personnel using the devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- A “visitor” is defined as a supplier, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be signed in, issued a lanyard to be worn at all times on site and escorted by a trusted employee when on site.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on CSO sites. A “visitor” is defined as a supplier, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the external or internal distribution of any media containing data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computers that store sensitive data must have a password protected screensaver enabled to prevent unauthorised use.

15 Protect Data in Transit

All sensitive data must be protected securely if it is to be transported physically or electronically.

- Data must never be sent over the internet via email, instant chat or any other end user technologies.
- The supported method of data transfer is via SFTP
- If there is a business justification to send data via email or via the internet or any other modes, then it should be done after authorisation and by using PGP encryption
- The transportation of media containing sensitive data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

Physical Media is transferred between the 3 Office by means of EMS (Secure mail used by CSO provided by An Post). To ensure the media is kept secure and safe for transit, media is placed in a black case which is robust and well padded. The lock is secured with a Strong Plastic one use security tag with unique serial number. The media number and serial tag are entered into a document and both are checked in on arrival. No tampering can take place without the tag being cut.

The document tape_audit can be found in the following location

\\smfile03\o\$\it_swords\IT_Swords Share

See images of sturdy black case and unique serial numbered tag





16 Protect Stored Data

- All sensitive data stored and handled by the CSO and its employees must be securely protected against unauthorised use at all times. Any sensitive data that is no longer required by the CSO for business reasons must be discarded in a secure and irrecoverable manner.

For details of relevant storage and handling criteria see Section 5 “Data Classification Scheme” of the Data Management Policy”

17 Security Awareness and Procedures

The policies and procedures outlined within must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.

- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing the Acceptable Use Policy.
- All employees that handle sensitive information will undergo background checks (such as criminal and probity screening checks) before they commence their employment with the CSO.
- All third parties with access to data are contractually obligated to become an Officer of Statistics and comply with the CSO secrecy provisions under the CSO 1993 Act. Declarations of Confidentiality must also be completed by contractors and their employers.
- Company security policies must be reviewed annually and updated as needed.

Instructions on how to deal with Malware

All staff have been given IT Security training, the following steps are carried out if a PC is suspected of having malware

- Staff member disconnects the network cable from back of the PC, all networks cables have been tagged with a red label.
- Staff members are instructed during Security Awareness training to phone the Service Desk, if they suspect their PC may be compromised in any way.
- The helpdesk will contact the relevant IT staff to deal with the incident
- IT staff will immediately remove the pc from the network and run an offline scan.
- If Malware is likely or has been discovered the PC will be rebuilt or replaced
- After rigorous testing (i.e. 2 separate scans from 2 different vendors) if IT staff are happy the PC is malware free, the PC will be put back on the network
- The PC will be monitored closely for any further malware activity.

18 Network security

- Firewall must be implemented at each internet connection and any demilitarized zone (DMZ) and the internal CSO network.
- A networking diagram detailing all inbound and outbound connections must be updated after significant changes.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the CSO data environment.
- Appropriate Firewall technology must be implemented where the Internet enters the CSO network to mitigate known and on-going threats.
- All inbound and outbound traffic must be restricted to that which is required for the data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented. (Refer to master Firewall Document on Lotus Notes)
- All outbound traffic has to be Authorised by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented.
- Disclosure of private IP addresses to external entities must be authorised.
- A topology of the firewall environment has to be documented and has to be updated in accordance to significant changes in the network.
- The firewall rules will be reviewed on an annual basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- No direct connections from Internet to CSO data environment will be permitted. All traffic has to traverse through the firewall.

Rules	Source IP	Destination IP	Action

19 Anti-virus policy

In the CSO the antivirus software used is supplied by Kaspersky Labs. This software use signatures, which identifies pieces of code found in a virus. When antivirus software scans a file for viruses, it checks the contents of a file against a dictionary of virus signatures. A virus signature is the viral code. Finding a virus signature in a file is the same as saying you found the virus itself. If a virus signature is found in a file, the antivirus software can take action to remove the virus. Antivirus will then quarantine this file and after 30 days will delete it.

Because new viruses are being created each day, the signature based detection approach requires frequent updates of the virus signature dictionary. Kaspersky Labs release updates every hour but this setting has been configured by the CSO to update every 3 hours.

Antivirus examines files when the computer's operating system creates, opens or closes them. In this way it can detect a known virus immediately upon receipt. ITSD staff can schedule antivirus software to scan all files on the computer's hard disk at a set time and date. This setting has been configured by the CSO to scan every night so as to avoid scanning of pcs during the work day.

The Server tasks are running Anti-Cryptor which uses behaviour analysis to detect and protect shared folders from encryption activity, KSN Usage which delivers a fast response to new threats, Real-Time Protection which is continuously scanning for all malware & Untrusted Hosts Blocking which will block remote hosts' access to shared server files if Real-Time Protection or Anti-Cryptor detects malicious activity

The Desktop tasks are running Device Control which restricts user access to devices, File AV which provides protection from viruses and other threats, Network Attack Blocker which protects the desktop from network attacks, System Watcher which collects data about the actions performed by applications on the desktop and submits it to other components such as File AV for improved protection & Web Control which will block known malicious web sites along with Mail AV which analyses activities performed by an object that may have been downloaded through an attachment and blocked if deemed malicious & Web AV which scans every web page opened and blocks any threats detected.

All servers and desktops are controlled through the KSC (Kaspersky Security Centre) and all settings are password protected which ensures only IT staff can modify settings There are 3 KSC's one for each location with the Master KSC updating on the hour from Kaspersky Labs, this ensures latest updates and signatures are available to the CSO Network.

20 Patch Management Policy

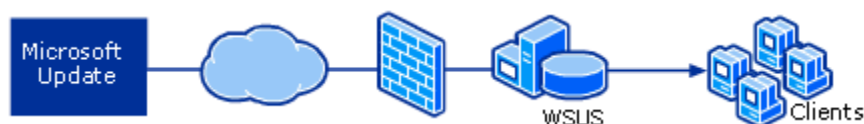
Twice a month, Microsoft release patches which are then downloaded onto the CSO WSUS Server (Dmintra02b)

WSUS provides a management infrastructure consisting of the following:

- I. Microsoft Update: the Microsoft Web site that distributes updates to Microsoft products.
- II. Windows Server Update Services server: the server component that is installed on a computer running a supported operating system inside the corporate firewall. WSUS server software enables ITSD to manage and distribute updates through an administrative console. A WSUS server obtains updates from Microsoft Update.
- III. Automatic Updates: the client computer component built into Windows operating systems. Automatic Updates enables both server and client computers to receive updates either from Microsoft Update or from a WSUS server.

Windows Server Update Services (WSUS) enables ITSD staff to deploy the latest Microsoft product updates to computers that are running the Windows operating system. By using WSUS, ITSD can fully manage the distribution of updates that are released through Microsoft Update.

CSO WSUS Deployment



Updates

Software updates consist of two parts:

- I. Update files: the actual files that are installed on client computers.
- II. Update metadata: the information needed to perform the installation, which includes:
 - Update properties: title, description, Knowledge Base article, Microsoft Security Response Centre number.
 - Applicability rules: used by Automatic Updates to determine whether or not the update is needed on a particular computer.
 - Installation information: command-line options to apply when installing the updates.

In the CSO we download only the metadata during the synchronization, leaving the actual update files to be downloaded after ITSD have approved the update.

The following classifications are downloaded:

- I. Critical Updates: Broadly released fixes for specific problems addressing critical, non-security related bugs.
- II. Definition Updates: Updates to virus or other definition files.
- III. Security Updates: Broadly released fixes for specific products, addressing security issues.

ITSD Staff then go through these patches/updates and decide which are relevant to the CSO and approve or decline as necessary. Only approved* updates are downloaded to the WSUS Server. ITSD staff have configured synchronisation of the WSUS server to Microsoft Update to happen automatically once a day at 3am. Revisions to updates are automatically approved, a revision is a version of an update that has changed e.g. updated applicability rules. WSUS uses the Background Intelligent Transfer Service 2.0 (BITS) protocol for all its file-transfer tasks, including downloads to clients and server synchronizations. BITS is a Microsoft technology that allows programs to download files by using spare bandwidth. BITS maintains file transfers through network disconnections and computer

restarts. New Computers are assigned to groups using the Updates Services Console and are automatically placed in the unassigned computers group. These are then moved to the appropriate groups which have been set up by ITSD staff in accordance with GPO* in active Directory. There are 6 groups in Active Directory and are configured through GPOs to update from the WSUS server at a particular time and day relevant to that computer group.

The allocated time for laptops is 11am every day, this is due to the portable nature of laptops. Due to laptops being encrypted, Microsoft updates can be installed only when a user is logged on.

Groups are as follows:

- I. SUS Computers Cork Tuesday
- II. SUS Computers Cork Wednesday
- III. SUS Laptops Cork
- IV. SUS Servers Cork
- V. SUS Computers Dublin Tuesday
- VI. SUS Servers Dublin

The updates are installed onto a test group of PCs and Servers. These test groups are then monitored and when ITSD staff are satisfied that the patches/updates are successful, updates are then installed on all Servers, PCs and laptops over a phased basis, usually over the rest of the month so that all updates have been installed before the next batch are released from Microsoft.

Occasionally out of sequence patches are released and these are approved and downloaded using the same approach as above unless we have been advised by Microsoft to do otherwise.

- Firmware will be upgraded when required by 3rd party support services.
- **SAN**
- The storage firmware and software are updated periodically as and when advised by the support company. As part of the support agreement the support company takes a proactive role in providing updates and scheduling the application of patches when they become available. A bi-annual health check also takes place as part of the support agreement.
- **Commvault**
- We do not have a schedule in place to update and patch the Commvault system. Service packs and upgrades are applied periodically on the advice of our support partner.
- Any exceptions to this process have to be documented.
- **Server Hardware**
- We do not have a schedule in place to patch firmware versions (BIOS, Drivers etc.) on servers. These are patched when required by a Vendor.

21 Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices.
- As part of the ESS Compliance requirements, CSO will run internal and external network vulnerability scans at least annually and after any significant change in the network (such as new system component installations, changes in network topology).
- Annual internal vulnerability scans must be performed by CSO internal staff or a 3rd party supplier and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities are resolved.
- Annual external vulnerability scans must be performed by an Approved Scanning Supplier (ASS) qualified by ESS. Scans conducted after network changes may be performed by CSO internal staff. The scan process should include re-scans until passing results are obtained.








Policy for handling Smarttech SIEM Incident Reports and Technical Vulnerabilities

- Smarttech log a ticket to the CSO helpdesk with an attached incident report.
- Report is sent to ITSD Cork who analyse it.
- Ticket is sent to the Firewall Team to block web addresses
- Ticket is sent from the Firewall Team to Device & Hosting Team
- Any PC's at risk are immediately quarantined and taken off the Network
- Devices & Hosting follow the recommendations of the report, this usually involves running scans on the PC which has been deemed to be at risk.
- Kaspersky Scan is carried out, if no threats have been found then a Malwarebytes Scan is carried out.
- If no threat has been found, the report is closed and Smarttech notified.

22 Software Installation:

Procedural Document for Installation of Software in the CSO

- All calls for software installations are logged through our service desk.
- Non-standard software calls are sent to the desktop manager for approval with a software approval form attached.
- If the software is new, then a request to acquire new software is sent using the service desk. This form must be filled out stating a business case and if there are licensing costs attached.
- The Desktop manager or Head of Infrastructure Division are the only approvers of non-standard software.
- Standard software installations or upgrades are installed manually or through SCCM and can only be completed by a member of the desktop team or another member of the technology division under instruction from the desktop manager. All software licenses are recorded and tracked by a member of the desktop team.
- All Microsoft software installations have to comply with our Enterprise agreement. Only authorised CSO users are licensed to use Office365, MS Project and Visio.
- PC's are build using SCCM, this is an image which installs the OS onto a PC. At all times we know which OS is installed and on which PC it is installed on

Search					
Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collections
	Windows 10 - 1507	All Systems	2	2	0
	Windows 10 - 1511	All Systems	0	0	0
	Windows 10 - 1607	All Systems	2	2	0
	Windows 10 - 1703	All Systems	0	0	0
	Windows 10 - 1709	All Systems	270	270	0
	Windows 10 - 1803	All Systems	145	145	0
	Windows 10 - 1809	All Systems	1	1	0

- Part of the OS image has a standard set of software, this software is the basic requirement used by staff in the Office.
- Once the new software request form is returned completed to the service desk it is assigned to the AP in charge of Software Deployment. He will consider the request and may ask a member of IT to ensure it is compatible with current CSO software. The AP will then make a decision based on these findings.



Request to Acquire New Software Product

Contact details	
Name:	
Grade:	
Division:	
Software product	
Name of software product:	
Specific version of product:	
Number of licences required:	
Business case	
Reason for requesting product:	
Alternative solutions:	
Long term plans for product usage:	
Cost	
Initial cost of product:	
Lifetime cost of product:	
Support issues	
Compatibility of product with the existing CSO IT operating systems:	
Level of support required from IT divisions:	
Additional Information	
Additional information to support request:	

Software Audits are run on a regular basis and software that is not used after a certain period of time will be removed. Software Audits can be found in the link here

[IT Service Delivery - Kaspersky Application Registry Reports converted to Excel](#)

23 Cryptography Policy

Information

This policy sets out the cryptography solutions available and the key management procedures with each product.

Applicability

This applies to all staff who use encryption.

A.10.1 Cryptography Controls

Objective

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A 10.1.1 Policy On The Use Of Cryptography

Where Cryptography should be used

The ISMS Asset Management Policy and the associated ISMS Asset Handling Criteria will specify the information assets and situations that require the use of cryptography.

Situations requiring Cryptography

Backups/Media – Where information is being backed up to another media (disk, CD, DVD, USB, Tape etc.) the requirement for cryptography will be specified. Distinctions may be made for media that is remaining within CSO, media that is going to contracted backup handling companies or to 3rd party data handlers.

Transmission – As per Control A.13.2.1 – Information Transfer Policies and Procedures - where information is being transmitted across a network. Distinctions may be made for internally transmitted and externally transmitted data.

Note that guidelines in the ISMS Information Exchange Procedure must also be adhered to.

Product Set

The currently available approved product sets using cryptography are listed in the attached appendices.

A.10.1.2 Key Management

The key management procedures for each approved product set are listed in the attached appendices.

As per Control A.18.1.5 – Regulation of cryptography – Cryptography controls shall be used in compliance with all relevant agreements, legislation and regulations.

Product selection will be carried out by Security & Networks. All appropriate public procurement rules will be followed.

Products will be reviewed at least annually by Security & Networks to re-evaluate them in terms of: -

- Key strengths
- Available version upgrades
- Appropriateness of deployment
- Key management

Appendix A- SSL Certs

Description

This is a standard internet feature for providing encryption during transmission between 2 points. Where required (i.e. all sites requiring the input of data) all websites are secured using SSL technology. All keys are 2048bits and SHA-2 compliant.

Deployment Considerations

Certs (other than for sites using the wildcard) need to be purchased in advance,

Suggested deployment

Should be used for all secure transmissions across a network.

Key Management

CSR Generation

CSRs are generated by the relevant server or application owner and provided to the Network Manager (or appropriate deputy)

SSL Cert Requests

Requests are submitted via the appropriate vendor channel and completed key packages are distributed to the server/application owner.

Key Management & Backup

Responsibility lies with the generator of the original CSR.

Key Expiry

- Varies depending on use case – minimum 1 year, maximum 3 years.

Key Strength

The SSL certificates themselves are 256 bit sha2 RSA encrypted certificates.

Appendix B - Secure FTP (BiteVise)

Description

This is usually accomplished over the internet (using https websites) and involves the sender authenticating themselves to the recipients' servers and initiating the transfer process. As this mechanism uses the SFTP protocol the data is encrypted while transferring between the two parties. The server will acknowledge a successful transfer of the file.

Use Case

Currently separate servers are hosted with access from Government Networks and the wider internet. Primarily used for small scale/ad hoc transmissions but a number of inbound transfers have been automated (e.g. GRO and AGS).

Key Management

Keys are generated and managed as per document held in Lotus Notes

IT Service Delivery - Encryption Packages used in CSO file transfers
--

Appendix C - Bit Locker

Description

This software used for encrypting disks comes as part of Windows Enterprise.

Deployment Considerations

Once off deployment and encryption of disk required.

Suggested deployment

Should be used for all laptops and selected important desktop PCs. Documented as part of the build documentation for laptops/windows tablets.

Key Management

Generation

S/W product generates the key based on Computer name & recovery account names.

Distribution

The S/W product is distributed to the computer by software delivery and the encryption mechanism initiated after delivery.

Storage

On completion of the encryption a recovery key is written back to a network share on cbfile01 (or onto usb stick for non-networked devices and thence to cbfile01)

Backup

Backed up via the normal server backups.

Access

Access is restricted to the Devices & Hosting and Networks and Security teams

Lost key recovery

Recovered from excel document detailing keys.

Key Expiry

The key doesn't expire.

Key Strength

AES256

Notes:

Windows 7 - BitLocker is front loaded - requires a password. If the password is input incorrectly 3 (three) times a warning appears. Five incorrect password attempts mean that the extended bitlocker key is required. Following the application of this extended key, the tpm must be reset. This can only be done by IT personnel who have access to the tpm and extended bitlocker details.

Window 8.1 - BitLocker is not front loaded. No tpm exists. Sec.pol/Local Policies is configured with maximum number of machine account lockout threshold attempts. This is set at 5 (five) for Interviewer tablets. It is set at 10 (ten) for laptops.

Windows 10 - BitLocker is not front loaded. No tpm exists. Sec.pol/Local Policies is configured with maximum number of machine account lockout threshold attempts. This is set at 5 (five) for Interviewer tablets. It is set at 10 (ten) for laptops.

Appendix D - GnuPG Encryption

Description

This is a software package for encrypting files. Used via a GUI called Kleopatra.

Deployment Considerations

Pre-exchange of keys required.

There are no licensing costs involved.

Suggested deployment

Through a setup.exe on cbfile01 for internal staff, instructions forwarded to outside departments on key creation and usage of Kleopatra. Also used for Eurostat dataset encryption.

Key Management

Generation

S/W product generates the key based on random string of characters/mouse movement.

Distribution

Each party exchanges their public key by secure email or post.

Storage

The Networks & Security Team holds the key on a private file share.

Backup

The file share is backed up by the normal file server backup regime (cbfile01 backup schedule).

Access

The Networks & Security Team have access to the key on the private file share.

Lost key recovery

The key can be recovered from the file share.

Key Expiry

Keys are set to not expire. Will only need to be recreated if user forgets the decryption password.

Key Strength

AES 256

Appendix E - 7Zip Encryption

Description

This is a software package for encrypting files.

Deployment Considerations

7Zip is available to all users

Suggested deployment

Should only be used for local applications.

Key Management

Generation

Password is assigned by the end-user.

Distribution

Password is distributed by the end-user.

Storage

No key involved. Password is stored by the end-user.

Backup

No key involved. Password is backed up by the end-user.

Access

No key involved. Password is stored by the end-user.

Lost key recovery

No key involved. Password may be recovered by password cracking S/W

Key Expiry

Key doesn't expire

Key Strength

AES256

Appendix F - Microsoft Office File Encryption

Description

This is a software package for password protecting files.

Deployment Considerations

This is a relatively easily cracked password protector. Cracker S/W is readily available on the internet.

Suggested deployment

Should only be used for internal use.

Key Management

Generation

Password is assigned by the end-user.

Distribution

Password is distributed by the end-user.

Storage

No key involved. Password is stored by the end-user.

Backup

No key involved. Password is backed up by the end-user.

Access

No key involved. Password is stored by the end-user.

Lost key recovery

No key involved. Password may be recovered by password cracking S/W

Key Expiry

Key doesn't expire

Key Strength

N/A – Password only.

Appendix G – Commvault Backup Encryption

Description

As LT06 tape drives support hardware encryption this option was chosen

Deployment

All tapes are encrypted as part of the 'copy to tape' storage policies

Generation

Commvault generates a different random 128 key for every data chunk it writes. Each job can contain multiple chunks, so each backup job can have multiple randomly generated keys.

Key Storage

The Key is encrypted and stored in the CommServe database.

When data chunks are pruned (erased), the database entry and the associated key for that data chunk is deleted. Open keys in memory are deleted using memset.

Key Recovery

For disaster recovery, keys are backed up regularly scheduled export and backup of the CommServe Database (DR Backup task).

Key Strength

The cipher used on the keys is Blowfish-128

Appendix H – Site to Site VPNs

Description

This is a standard internet feature for providing encryption during transmission between 2 points.

Deployment Considerations

Needs to be configured in advance of use.

Suggested deployment

Should be used for all secure transmissions between sites that require ongoing connectivity.

Key Management

Generation

Done via the use of a shared secret and the following parameters:

Backup

Backed up by the normal firewall backup

Access

Setup documentation is stored securely in Lotus Notes – Private Document with access only to Firewall Team.

Key Strength

XXXX

24 Wireless Policy

- Installation or use of any non-corporate wireless device or wireless networks intended to be used to connect to any of the CSO networks or environments is prohibited.
- Only approved CSO Corporate Devices (i.e. devices purchased by the CSO) are allowed to join the CSO wireless Network
 1. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
 2. Any other security related wireless supplier defaults should be changed if applicable.
 3. An Inventory of Authorised access points along with a business justification must be maintained. (See Information Asset Register)

25 Segregation in Networks Policy

VLANS & SWITCHES

1. Switches are installed and racked in secure comms rooms on all three CSO sites.
2. All core switches are password protected with access limited to authorised IT staff and support engineers.
3. Access to the Comms rooms is by flexi card with access privileges updated by Facilities Management in Cork. Access requests are decided at HEO or AP level in the IT area and communicated to Facilities Management.
4. Traffic on the Switches is segregated by VLANs with separate VLANs for data and voice. Further segregation is achieved with users spread over multiple VLANs with unique DHCP scopes for each VLAN. Servers and other ancillary equipment are on a separate VLAN. The use of multiple VLANs with divergent DHCP Scopes helps to mitigate against broadcast storms.
5. The Test and Development network is on a separate switch and connected to the Production network by patch cable.
6. Support contracts are in place for all Switches.
7. Patching of Switches is done in consultation with our support Engineers and only proven and stable patches are applied.

26 Equipment (IT) Maintenance Policy

Server Maintenance etc. documents are stored under the following location

\\cbfile01\CSS\User(Public)2\Paperwork\Licensing\

These are currently compiled and maintained by Angela Horgan ITSD Cork

Under this location there is a Folder for each Licensing Year (e.g. Licensing 2018) and under this location there are the following documents

1. Licensing Year - With the 4 Quarter Warranties for that year listed
2. Licensing Projections - With all the renewals for the particular year
3. Servers Per Rack - Which Lists all Physical Servers in the Cork Comms Room at that time:
4. Quarter "X" Renewals - Which lists the next Quarter Servers for Warranty Renewal or Server Replacement.

(Servers are Currently purchased with a 5 Year Warranty)

Procedure for Server Maintenance:

We contact the Server "Owner" and find out if the server warranty is to (a) be extended or (b) the server replaced or (c) the server decommissioned.

The maximum term for server warranty extension at the moment is up to 7 years.

(a) If the warranty is to be extended, then the relevant company providing the warranty is contacted and a price obtained for either a one- or two-year extension

The price is checked and if "reasonable" then the warranty is extended, and the server continues in operation

(b) If the server is to be replaced, then a "REQUEST FOR SERVER" is required from the Server Owner and a price is obtained for the new server instead. \\cbfile01\CSS\User(Public)2\Paperwork\Forms\

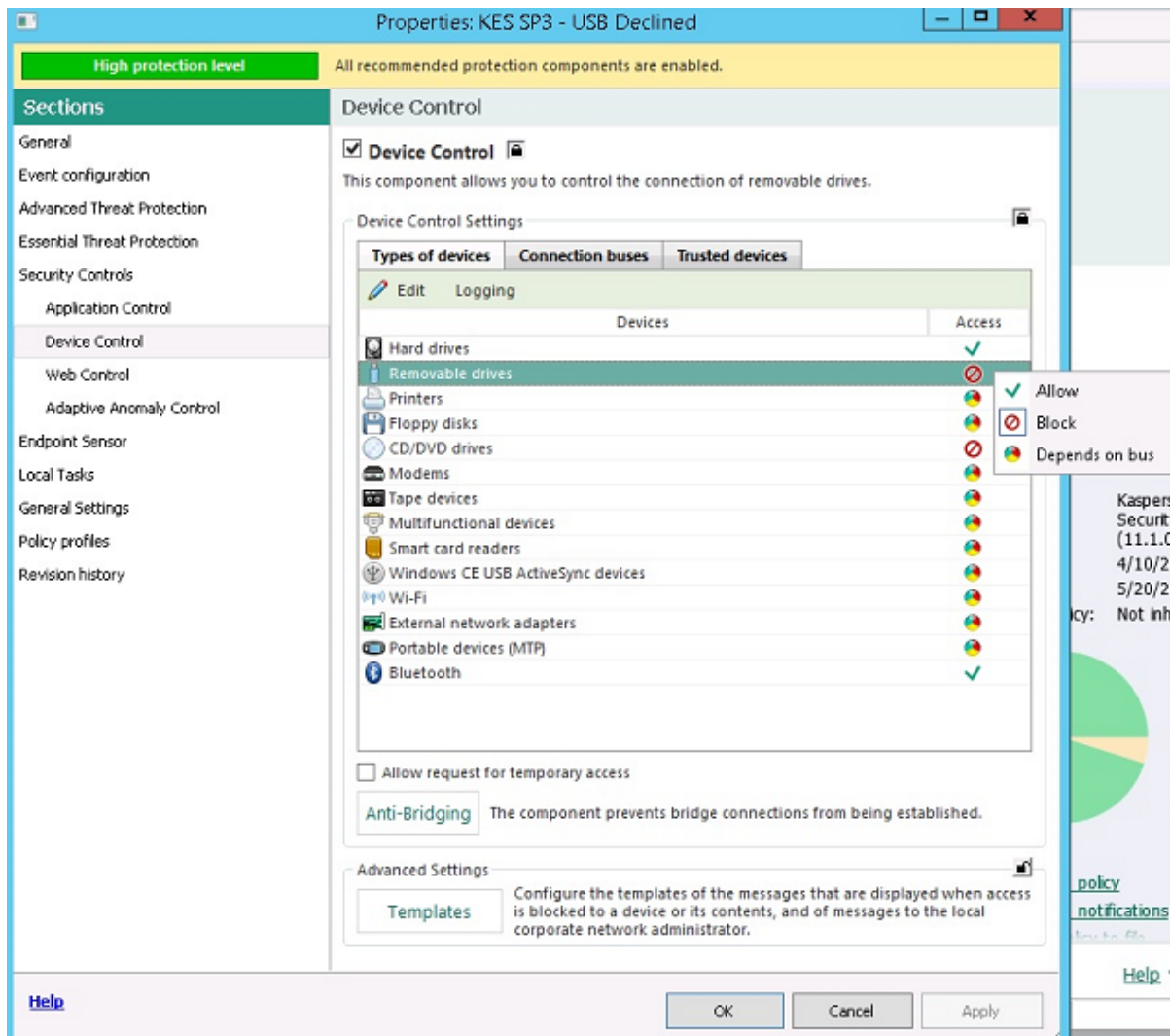
(c) If the server is to be decommissioned, then this is recorded on a Service Desk Call and the Physical Server Destruction Policy is followed (see Section 6 Disposal and Destruction Policy).

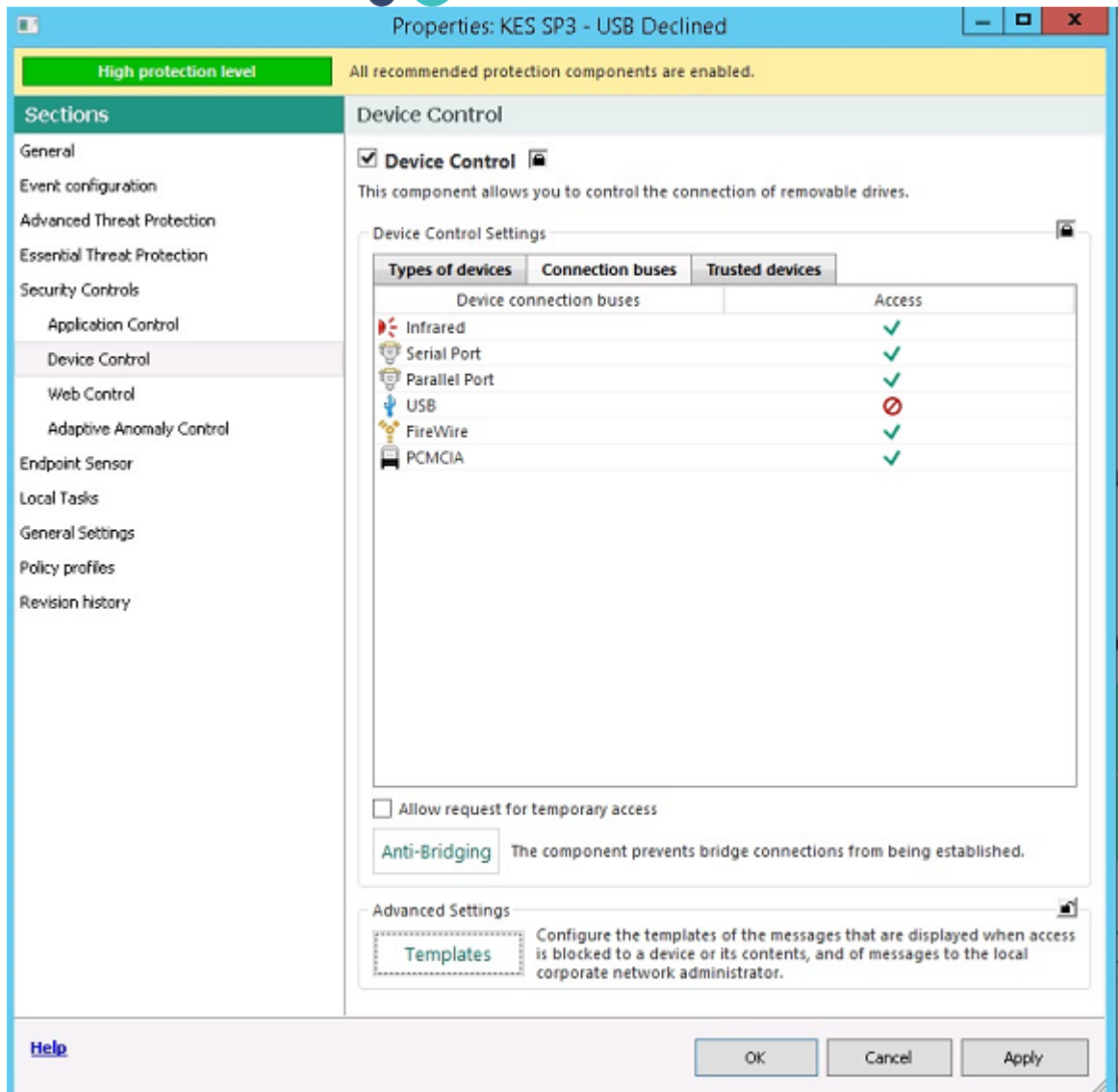
27 Management of Portable Electronic media & USB Access.

When PCs are built they are put into a security group in Kaspersky Security Centre which manages the lock down of all removable drives. There are two security groups, one which allows access to media drives and the other which does not allow access. The default for all staff is for their media/removable drives to be locked down. In order for the drives to be opened, a business case must be submitted to the service desk by the head of division of the staff member requesting this. Once this request is submitted the case is examined by the AP in charge of hosting & devices and a decision will be given. In the case of approval, the PC is then put into the allowed group. A record of all user requests is kept on the Service Desk and also on Lotus Notes see link

[IT Service Delivery - Business Cases for USB Access](#)

See below screen shots of the Kaspersky Security Group which locks down all removable drives





(From Office Notice 13/2013)

CSO Policy on the use of portable electronic media.

1. This notice sets out rules on the use of portable electronic media in the CSO.
2. For the purposes of this Office Notice portable media includes:
 - mobile ICT equipment such as laptop, tablet, mobile phone, PDA, iPod or similar device
 - storage media such as CD, DVD, USB stick, memory card, diskette, magnetic tape, external or removable hard drive
 - any other portable device capable of storing or transmitting information in electronic format.
3. Confidential or personal information may not be held, copied or transmitted in any format outside the CSO.

4. Confidential or personal information may not be held on or copied onto any portable media device, or any desktop Local Disk (C: drive).

5. Limited exceptions to the above for backup and other business purposes are specified in this Office Notice. No other exceptions are allowed.

6. Control of USB and other communications ports -

By default, USB and other ports on CSO desktop and laptops are not enabled. The reason for this is to protect data security and to reduce the risks from viruses and other malware.

7. If there are genuine business reasons for doing so, IT Service Delivery may:

a) temporarily enable the USB or other communications port on a user's desktop or laptop,
OR

b) copy information to/from a portable storage device.

All requests for a) must be logged via the IT Service Desk with a business case authorised at Head of Division level or above. USB & communications ports will only be enabled for a specified purpose and limited period (maximum three months) after which the ports will be automatically disabled.

All requests for b) must be logged via the IT Service Desk at AP/Statistician level or higher and must also be accompanied by a declaration (Appendix A) that the release of the information outside the CSO is in compliance with the Statistics Act and Data Protection Acts.

A record of PCs and laptops with enabled USB ports will be maintained by IT Service Delivery.

Officers using portable storage media should satisfy themselves that the media and content is from a trusted source and has not been compromised.

8. All use of portable media devices must comply with this Office Notice and with the Statistics Act and Data Protection Acts. Attention is also drawn to the rules on the Retention and Disposal of electronic media as set out in Office Notice 12/2013 ()

9. Exceptions:

(i) System or network backups to portable media as administered by IT Service Delivery.

(ii) Encrypted USB sticks used by CSO Household Survey Field Staff and Tourism Enumerators. These encrypted USB sticks are provided by CSO IT for the specific purpose of backing up CSO field data and should not be used for any other purpose or used on non-CSO devices.

(iii) Census of Population POWSCAR data (i.e. Census commuter datasets for research purposes) may be transmitted to licensed users on CD or similar media. The use of POWSCAR data is controlled under Section 20(c) of the Statistics Act and is subject to the procedures on Research Microdata Files set out in Office Notice 06/2011.

(iv) Disclosure of personal information required by law (e.g. provision of data for Eurostat or C&AG Audit).

(v) CSO email systems accessed on CSO devices provided for mobile working as set by IT Service Delivery.

10. Information, compliance and audit.

Section managers are requested to ensure that staff are familiar with and comply with the requirements of this Office Notice.

The CSO may, from time to time, audit the implementation of this Office Notice, to confirm compliance and support good practice.

Managers should bring this Office Notice to the attention of any staff who are not on Lotus Notes and/or those who are on annual, sick or other forms of leave.

Appendix A - Request to IT Service Desk to copy information onto portable media

All requests to IT to copy data onto portable media must include an authorisation form. This must be completed at AP/Statistician level or higher and attached to the IT Service Desk request.



Authorisation to
copy data to portab

Joe Treacy Director

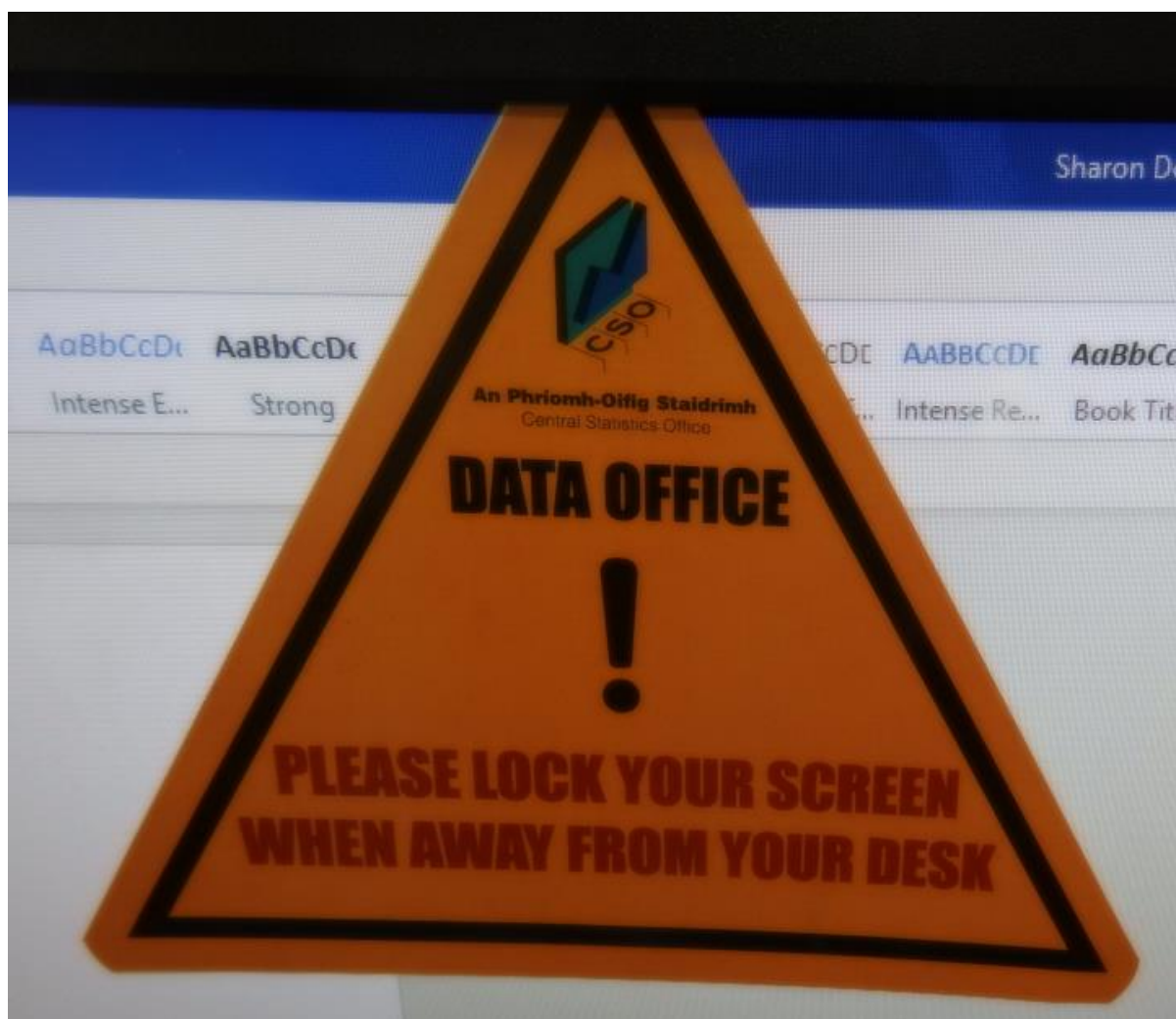
IT and Corporate Services

28 Unattended User Equipment.

The CSO has a Clean Desk Clear screen policy in place. Staff are regularly reminded to lock their PCs if they are going to be left unattended. Staff have undergone Security Awareness training sessions and posters have been put in strategic places such as beside printers, flexi clocks, canteen etc.

Staff ID cards are provided to all staff and must clearly be worn otherwise staff members cannot access the building. The cards double as swipe cards which open and close the main building doors. Only IT staff have access to Comms Room etc using the swipe cards.

See below an example of reminders given to staff



29 Legislative Requirements which may impact Cryptography

References Legislative

International Standards

- ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements.

- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management

- ISO/IEC 27005: 2008 Information Technology – Security Techniques – Information Security Risk Management

- ESS European Statistical Specifications

- Data Protection Act 1988 and Amendment Act 2003
- The Electronic Privacy Regulations 2011 (S.I. 336 of 2011) giving effect to the EU ePrivacy Directive 2002/58/EC
- The Criminal Damage Act 1991, Section 2,3,4,5
- The Criminal Justice (Theft and Fraud Offences) Act 2001, Section 9
- Child Trafficking and Pornography Act 1998
- British-Irish Agreement Act, 1999, Section 51 – Data protection in cross-border bodies
- Companies Acts 1963-2013
- Electronic Commerce Act 2000
- Copyright and Related Rights Act 2000
- Defamation Act 2009
- Consumer Protection Act 2007
- EC (Protection of Consumers in respect of contracts made by means of distance communication) Regulations 2001
- Employment (Information) Act 1994
- Employment Equality Acts 1998 and 2004
- Unfair Dismissal Acts, 1997 to 2001
- European Convention of Human Rights Act 2003

Others which may be worth reviewing:

- Communications (Retention of Data) Act 2011 – for Internet and Telephone Service Providers
- Freedom of Information Acts 1997 and 2003 – for public sector bodies
- The Official Languages Act 2003 – for public sector bodies
- Offences Against the State Act – Section 30
- The Convention on Cybercrime