

**Gambling Commission Information
Security Management System (ISMS)
policy**

November 2010

Version 4.11

Document version control

This document is owned by the Head of ICT

Date	Changed by	Summary of changes made	Version number
10/08/2006	T Boland	Draft	1.0
18/10/2006	A Quigley	Final Edit	2.0
10/04/2007	T Boland	Live	3.0
12/02/2008	T Boland	Updated	4.0
10/12/2008	T Boland	Updated	4.3
08/01/2009	A Quigley	Updated	4.4
07/05/2009	A Quigley	Updated	4.5
09/09/2009	M Goddard	Post-audit updates	V 4.6
18/10/2009	T Boland	Revised	V 4.7
26/10/2009	L Wintle	Updated/Formatted	V 4.8
24/11/2009	M Goddard	Para 5.5.4 updated	V 4.9
05/01/2010	M Goddard	Paras 4.1.4 and 4.5.13 updated	V 4.10
29/06/2010	M Goddard	New para 4.2.2 and amended para 4.7.3	V 4.11

Contents

1	Summary	4
2	Scope	4
3	Forward	4
4	Information systems security	6
	End user equipment	
	Software	
	System and data access	
	Virus protection	
	Use of passwords	
	Use of email	
	Internet access and use	
	Protecting systems and network equipment	
	Use of telephone systems	
5	Physical security policy for the protection of assets	18
	Physical security	
	Access cards	
	Identity badges and visitor security	
	CCTV	
	Document security/clear desk	
6	Breaches, exemptions and logging	21
	Security breaches	
	Logging	
	Exemptions to security policy	

1 Summary

- 1.1 This document details the ISMS (Information Security Management System) policy for the Gambling Commission (the Commission).

2 Scope

- 2.1 All permanent employees, contracted employees, contractors and third parties working on behalf of the Commission that have or are likely to have access to Commission premises and information processing systems either on-site or remotely.

3 Forward

- 3.1 The Commission attaches great importance to the security of its physical assets, its information processing systems and the information that they contain. 'Information processing systems' means any system owned and/or used by the Commission, its employees and any third parties engaged by the Commission.
- 3.2 The ISMS policy shall be communicated to all employees and relevant internal parties, subject to appropriate management authority.
- 3.3 The Commission's ISMS and ISMS policy shall cover the whole of the organisation, including all business processes, offices (including homeworking locations), assets and technology and no exclusions shall apply unless agreed (see section 6.3).
- 3.4 The objective of this policy is to underpin the confidentiality, integrity and availability of all of the information assets within the Commission's ISMS, as defined by this policy.
- 3.5 The objectives and principles of this policy underpin the Commission's approach to information sharing.
- 3.6 This policy is supported by the Commission's senior management, has been approved by the Commission's Board and is managed by the Information Asset Group. The group is responsible for supporting the goals and principles of information security and business continuity in line with the business strategy and objectives.
- 3.7 The Group shall review and approve this policy annually on or before the stated review date, or sooner if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness.
- 3.8 This policy supports the Commission's Information Risk Policy which defines the Commission's approach to information risk assessment and risk management, as well as setting out how the Commission identifies security controls and security control objectives. The Information Risk Policy is consistent with the Commission's wider Risk Management Framework Guide.
- 3.9 This policy supports the Commission's compliance with its legislative, regulatory and contractual requirements and is underpinned by other key organisational policies (listed below).
- 3.10 This policy is a key constituent part of the all employees' induction and ongoing information security awareness, training and development within the Commission.
- 3.11 Employees are required to take personal responsibility for protecting the Commission's information assets from security threats by complying with our security policies and procedures and challenging or reporting breaches of security. Line and process managers

are required to protect the Commission's information assets from security threats by ensuring all persons with access to them are aware of their organisational security role and responsibilities and are motivated and trained to achieve these.

- 3.12** Our ability to maintain our reputation, and the levels of service to our customers, depends on the highest standards of professionalism and integrity. It is paramount that these standards include the way in which we use and protect our assets, information and information systems. Any loss of confidence in our ability to provide these services could cause our organisation to suffer. New technology exposes the Commission to new and potentially greater risks because much greater reliance is placed on automated systems and because of the extensive use of networked computers. We want to reap the benefits of the new technology but we will not take unacceptable risks to do so. It is the policy of the Commission to secure our physical assets, information and systems in a manner which meets or exceeds accepted best practice. We will ensure the continuity of our business operations and manage business damage by the implementation of controls to minimise the impact of security incidents.
- 3.13** It is our policy to ensure that:
- all data is appropriately protected and is not divulged to any third party without appropriate authorisation
 - the premises are protected by suitable physical security and environmental controls, and where appropriate, access is restricted to authorised employees
 - confidentiality and integrity of all information is maintained; information is accessible to all employees according to business need and is protected against unauthorised access
 - access to organisational data and personal data is appropriately controlled
 - contractual, regulatory and legislative requirements are met
 - a business continuity plan is devised, tested and maintained
 - all in house systems development is appropriately controlled and tested before live implementation
 - all employees are provided with training in information security awareness and individual responsibilities defined
 - all employees are aware of their responsibility to adhere to the policy and ensure that all breaches of information security, actual or suspected are reported and investigated.
- 3.14** This policy, and the subordinate policies to this document, provides a clear statement of our commitment to protect all physical and information assets from threats internal and external, intentional or accidental. This policy is issued and maintained by the ICT Manager, who also provides advice and guidance on its implementation and ensures compliance. All employees and consultants within the Commission are directly responsible for implementing and complying with this policy.
- 3.15** An Information Security Management System, compliant to ISO27001 (Information security management systems) provides the framework for the implementation of this policy within the Commission and is supported by a comprehensive set of policies and procedures. The ISMS is managed by the Commission's Information Asset Group whose members are responsible for setting objectives and priorities.
- 3.16** This policy is supported by and aligned with other Commission policies that underpin the Commission's ISMS. These include:
- Business Continuity Policy
 - Disposal of IT Equipment Policy

- Incident Management Policy
- Information Risk Policy, Risk Treatment Plan and Statement of Applicability
- Risk Management Framework Guide
- Statement of Internal Audit Procedures
- Record Classification and Retention Schedule
- System Back-Up Policy
- Finance Policy
- The Employee Handbook

3.17 Security priorities shall be informed by periodic information security risk assessments.

3.18 This Security Policy, which has been endorsed by the Commission Board, contains standards and guidelines that all users of Commission information assets must comply with.

3.19 This policy shall be subject to the same monitoring and maintenance schedules as other parts of the Commission's ISMS.

4 Information systems security

4.1 End user equipment

4.1.1 This policy section has been established to maximise the security, safety, maintainability and asset control of all Commission computer equipment.

4.1.2 All computer hardware and software in use at the Commission must be supplied through the ICT Helpdesk. Employees may not use or physically connect their own computer equipment on Commission premises without prior authorisation from the ICT Manager.

4.1.3 All portable computer equipment taken off-site must be kept under secure conditions at all times (eg. in a locked boot of a vehicle). Use of BlackBerry devices for the receipt and transmission of email must be in accordance with the BlackBerry Usage Policy and Agreement. Portable equipment such as laptops should not be left on desks in Victoria Square House out of hours or be left unattended for long periods of time.

4.1.4 All computer equipment allocated to employees is for business use only and must not be used by non-Commission employees including friends and family. No changes are to be made to the configuration of computer equipment except by authorised technicians or unless instructed to do so by said technicians. The use of all cryptographic controls shall be in line with the Commission's information handling guidelines and national government guidelines (where applicable) and shall be used in compliance with all relevant agreements, laws, and regulations. Secret and private cryptographic keys shall be stored on an encrypted device in a safe and shall have limited access.

4.1.5 Employees must not move any Commission desktop equipment from its current location, whether for conducting demonstrations or in connection with office moves, without prior agreement or assistance from the ICT Helpdesk.

4.1.6 Employees must not take any computer desktop equipment home without prior agreement from their line manager and agreement in writing (eg. email) from the ICT Helpdesk. The ICT Helpdesk must be informed of the expected and actual date of return.

- 4.1.7** When moving hardware to a new location, the ICT Helpdesk will take a full data back up, dismantle the hardware and bubble wrap it. Then ICT Helpdesk will supervise the removal and installation in new premises using a recognised Commission removal contractor.
- 4.1.8** All upgrades to computer equipment must be requested using internal departmental procedures and forwarded to the ICT Helpdesk for consideration.
- 4.1.9** Before disposing of computer hardware, all data must be deleted and hard discs low level formatted; this includes all PCs servers and mobile devices. The ICT Helpdesk will perform this function in accordance with the Hardware Disposal Policy.
- 4.1.10** All Commission equipment is authenticated as a Commission machine through Active Directory membership.
- 4.1.11** Access to Commission data or network can only be achieved using a Commission recognised computer or by use of the approved VPN client and appropriate authentication protocol. Accessing the Commission's data remotely is governed by this policy.
- 4.1.12** Any system, software or hardware faults must be reported to the ICT Helpdesk who will execute repairs and replacements as required ensuring continued availability and integrity. Fault calls will be logged on the ICT Helpdesk tracking software and ICT Helpdesk will log calls with third party suppliers where support contracts are in place. ICT Helpdesk will monitor responses and resolutions, update the tracking software and notify data owners and employees where appropriate.

4.2 Software

- 4.2.1** This policy section has been established to control software distribution and usage within the Commission. It is important that all software in the organisation is properly licensed, meets the requirements of the Copyright, Designs and Patents Act 1988 and that the Commission can prove ownership if challenged. The import (download) of software from the Internet is one of the main ways that viruses get into organisations and is not permitted unless authorised by ICT Helpdesk.
- 4.2.2** This policy section provides for the protection of material held by the Commission which may be considered intellectual property and it is the responsibility of all employees to maintain this protection, including copying or duplicating any media. This policy is not exhaustive or intended as a substitute for expert legal advice and further information should be sought where necessary. The ICT department shall be responsible for maintaining, disposing and transferring software licences.
- 4.2.3** PC software packages are varied in design and content: what is suitable for a single user may not be suitable for the rest of the organisation or for a networked installation. All software that comes into the organisation must be evaluated and assessed to establish whether it is a suitable tool for use within the Commission and to ensure copyright is not violated. It must also be tested to ascertain if its installation will interfere with other software and whether the reaction compromises the functionality or security of either package.
- 4.2.4** Only Commission ICT Helpdesk, or an authorised agent of the ICT department, may install or modify software eg Microsoft Office, or modify operating system parameters eg registry settings or screen savers.
- 4.2.5** The ICT department must approve all software used on Commission equipment. If it is found that there is a need for software that is not currently used in the organisation, a business case must be put forward by the department manager to the Head of ICT who will assess its impact on the technical architecture and consider it for approval.

- 4.2.6** Employees must not attempt to load any executable software from any other machine onto their own, or to download shareware or other executable software from the Internet, or otherwise try to gain access to software other than through the ICT Helpdesk.
- 4.2.7** This includes music and video player software for example iTunes.
- 4.2.8** Employees must not make illegal copies of licensed software.
- 4.2.9** Employees must not load or distribute pornographic, racist or other offensive material onto their own or colleagues' workstation(s).
- 4.2.10** Employees provided with end-user software development tools (eg MS Access) must ensure that all software applications developed by them are clearly documented and backed up.
- 4.2.11** All upgrades to software must be requested using internal departmental procedures and sent to the ICT Helpdesk.
- 4.2.12** All changes to information processing facilities and systems will be controlled. Patches and software upgrades are only to be installed by the ICT department. All patches and software upgrades will be tested in an isolated test environment prior to being released for production. Implemented patches and upgrades will be recorded in either Windows Server Update Services or TrackIT. Where the patch or upgrade applies to an operating system any business applications running on that operating system will be tested and reviewed.
- 4.2.13** Regular software audits to detect unauthorised software installations and compliance with licensing restrictions are performed automatically through the helpdesk software (Track IT) and recorded and reviewed within this system by the ICT Manager.
- 4.2.14** All software operating procedures shall be documented, maintained and made available to all users who require them via desk instructions and or software manuals.
- 4.2.15** For internally developed and bespoke applications the source code will be maintained within a secure source code repository with limited access.

4.3 System and data access

- 4.3.1.** This policy section has been established to recognise that data is a valuable corporate commodity that must be protected both from misuse within the organisation and from corruption introduced from external sources.
- 4.3.2.** All personal data held on Commission computer systems is subject to the provisions of the Data Protection Act 1998 (DPA) and as such is not to be divulged to any non- Commission employee or organisation unless for the purposes covered by the Commission's DPA registration. All such data is the property of Commission.
- 4.3.3.** Any information being made available on any Commission web sites shall be protected to prevent unauthorised modification.
- 4.3.4.** Employees will be granted access to data appropriate to their roles and responsibilities, through the use of active directory domain security groups. This will reduce opportunities for unauthorised or unintentional modification or misuse. Employees must not attempt to gain access to other directories, file servers, computers or data to which they have not been authorised, whether from within the Commission premises or from a remote system.

- 4.3.5.** Commission employees may only access Commission corporate data and systems from remote locations using a VPN encrypted connection using the approved VPN client and appropriate authentication. All connections will be locked out after 3 unsuccessful attempts. Employees must contact the ICT Manager to enable VPN access on their Active Directory account and to request access to the VPN software and appropriate authentication system.
- 4.3.6.** All permanent home workers will access Commission systems using an encrypted MPLS (Multi Packet Layer Switch) connection provided by the Commission. All viewing of information, edit and creation of data is to be done using terminal services (Application Launcher) technology to ensure secure remote access without permanently storing data on the remote computer. The MPLS network is subject to end to end encryption technology and user authentication, monitored by the network provider to protect it from threats and maintain security for the systems and applications using the network including information in transit. Terminal services sessions are locked after 5 minutes inactivity requiring authentication to reactivate, disconnected after 2 hours of inactivity and terminated after one day of inactivity.
- 4.3.7.** It is not permissible to install, or have installed by a third party, any software which will allow remote access to Commission systems without express prior written agreement of the exact methodology from the Head of ICT. The Head of ICT has the right to disconnect from the network any device which they believe constitutes a security threat to the organisation until that threat is removed.
- 4.3.8.** Wherever possible employees must not store corporate data (ie all data including personal working data) on PC hard drives but within the appropriate networked system. ICT Helpdesk will notify users which drive or system is appropriate.
- 4.3.9.** ICT Helpdesk is responsible for the security and backup of all corporate data held on servers at Commission sites. Any data stored on PC/laptop hard drives is not backed up and it is stored there at the end users own risk.
- 4.3.10.** All corporate systems and data must have assigned owners. Data owners are responsible for ensuring the safety, integrity, confidentiality and availability of systems and data within their remit.
- 4.3.11.** Data owners are responsible for periodic risk assessments of access to the data they steward and must satisfy themselves that the data under their stewardship has appropriate access and change controls and that these are properly followed. Data owners or their nominated representatives shall be responsible for the formal authorisation of access requests, their periodic review and revocation.
- 4.3.12.** The Commission will not be responsible for any data corrupted whilst being imported into Commission systems from outside systems. It is the responsibility of the user to ensure beforehand that such imports are capable of being used by Commission corporate systems, consulting, working with and gaining authorisation from ICT Helpdesk as necessary.
- 4.3.13.** If large amounts of data, in excess of 500 Megabytes, have to be moved around the network, the ICT Helpdesk must be contacted for advice as to when such transfers can be achieved, without compromising network access for other users.
- 4.3.14.** All data transferred to removable media must be done using the Connect Protect software, which requires the user to obtain prior authorisation before the copy is possible. This provides the Commission with an audit trail of all documents and files that are copied to and or deleted from removable media. The ICT Manager will monitor on a weekly basis what files are being copied to removable media using the Connect Protect software.

Authorisation will be granted or denied based on the classification of the data being transported.

- 4.3.15.** Access to specific applications will be granted on request through ICT Helpdesk who will contact the data owner and request permission and access levels as appropriate.
- 4.3.16.** When an employee changes role or department, HR or the employee's manager will inform ICT Helpdesk and access will be removed from specific applications and directories.
- 4.3.17.** Only ICT employees with administrative domain access can remotely control Commission servers.
- 4.3.18.** All remote access will be locked after 5 minutes inactivity and be controlled by secure, strong passwords.
- 4.3.19.** Agreements with third parties involving accessing, processing, communicating or managing Commission information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.
- 4.3.20.** All third party remote access accounts are controlled by ICT Helpdesk and are only enabled on request. The request will be logged on the ICT Helpdesk system and the account left open until the third party has completed the support task or the end of one working day whichever occurs first, the account will then be disabled. Remote access accounts will not be left enabled overnight or at weekends under any circumstances.
- 4.3.21.** All third party remote access accounts are specific to the server (software) that the particular third party is supporting. Access is controlled through Active Directory and Group Policy to ensure that the remote access account is only able to access data on the server specific to that third party.
- 4.3.22.** The Commission ensures that all information involved in electronic commerce passing over public networks is protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification by the use of trusted commercial software and hardware appliances.
- 4.3.23.** The Commission restricts open inbound connections (ports) to specific application servers and destinations and only where deemed necessary for specific business requirements. By default all inbound ports are closed and opened only by exception. Configuration of open ports may only be changed by the Commission's appointed network security provider who must be provided with the change request in writing by the Head of ICT.
- 4.3.24.** Physical and logical access to diagnostic and configuration ports is controlled through membership of appropriate Active Directory groups and/or physically separate network points and VLANs that are not available to general users.
- 4.3.25.** VLAN technology is used to separate distinct groups of information services (eg servers, PCs, VOIP telephones, printers, high volume scanners and external connections) providing an additional security layer and streamlining/prioritisation of network traffic. Servers are segregated into departmental functions where applications in use on particular servers are departmentally specific or where a sensitive system requires an isolated or dedicated environment. VLAN routing is used to ensure only authorised network traffic can traverse specific VLANs and in combination with IP routing controls ensures specific separate network segments are maintained where appropriate and information flows do not breach the access control policies of business applications.
- 4.3.26.** Audit logs are kept of user activity, exceptions, and information security events are produced and kept for a minimum of three months to assist in future investigations and

access control monitoring. Logging facilities and log information is protected against tampering and unauthorised access by locating log information on server locations only accessible by domain administrators. Procedures for monitoring the users of information processing facilities are established and the results of the monitoring activities are reviewed regularly by the ICT Manager.

- 4.3.27.** The domain administrator account password is not to be routinely used or known by any (including ICT) employee other than the Head of ICT. In an emergency scenario, the domain administrator password can be accessed from a sealed envelope held in the ICT safe. Any use of the domain administrator account and password must be logged in the 'Use of GC Admin Account Log', maintained by the ICT Manager and is subject to approval by the Head of ICT.
- 4.3.28.** The ICT Helpdesk will be responsible for the creation of users and allocation of access privileges to all information systems, this includes individual systems that require specific users to be created outside of Active Directory.
- 4.3.29.** Connection to Commission networks using wireless LAN technology is restricted to only where the wireless connection is used to support an encrypted VPN connection or an encrypted MPLS connection authenticated by the Commission.

4.4 Virus protection

- 4.4.1.** This policy section has been established to protect all information processing systems at risk from virus attack. The Commission will maintain a multi-layered anti-virus protection designed to ensure that security is maintained at server and PC/laptop level. Additional anti-virus measures are installed and maintained as an integral part of the email system. These measures will ensure detection, prevention and recovery controls are in place to protect against malicious code entering or leaving the organisation.
- 4.4.2.** Employees must not disable or remove the virus checking software on their PC/laptop. The anti-virus software must be running at all times.
- 4.4.3.** All suspected viruses or pop up messages from the anti virus software must be reported immediately to the ICT Helpdesk and the PC/laptop must not be used until it has been checked by ICT Helpdesk and re-approved for use.
- 4.4.4.** Employees should be on guard for virus-containing emails from unexpected sources with unexpected subject lines and or senders. If suspicious email messages arrive the ICT Helpdesk must be contacted immediately for advice before opening the email.
- 4.4.5.** Any computing equipment brought onto the Commission's premises by consultants or other persons proposing to connect to the Commission corporate network must first be checked by ICT Helpdesk to satisfy the requirement that sufficient anti-virus and security measures are in place. If insufficient measures are discovered then the user will have the option of either having the Commission anti-virus software loaded or not attaching to the network.
- 4.4.6.** Employees should always request CDs, memory sticks and floppy disks to be virus checked by the ICT Helpdesk before despatching them outside of the organisation.
- 4.4.7.** Mobile ActiveX controls can only be installed and configured by ICT Helpdesk where they are necessary to meet appropriate business system requirements.
- 4.4.8.** All reported incidents of suspected malicious code or viruses will be recorded in TrackIT by ICT Helpdesk and escalated in accordance with the ISMS policy.

4.5 Use of passwords

- 4.5.1. This policy section has been established to minimise the risk of illegal access to corporate systems. Every user of a computer system must have a unique user name or user ID for this system. To enhance the security of this individual ID, the user enters a second identification, a password, which is known only to that person and to the relevant system itself.
- 4.5.2. All Commission systems incorporate user names and passwords as standard. Some systems synchronise an ID and password with a related system such that the ID and password only needs to be entered once.
- 4.5.3. Every user who requires access to a Commission ICT system must have a personal user ID for the network and any IT System they will use. These logins and passwords will be controlled by Active Directory and Group Policy. Only this ID should be used unless specific business requirements dictate otherwise.
- 4.5.4. Each new employee is given a network login and temporary password; the system will prompt for a new password on first login.
- 4.5.5. Passwords are supplied for personal use. Except as in the next bullet below, employees must not divulge passwords to any other person other than in exceptional circumstances to the ICT Helpdesk. If a user password becomes known to the ICT Helpdesk it will be reset, prompting the user to change the password immediately after it becomes known.
- 4.5.6. Where Departments manage a number of 'generic' logon IDs for specific tasks it is the responsibility of the Department managers to manage the use of these and to keep a detailed log of their use for audit purposes.
- 4.5.7. Passwords are Group Policy controlled and must be changed every 42 days prompted either by the system or by ICT Helpdesk. The system remembers 24 passwords and will not allow repeat passwords from this historical 24.
- 4.5.8. No passwords are to be stored in data, software or function keys (ie F1- F12), or written down. Where administration passwords have to be recorded for Disaster Recovery purposes they must be secure and locked in the ICT safe.
- 4.5.9. The Head of ICT will control allocation of domain administration access accounts.
- 4.5.10. Strong passwords for network/PC access must contain characters from at least 3 of the following 4 classes:
 - a. Letters upper case A,B,C etc
 - b. Letters lower case a, b, c etc
 - c. Numerals 0,1,2,3 etc
 - d. Non-alphanumeric ("special characters") @{}£% etc.Additionally passwords must be a minimum of 7 characters long and must not contain any parts of your name.
- 4.5.11. Passwords for specific applications generally have more relaxed rules than those above, however users are recommended to follow the same rules as above where possible.
- 4.5.12. The use of Power-On passwords on Commission equipment is prohibited. Employees must not 'power on password protect' their PC/laptop but use the operating system logon procedure and only the username and password provided to them.
- 4.5.13. Employees must not use personal passwords for business use.

4.5.14. The use of passwords on individual files, eg MS Word documents, is discouraged as this could prevent other users accessing corporate data when someone leaves the organisation. Where this is deemed necessary within a department, clear documentation should be filed which is accessible to that department's line manager.

4.6 Use of email

4.6.1 This policy section provides instruction for the responsible use of the email system; the Commission has a responsibility to:

- abide by information legislation that applies to email communication including the DPA, Freedom of Information Act 2000 (FOI) and Regulation of Investigatory Powers Act 2000
- ensure that people are not being abusive or writing messages where the content is untrue or could be construed as being untrue
- ensure that our employees are clear on their responsibilities regarding email communication.

4.6.2 Employees may use external email for legitimate business purposes and for essential personal communications. Email messages can be used for different types of communication and can constitute a formal record of proceedings. The types of communication include general business discussions, dissemination of information, agreement to proceed and confirmation of decisions made. Thought should be given when addressing email, only include those people who are required to respond in the 'To' address box. Use 'cc' and 'bcc' when the email does not require an action. If the email is for information only (FYI) then this should be stated at the start of the email to enable the recipient to quickly identify what is required of them.

4.6.3 All emails and attachments sent to external organisations must comply with Commission style guidelines and include warning messages giving legal protection from interception, copying and the use of liability disclaimers. The privacy and confidentiality of messages sent via email cannot be guaranteed. It is the responsibility of all employees to judge the appropriateness of using email when dealing with sensitive subjects. Remember that any email you write or store may be liable to be disclosed under DPA or FOI. Don't make changes to someone else's message and pass it on without making it clear where you have made the changes, this could be viewed as misrepresentation.

4.6.4 Email must not be used for inappropriate forms of personal communication. See the Commission Harassment and Bullying Policy for further information on issues related to racial or sexual harassment or bullying. Harassment, whether through language, frequency of messages, or size of message text, is unacceptable.

4.6.5 Employees must not use email in a way that could be construed as defamatory about a third party, whether to another employee or an individual or organisation outside the Commission. Various pieces of legislation relating to written communication apply equally to email messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation and discrimination.

4.6.6 The mail system is intended to be used as a messaging system. Important messages and documents must be saved in the appropriate departmental filing structure on a file server. Employees must ensure that all information of a sensitive nature that is sent via email is treated with care in terms of drafting and addressing. Sensitive information sent via email that is incorrect might provide a case of initiating legal proceedings against the person

sending the information and/or the Commission. Sensitive information can include commercial information and information about specific individuals or groups. Be aware that the recipient of your message might forward it to others without recognising the need to seek your consent. You cannot be sure who these other recipients will be.

- 4.6.7** The email system must not be used for sending of global emails, where there is an urgent business need to do so the Corporate Affairs team will send an urgent email alert. The 'Intranet' is the appropriate means for notification of news items to large numbers of employees.
- 4.6.8** In general, the privacy of the content of emails will be respected. There will be exceptional circumstances, however, when the Commission may require access to email accounts including their contents. These include:
- unexpected or prolonged absence of an employee, where not dealing with the email in a timely manner adversely affects the running of the Commission
 - line of business enquiry
 - to fulfil a legal requirement eg a Subject Access Request under DPA or a FOI request.
- 4.6.9** Where it is not possible to ask permission from the employee whose mailbox needs to be accessed, the procedure for gaining access is:
- gain authorisation from their line manager
 - submit a request to ICT Helpdesk
 - document the reasons for accessing the mailbox
 - inform the mailbox owner.
- 4.6.10** Employees must not attempt to forge email header information relating to another person or organisation. The commonest breach of confidentiality is wrongly addressed email; if you receive an email that was intended for someone else let the sender know as soon as possible.
- 4.6.11** Employees must not create or forward 'chain letters' or other 'pyramid schemes' of any type, or send unsolicited commercial mailings. Bear in mind anything you receive may not have originated from where it says it does, as email headers are easily forged.
- 4.6.12** The Commission has the right to monitor the use of all mail facilities, including personal emails. People who administer the system do have access to all mail if deemed necessary. Messages relating to, or in support of illegal activities as stated above may be reported to line managers and/or HR.
- 4.6.13** Large email attachments in excess of 8Mb cannot be guaranteed to be transmitted successfully over the Internet. ICT Helpdesk will advise employees of alternative methods for large file transfers.
- 4.6.14** Excessive personal use of email will be considered a breach of this policy, employees should discuss with their line manager what constitutes 'excessive personal use' if they are concerned. All mail is scanned for inappropriate content whether incoming or outgoing.
- 4.6.15** Emails with attachments greater than 10Mb will neither be sent nor received; contact ICT Helpdesk for alternative methods of transferring large files.
- 4.6.16** It is the responsibility of all employees to manage and file their email messages appropriately. This is important in order to comply with legislation and to ensure that

individuals can easily locate information relating to a specific topic or area of the organisation.

- 4.6.17** The maximum mailbox size is currently 275Mb employees will receive a warning message at 250Mb and should archive some email; contact ICT Helpdesk if you need assistance using this feature. Once 275Mb is reached employees can no longer send email (although email will still be received in all circumstances).
- 4.6.18** Where email is accessed remotely it must only be done over an encrypted VPN connection, encrypted MPLS connection, by Commission supplied BlackBerry or using an SSL connection for Outlook Web Access.
- 4.6.19** In addition to the Commission's network and system access controls as detailed within this policy, electronic messages are delivered via an authorised agent to protect the identity of the messaging infrastructure and virus scanned prior to entry to the Commission's network.
- 4.6.20** Selected classified messages and attachments are delivered and received via an approved, encrypted, external messaging service, dependant on their Government Protective Marking Scheme (GPMS) status.

4.7 Internet access and use

- 4.7.1** This policy section has been established to provide guidelines on how and when to make appropriate use of the Commission corporate Internet connection such that the integrity of both the organisation and its individual employees are not compromised.
- 4.7.2** Employees may only use Internet information facilities during working time for business or training purposes. During non-working time such as lunch breaks employees may use these facilities for appropriate and reasonable personal interests if authorised by department management, however note point 4.7.7 below.
- 4.7.3** The Commission's Internet access, and any Commission equipment capable of accessing the intranet, *must not* be used for any of the following:
 - the creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
 - the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
 - the creation or transmission of defamatory material
 - the transmission of material that infringes the copyright of another person
 - the sending of unsolicited commercial mailings
 - deliberate unauthorised access to facilities or services accessible via Commission internet connections
 - deliberate activities with any of the following characteristics:
 - wasting networked resources and the effort of employees involved in the support of those systems
 - corrupting or destroying other users' data
 - violating the privacy of other users
 - disrupting the work of other users
 - "Denial of service" attacks
 - breach of authentication or security measures
 - any attempt to gain access to any other account, host or network

- continuing to use an item of networking software or hardware after ICT has requested that its use cease because it is causing disruption to the correct functioning of the Internet facility
- other misuse of the Internet or networked resources, such as the introduction of "viruses"
- using the system to engage in any other illegal act
- personal use of Commission internet or networking facilities for personal financial gain.

- 4.7.4** Employees are not permitted to create and maintain externally accessible personal web sites and web logs or blogs whilst at work. Employees' externally accessible personal web sites or web logs must not use a Commission email address as a point of contact or contain any links to the Commission's web sites. Information posted on these personal websites or web logs should not enable the reader to identify the Commission or any of its departments, colleagues, customers or other stakeholders.
- 4.7.5** Unlawful conduct or conduct that violates regulation or the accepted norms of the Internet community, whether or not expressly mentioned in this or any other corporate policy is unacceptable. The Commission will remove access from anyone that it decides is using the Internet in a manner that damages its reputation and goodwill.
- 4.7.6** When accessing other networks via the Commission network, you are subject to the acceptable use policy of those other networks.
- 4.7.7** The Commission monitors the use of all Internet activities, including personal emails. This includes all dates, times, web site names, user name, workstation and time spent accessing individual sites. Alert emails are sent to the Head of ICT of when attempted access to "banned sites" has been made. Details are passed to the Director of People & Organisational Development, if it is considered a breach of this policy and may be dealt with in accordance with the Commission's Disciplinary Procedure.
- 4.7.8** The Commission monitors email use including personal emails. Reports are generated weekly and monthly and passed to the ICT Manager and Director of People & Organisational Development. Any use considered to be excessive may be dealt with in accordance with the Commission's Disciplinary Procedure.
- 4.7.9** Do not post on the Internet (eg on technical support sites, bulletin boards, chat rooms, etc.) any information that could be used by external parties to access or otherwise attack Commission information systems. Such information includes, but is not restricted to the following: Usernames; Passwords; Computer/Server Names; Software and Operating System Versions; Network Topologies, Hardware Configurations, etc.
- 4.7.10** Use of internet sites, such as MySpace, Face book and You Tube which allow Social Networking have become extremely popular. When using such technology it is important to be aware of the risks and take steps to protect yourself and the Commission. Be careful about how much information you divulge about yourself. Posting personal information could potentially lead to unwanted attention and could even put you at risk of fraud. Users frequently forget that these sites are accessible to all. If you contribute comments about an identifiable individual, you should bear in mind that anyone anywhere will be able to see what you have posted, including that individual themselves. Do not make offensive or derogatory remarks about Commission employees or stakeholders, and do not post obscene or derogatory images. The Commission reserves the right to take disciplinary action if appropriate and, in extreme cases, defamation can lead to legal action. When using social networking sites pay particular attention to the points made in paragraph 4.7.2 and 4.7.5.

4.7.11 All information involved in electronic commerce and/or information being made available on publicly accessible systems and/or passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification by the use of secure servers, firewall appliances, use of specific open ports and transmission of information using SSL and VeriSign certificates.

4.8 Protecting systems and Network equipment

- 4.8.1** This policy section has been established to maximise the security and safety of computer premises and the equipment within and to make sure that only authorised personnel have access to Commission IT Systems.
- 4.8.2** When a new employee enters the organisation, ICT Helpdesk will be notified of their IT requirements before they join. The new user's departmental managers or HR will inform ICT Helpdesk via email with the new starters' IT requirements and to arrange a user ID and access permissions.
- 4.8.3** Managers or HR will notify ICT Helpdesk the date of departure of any employees who temporarily (e.g. maternity leave) or permanently leave the organisation. Authorised ICT employees will then disable or remove all user accounts for permanent leavers.
- 4.8.4** When an employee leaves the Commission their account is disabled and all group membership removed on the day they leave and personal data and emails archived within one week of them leaving.
- 4.8.5** All access to Commission information processing systems will be through authorised routes only; any violation may incur disciplinary or legal proceedings.
- 4.8.6** All workstations must be either 'locked' via a password protected screen saver or 'logged off' if left unattended, group policy will automatically lock all PC's after 5 minutes of inactivity.
- 4.8.7** Unless specifically exempted by ICT Helpdesk all employees must exit all applications and the network at the end of their working day and shutdown their PC.
- 4.8.8** The Commission premises all contain IT infrastructure network equipment (e.g. Hubs, routers etc.). Such equipment is usually located in locked Computer rooms or data communications cabinets and is easily identified. Unauthorised employees must not attempt to gain access to any of the devices contained within these areas.
- 4.8.9** Only authorised employees may make adjustments to voice and data cabling within the Commission's premises, power and data cables will be protected by routing under floors or in ceilings and will be terminated in the Computer room or locked data cabinets.
- 4.8.10** All use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance, identified issues should be escalated to the ICT Manager. ICT will monitor server capacity monthly.
- 4.8.11** Only authorised ICT Helpdesk employees may enter the Computer Rooms unaccompanied. Other employees, authorised agents or visitors may only do so after specific authorisation from the Head of ICT, and must be accompanied.

- 4.8.12** ICT Helpdesk must be given notice of any visitors who may require the use of Commission systems, their purpose, what systems they wish to use, and who will be responsible for supervising their work. Any such use must be authorised in writing by the ICT manager.
- 4.8.13** All Commission clocks of all relevant information processing systems within the organisation or security domain shall be synchronised with a reputable network time source.
- 4.8.14** All Commission networks are managed and controlled through secure firewalls, in order to be protected from threats, and to maintain security for the systems and applications using the network.
- 4.8.15** The ICT team will maintain timely information regarding security patches and software updates. Security patches, software updates and the organisation's exposure to vulnerabilities will be evaluated by the ICT team. Updates will be rolled out to end user equipment automatically to ensure all equipment is maintained at the approved security patch level.
- 4.8.16** The ICT Team will ensure that all security features, services levels and management requirements of all network services are identified and included in any network services agreement, whether these services are provided in-house or outsourced.
- 4.8.17** System documentation will be stored securely and only be accessible to the ICT Team.

4.9 Use of Telephone Systems

- 4.9.1** All employees will be allocated a direct dial telephone number when they join the Commission that will require a username and password to access.
- 4.9.2** Where appropriate to their role employees will be allocated a password protected voicemail account.

5 Physical security policy for the protection of assets

5.1 Physical security

- 5.1.1** This policy section focuses on physical security and covers associated security issues. Physical security includes doors, locks, cupboards, security grilles and any other physical barrier designed to protect assets. It also encompasses the building having 24hr security with access either by ID card or signed for visitor badges which are issued only with the Commission's – or other building tenant's – authority.
- 5.1.2** All doors, windows, and other access points to buildings are provided with secure locks and catches of an approved standard. Environmental / fire barriers have also been provided as an additional safeguard. These devices are maintained in good working order and records kept of all key holders and of those who have access to keys.
- 5.1.3** Lockable cabinets, cupboards or drawers as appropriate are provided for each employee so that they can keep personal belongings secure while they carry out their duties.
- 5.1.4** Contracted secure off-site storage is provided for select Commission documents. Requested files are tracked to prevent data loss and stored in the lockable filing cabinets when not in use.

- 5.1.5 Access to the 4th floor of Victoria Square House is controlled by both proximity card readers and CCTV. The card readers are located at all entry and exit points of the floor, excluding exits designated for emergency use only. These are covered by CCTV and checked regularly by both the Facilities Team and the Building Security. Each employee's usage of each door reader to gain access is recorded for three weeks for audit purposes.
- 5.1.6 No employee may transfer a Protectively Marked information asset from outside of the scope of the Commission's ISMS without the permission of the Information Asset Owner or their delegated authority. The transfer of information assets outside of the scope of the Commission's ISMS must be done in line with the Commission's published information handling guidelines.

5.2 Access cards

- 5.2.1 Employees must keep their access cards in a safe place at all times when not at their place of work.
- 5.2.2 Employees must inform Facilities immediately if they lose their access card or believe it to be stolen.
- 5.2.3 Employees must arrange to replace damaged or defective cards.
- 5.2.4 Employees must use their access card when accessing the floor on every occasion.
- 5.2.5 Employees must wait until the card reader shows a flashing set of green / red lights before operating it with their card.
- 5.2.6 Employees must not permit others to use their access card or allow access to others when entering the building.
- 5.2.7 Employees must report any incident of misuse or malfunction of the access control system to the Facilities team.
- 5.2.8 The door entry system should be in place 24hrs a day, 7 days a week.
- 5.2.9 Access to the floor and its internal doors will be by swipe cards.
- 5.2.10 Doors should be kept shut.
- 5.2.11 Swipe cards should be issued to all employees and should be returned if an employee leaves the organisation if not cancelled by Facilities.
- 5.2.12 An additional 14 cards are issued, one to the Building Manager in case of emergencies, one to the building security team, six to the cleaning contractors who will sign the card in / out at the rear security desk, two to the archiving company, two to the vending company, one to the building engineers and one to the data backup company in case of emergencies. All have timed restricted access and are still required to sign in / out at security.
- 5.2.13 Access by employees will be from 6am to 9pm Monday to Friday.
- 5.2.14 Weekend working is by prior arrangement with their line manager and the Facilities Manager who can adjust their swipe access times.
- 5.2.15 Facilities will keep records of out of core time working and will be able to monitor the access times using the card access system.

5.3 Identity badges and visitor security

- 5.3.1** Security badges will be issued to all employees, visitors, contractors, temporary employees and any other person who needs access to the Commission's premises for any reason, other than members of the emergency services. The issued badge is both a door access card and security badge.
- 5.3.2** Postal / delivery service visitors must sign in at the rear door security desk, should be restricted to the rear entrance area and post room unless accompanied by an employee. Contractors, postal / delivery service visitors will be isolated from information processing facilities where possible.
- 5.3.3** Access to the post room is restricted to those employees working as part of the post room function.
- 5.3.4** Badges issued to employees will display the name of the employee and where possible, their photograph.
- 5.3.5** All visitors to Commission's buildings must be issued with a temporary paper badge which clearly identifies them as a building visitor giving their name, the organisation they represent and an expiry date.
- 5.3.6** All visitors should be accompanied by an employee from and to Reception.
- 5.3.7** Visitors must display their security badges prominently at all items while they are on Commission premises and should be courteously challenged if the badges are not displayed.
- 5.3.8** Employees must keep their security badges in a safe place when they are not at their place of employment.
- 5.3.9** Employees must inform facilities immediately if they lose their security badge or believe it to be stolen.
- 5.3.10** Employees must comply with the building Security Guards' requests in security matters.

5.4 CCTV

- 5.4.1** Where security risks are considered high the use of CCTV is employed as a deterrent to intruders and to provide a means of retrieving relevant information should an incident occur.
- 5.4.2** The primary function of CCTV cameras is the protection of Commission assets. The cameras will be used, where possible, to offer some protection to employee's property although this is a secondary function. Systems will be reviewed at regular intervals to ensure they are still appropriate for the task, and modified to reflect any changes to the building or areas covered by the cameras.
- 5.4.3** CCTV coverage is kept for 2 weeks. The duration of recording required each day will be dictated by both the quality and the storage capacity. It is recommended that there should be sufficient storage capacity provided for up to 8 cameras recording from 6pm to 7am Monday to Friday and round the clock for Saturday and Sunday.

- 5.4.4 CCTV is not a means of monitoring employee's movements even though they may occasionally be captured on video when it is active. To this end, a statement will be issued to employees warning them that this is the case and obtaining their consent for the occasional capture of their image on the cameras.
- 5.4.5 A warning sign for visitors will be provided at both entrances to the floor.
- 5.4.6 Access to the footage from the CCTV cameras can only be done with the permission of a Director and the Head of ICT.
- 5.4.7 Members of Facilities will only have access, from their PCs (pop-up windows), to images from the cameras which are positioned in the door entry panels at both the front and back doors as part of the door access system. They will then be able to give access both to visitors and contractors in a safe and secure manner.

5.5 Document security / Clear desk

- 5.5.1 Employees must keep their work place clear of all confidential and sensitive documents when they are away from their desk or office.
- 5.5.2 Employees must check all information they communicate to others to ensure that information is not transmitted unintentionally. This is particularly important when forwarding emails, which may contain such information in the previous thread.
- 5.5.3 Employees must not copy information, documents or data unnecessarily, or contravene copyright laws.
- 5.5.4 Access to areas containing sensitive information such as the Intelligence Room and the two case rooms, is restricted to authorised personnel only by the use of access control systems. The doors to these restricted areas must be closed when they are not occupied or when their work necessitates confidentiality. These arrangements must be reinforced by the use of locked cupboards and cabinets within these rooms.
- 5.5.5 Employees must ensure that all confidential information is stored in locked cabinets or drawers at the end of the working day and at other times when they are out of the building (eg business trip).
- 5.5.6 Employees must ensure that all confidential information is disposed of securely, i.e. by using confidential recycling, shredding etc as provided. This will be reinforced by Facilities removing all documents left on printers / photocopiers at approximately 4pm each day and placing them in the nearest confidential recycling bin.
- 5.5.7 All confidential / paper waste is disposed of in a controlled manner fortnightly by an accredited company and a disposal certificate issued. All shredding is carried out on the building's premises witnessed by Facilities.

6 Breaches, exemptions and logging

6.1 Security breaches

- 6.1.1 You must comply with this and all other authorised security policies and procedures which are issued by the Commission.
- 6.1.2 Any breaches of this policy should be reported and escalated immediately to your line manager who in turn should report the breach to the Information Asset group to be logged and reviewed.

6.1.3 Serious security breaches may result in disciplinary action or investigation. Any disciplinary action will be taken in accordance with the Commission's Disciplinary Procedure as published in the Employee Handbook and on the intranet.

6.2 Logging

6.2.1 All security incidents will be logged in accordance with the Security Incident Management Policy.

6.2.2 Employees are encouraged to be vigilant and report all security and potential security breaches to their line manager, the Head of ICT or the Facilities Manager.

6.2.3 For further information on concerns about improper conduct and whistle-blowing refer to the Commission's Corporate Governance Framework.

6.3 Exemptions to security policy

6.3.1 Some users of the Commission's systems may have permitted exemptions to some paragraphs in this document in order to do their work.

6.3.2 It is your line manager's responsibility to ensure you have been formally granted the requisite exemptions to this policy, if any apply.

6.3.3 Where any exemption to this policy or the wider information security management system applies, these exemptions shall be added to the appropriate risk assessment and evaluated according to the Commission's Information Risk Policy. The justifications for these exemptions shall be included in the record as well as notes on authorisation and escalation levels engaged.