THE MORAY COUNCIL

CORPORATE INFORMATION SECURITY POLICY

Document Revision			
Title	CORPORATE INFORMATION SECURITY POLICY	**Date Created**	06 January 2008
Author	Mike Alexander, ICT Project Leader	**Date of Issue**	27 October 2008
Client	Corporate	**Status**	**COMPLETE - ISSUED**
Document Control			
Document Version	2.0	**Date of Release**	**09 January 2009**
Issued by	Mike Alexander, ICT Project Leader		

Amendments issued since publication

Amendment No.	Date	Comments
001/MJA	**29/10/2008**	Draft document (Version 2.0) issued for consultation.
002/MJA	**06/01/2009**	Final draft following consultation.
003/MJA	**19/01/2009**	**Document issued.**

Related Documents

1. Moray Council: Computer Use Policy
2. Moray Council: Records Management Policy
3. Code of Connection for the GSi
4. JANET Acceptable Use Policy

Reference Documents

1. BS ISO/IEC 27001:2005 – Information Security Management Systems - Requirements
2. BS ISO/IEC 27002:2005 – Code of Practice for Information Security Management
3. Data Protection Act (1998)
4. Computer Misuse Act (1990)
5. Human Rights Act (1998)
6. Regulation of Investigatory Powers (Scotland) Act (2000)
7. Freedom of Information (Scotland) Act (2002)
8. ICO – Data Protection: Privacy Impact Assessment Handbook
9. Payment Card Industry Data Security Standard v1.2 (October 2008)
10. HMG Infosec Standard No. 1 – Residual Risk Assessment Method
11. HMG Infosec Standard No. 2 – Risk Management and Accreditation of Information Systems
12. HMG Infosec Standard No. 3 – Connecting Business Domains
13. HMG Infosec Standard No. 4 – Communications Security and Cryptography
14. HMG Infosec Standard No. 5 – Secure Sanitisation of Protectively Marked or Sensitive Information
15. CESG Infosec Memorandum No. 12 – Dealing with Malicious Software
16. CESG Infosec Memorandum No. 21 – Risk Management of Mobile Code
17. CESG Infosec Memorandum No. 26 – Passwords for Identification and Authentication
18. CESG Infosec Memorandum No. 35 – Remote Access to Public Sector IT Systems
19. e-Government Interoperability Framework (e-GIF)
20. e-Government Security Framework

[This page is intentionally blank]

Table of Contents

1 POLICY

1.1 INTRODUCTION

The Moray Council (hereafter referred to as the Council) makes extensive use of Information and Communications Technology (ICT) and Information Systems (IS) in order to realise both its business and strategic objectives of delivering services to the public.

The Moray Council has a responsibility to ensure that information is properly collected, processed, maintained and disposed of. Information held by the Council can be personal and/or highly confidential. Consequently the Council needs to protect this information and the ICT/IS facilities used to store and process the information.

The Council also has obligations to its staff and to the public to clearly define the requirements for the use of its ICT facilities and information systems. This is to ensure that users of ICT/IS facilities do not unintentionally place themselves, or the Council, at risk of prosecution by carrying out computer-related activities outside the law.

For these reasons, it is imperative that proper controls are in place to manage information security.

1.2 WHAT IS INFORMATION?

Information is an asset, one which can exist in a variety of formats. These can include:

- Spoken conversations;
- Hand written or printed paper;
- Faxes;
- Emails;
- Mobile phone texts;
- Computer storage;
- Computer network transmissions;
- Computer media (disks, tapes, CDs, DVDs, USB memory sticks, film, microfiche, etc.);
- Databases;
- CCTV recordings;
- Digital/mobile phone camera images.

As with other assets, information has a value both to the Council and others. As such, the Council has a responsibility to ensure that its information assets are properly collected, maintained, disposed of and are available only to those who require access to them.

1.3 HOW IS INFORMATION SECURITY MANAGED?

The Moray Council has taken the decision to develop information security practices based on the recommendations of the 'International Organization for Standardization' (ISO) and the 'International Electrotechnical Commission' (IEC). Their code of practice for information security management is known as ISO/IEC 27002:2005, and is regarded as 'best commercial practice' within both the public and private sectors. The ISO standard supersedes the British Standard known as BS 7799-1.

1.4 SCOPE

This Information Security Policy is effective from the date of approval, and applies to all of the Council's information systems. The policy, rules and conditions apply to all employees, contractors, volunteers, consultants, agency staff and other users of the Council's information systems, irrespective of the platforms used or where they are located.

The Information Security Policy plays a part in ensuring that:

- Information can only be accessed by those who both require such access and are authorised to do so;
- Information cannot be altered either inadvertently or maliciously;
- Information is available to those authorised to access it as and when required;
- The Moray Council fulfils its obligations under the Copyright Designs and Patents Act 1988, the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002, the Computer Misuse Act 1990, and any other current regulations or legislation;

- Business continuity plans are put in place and tested to guarantee services are available to information users when required.

1.5 LINKS WITH OTHER COUNCIL POLICIES AND STANDARDS

This information security policy should be viewed as complementary to the following Council Policies:

- Records Management Policy;
- Computer Use Policy;
- Business Continuity Policy.

1.6 SUPPORTING SUB-POLICIES, PRINCIPLES AND STANDARDS

This information security policy provides direction on how The Moray Council will manage the confidentiality, integrity, and availability of information. ISO/IEC 27002:2005 is used as the template for determining best practice. This policy will be communicated throughout the organisation to users in a form that is relevant, accessible and understandable. To this end, it will be supported by appropriate sub-policies, documentation, and training materials.

1.7 POLICY IMPLEMENTATION

It is the responsibility of all users to comply with this policy. To this end, all departmental and service managers (including Head Teachers) should monitor the use and management of their relevant information systems and ensure adherence to this policy.

The implementation of this Policy ensures the protection of the Council's ICT infrastructure, which is taken to include (but may not be limited to):

- All Council Information held electronically;
- All physical data and voice communications networks and components;
- All software applications resident on applications servers, file servers and networking equipment;
- All file and applications server hardware;
- All PC systems and accompanying software applications;
- All corporate software applications;
- All storage media;
- Internet and e-mail services;
- All ICT related systems and software applications documentation.

The rigorous implementation of this Policy also helps to ensure the security, validity and integrity of all electronically stored data, systems and applications software. It will also contribute to the achievement of acceptable levels of systems availability.

1.8 POLICY ENFORCEMENT

Failure to adhere to this policy may result in a breach of Financial Regulations, Standing Orders, policies such as the Computer Use Policy, current legislation, and/or agreements with third parties upon which business functions depend. Therefore any suspected breach of this policy, as well as any other information security concerns (such as perceived weaknesses in information system security), should be reported at the earliest opportunity to the Information Security Officer. Contact details can be found in Appendix C.

The application of this policy will be monitored by the Information Security Officer and may be subject to audit from time to time to assess compliance with its contents. Where there is found to be a breach of the policy, the Information Security Officer will notify the relevant departmental management, and give consideration to any further actions that might be required.

1.9 NON-COMPLIANCE

Non-compliance is defined as one or more of the following:

- A breach of the Council's overarching Information Security Policy and associated sub-policies, standards or controls;
- Unauthorised removal, disclosure or viewing of confidential information belonging to the Council;
- Unauthorised modification to information, software or operating systems;

- The use of hardware, software, communication networks, equipment, data or information for illicit purposes, which may include violations of law, regulation or reporting requirements of an enforcement agency or Government body;
- Failure to report an apparent or suspected breach of the Council's Information Security Policies to the Information Security Officer, supervisor or manager.

As with any other approved policy of the Council, violation or non-compliance with the Council's Information Security Policy may be treated as misconduct. In the event of a breach by a Council employee, ICT facilities may be suspended/removed and disciplinary action taken in accordance with the Council's Disciplinary Procedure. Action against non-Council employees may result in removal/suspension of IT facilities, removal from site, cancellation of any contracts and possible legal action.

1.10 POLICY REVIEW

1.10.1 Internal Review

The Information Security Officer will perform periodic reviews of the following:

- The effectiveness of the Policy, demonstrated by the nature, number and impact of reported security incidents;
- The cost and impact of controls upon business efficiency;
- The effects of changes to technology.

At a minimum such reviews will be performed annually and reported to the Chief Financial Officer.

1.10.2 Independent Review of Information Security

In order to ensure the effectiveness of this Policy, the implementation of the Policy will from time to time be subject to review by an independent third party organisation.

Such a review will be conducted to provide assurance that operational practices properly reflect the Policy, and that the Policy is feasible and effective. Reviews will be conducted periodically, in particular when significant changes to the security implementation occur.

The choice of third party organisation may either be the Council's External Auditors, or external consultants specialising in such reviews, where either of these organisations have the appropriate skills and experience.

1.11 TERMS AND DEFINITIONS

Refer to Appendix A "*Terms and Definitions*" and Appendix B "*List of Abbreviations*".

[This page is intentionally blank]

2 ORGANISATION OF INFORMATION SECURITY

2.1 GENERAL

The Moray Council endeavours to ensure that suitable frameworks exist to initiate and control the implementation of information security both within the Council and between itself and external organisations.

2.2 ALLOCATION OF INFORMATION SECURITY RESPONSIBILITIES

It is important that staff at all levels appreciate that they have an individual responsibility to ensure information is handled sensibly and appropriately. This section outlines those responsibilities, as well as those of specialist information security individuals and groups within the Council. These ensure that sources of specialist information security knowledge and advice are readily available, contacts with external security specialists are developed and maintained, standards and assessment methods are monitored, and that suitable liaison points exist to deal with security incidents.

2.2.1 All Users

All users are expected to adhere to a basic set of information security tenets. Their responsibilities include, but are not limited to:

- Maintaining the confidentiality of the Council's information;
- Following appropriate security procedures for the Council's systems;
- Using authorised, Council procured software only, and preventing the unauthorised introduction of new software;
- Choosing effective computer passwords and keeping them confidential;
- Ensuring workstations are locked or logged off when unattended;
- Ensuring the security of any information taken off-site;
- Using email, public networks and the Internet in a professional manner and in accordance with the Council's Computer Use Policy;
- Taking appropriate precautions against malware, including viruses, Trojan horses and spyware;
- Reporting security breaches, weaknesses, or unusual software malfunctions to the Information Security Officer, supervisor or manager.

2.2.2 Managers and Supervisors (including Head Teachers)

The Council's manager's responsibilities include, but are not limited to:

- Authorising the publication of the Council's information;
- Authorising access to the Council's systems;
- Regular reviews of access rights for their staff;
- Promoting the Council's information security policies during the recruitment process (in job descriptions and in contracts of employment) and during staff induction training;
- Ensuring that contingency plans are in place to enable business to function in the event of a major incident;
- Putting recovery procedures in place to recover their business and operational processes should a major incident occur;
- Ensuring their team members comply with information security policies;
- Escalating reported security breaches, weaknesses or unusual software malfunctions through the appropriate channels.

2.2.3 Data Custodians

Senior Responsible Officers within Council departments will be nominated to act as the information owners for specific sets of information held or used within departments. Their responsibilities include, but are not limited to, ensuring that:

- Their systems are documented and managed appropriately to guard against operational failures;
- Security requirements are included in any changes to their systems;
- Only authorised users have access to their systems;
- There exists documented contingency plans for their systems;
- Users of their information systems are aware of their responsibilities for security;

- Good records management practices are adhered to in accordance with the Council's Records Management policies. These include the proper operation of retention schedules that are set for manual and electronic datasets and the timeous destruction of time-expired material in order to comply with access to information legislation and provide good business practice.

2.2.4 ICT Services

ICT Services manages the Council's ICT infrastructure, core ICT systems, and desktop devices. From the perspective of information security, its responsibilities include, but are not limited to, ensuring that:

- Network links and domains are appropriately separated and protected;
- In-house applications and services are developed with security in mind;
- New developments, technologies and systems are adequately assessed prior to deployment;
- Computer systems are protected against malware, including viruses, Trojan horses, and spyware;
- Users and administrators of ICT systems and services are aware of their responsibilities for security;
- There exists documented contingency plans for the ICT systems under their control;
- Systems are monitored to check for security breaches;
- Any such security breaches, weaknesses, or unusual software malfunctions are reported to the Information Security Officer.

The responsibilities of ICT Services are further expanded in Section 6, "*Communications and Operations Management*".

2.2.5 Information Security Officer

The Moray Council has designated the role of Information Security Officer, the remit of which includes moving the Council towards an alignment with ISO27000. This includes the development and review of information security policies, guidelines and procedures for the Council, as well as implementing specific security related projects and raising staff awareness of issues that they face.

In addition, the post is tasked with disseminating best practice to Council departments and services and, where necessary, identifying appropriate controls to improve information security. The responsibility for implementing the controls remains with the appointed owner for each information asset (see 2.2.3).

The Information Security Officer will provide regular security reports to both the Head of ICT Services and the Chief Financial Officer.

2.2.6 Corporate Personnel Services

The responsibilities of Personnel Services include, but are not limited to:

- Promoting the Council's information security policies during the recruitment process (in job descriptions and in contracts of employment) and during staff induction training;
- Providing ICT Services with information regarding termination or change of employment of staff within the Council;
- Supporting the application of disciplinary procedures where appropriate.

2.2.7 Co-operation between organisations

The Council maintains links and participates in forums organised by organisations with a relevant interest in information security, e.g. Society of IT Managers (SocITM), British Computer Society (BCS), Office of Government Commerce (OGC), and Communications-Electronics Security Group (CESG) who are the National Technical Authority for Information Assurance.

In addition, the Council will maintain appropriate relationships with the police, telecommunications suppliers, IT suppliers, and specialist service suppliers to ensure that information security issues, concerns, and incidents are properly handled.

Exchanges of security information will be restricted to ensure that confidential information of the organisation, and details of the specific controls implemented, is not passed to unauthorised persons.

2.3 CONFIDENTIALITY AGREEMENTS

Confidentiality or Non-Disclosure Agreements using legally enforceable terms should be considered where there is a requirement to protect confidential information. Such agreements protect the Council's information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorised manner.

The following should be considered when implementing such agreements:

- A definition of the information to be protected;
- The expected duration of the agreement, including cases where confidentiality might need to be maintained indefinitely;
- Required actions when an agreement is terminated;
- Responsibilities and actions of signatories to avoid unauthorised information disclosure;
- Ownership of the information, and how this relates to the protection of confidential information;
- The permitted use of confidential information, and rights of the signatory to use the information;
- The right by officers of the Council and its auditors to audit and monitor activities that involve confidential information;
- Process for notification and reporting of unauthorised disclosure or confidential information breaches;
- Terms for information to be returned or destroyed at agreement cessation;
- Expected actions to be taken in case of breach of the agreement.

2.4 AUTHORISATION PROCESS FOR ICT FACILITIES

Before any ICT hardware or software is procured, or commitment is made to procure, formal approval will be required from ICT Services by the appropriate capital or revenue budget holder.

The budget holder will be responsible for ensuring that the procurement and planned implementation of the desired ICT equipment adheres fully to this Policy, and is in accordance with the Corporate ICT Action Plan, any appropriate Departmental ICT strategies and any relevant ICT system implementation plan.

Where necessary, a risk assessment will be conducted to ensure that any new vulnerabilities are properly assessed and addressed, and that any new controls are properly authorised.

Where it is considered necessary or beneficial to make information regarding the technical infrastructure available to potential suppliers or service providers, such information will be marked "*Confidential - Restricted*" and vetted by the Information Security Officer prior to release. Where appropriate a Non-Disclosure Agreement (NDA) may be sought before the release of such information.

2.5 THIRD PARTY ACCESS

Careful consideration must be given to how partners and customers use Council facilities. This includes, for example, members of the public who call in person at Council offices, and business partners who arrive at Council premises in person or access Council computer systems remotely. The reasons for this are apparent. Allowing customers to enter offices designated 'Council staff only' could put confidential information at risk of unauthorised access. Similarly, information security could be compromised by allowing access to Council ICT systems by external parties with inadequate security management procedures in place.

For the reasons outlined above, access to information processing facilities by external parties must be controlled, whether the type of access be physical (e.g. to offices, computer rooms, or filing cabinets) or logical (e.g. to Council computer databases and other computerised information systems).

It is expected that staff will ensure that external parties, whilst on Council premises, are adequately supervised. In extreme cases, this may mean making sure that the external party is accompanied at all times when working in areas or on tasks that pose a high risk to information security.

ICT Services will ensure that external party logical access is controlled by adequate technological and/or contractual barriers e.g. firewalls and codes of connection.

For all types of access, it is recommended that a risk assessment is prepared and regularly reviewed. In addition, the use of third party agreements and confidentiality clauses should be considered, particularly where access is required by business partners.

3 ASSET MANAGEMENT

3.1 GENERAL

Appropriate measures will be established to ensure that protection of the Council's information and information processing assets.

3.2 INVENTORY OF ASSETS

Inventories of information assets, including hardware, software and key information will be developed and maintained within ICT Services. Such inventories should include all information necessary in order to recover from a disaster, and should include the type of asset, the format, location, backup information, licence information, and a business value. Where possible the content of the inventories should be aligned with other asset inventories within the Council.

Council Departments and service areas will be responsible for ensuring that ICT are informed in a timely fashion of any amendments required to the information asset inventories.

The following is a non-exhaustive list of the types of assets that should be recorded:

- Information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- Software assets: application software, system software, development tools, and utilities;
- Physical assets: computer equipment, communications equipment, removable media, and other equipment;
- Services: computing and communications services, general utilities (e.g. heating, power, lighting, air-conditioning);
- People, and their qualifications, skills, and experience;
- Intangibles, such as reputation and image of the organisation.

3.3 OWNERSHIP OF ASSETS

ICT Services will work with departments to ensure that all major information assets are accounted for and have a nominated owner. The information owner will be responsible for periodically reviewing access restrictions and classifications, taking into account applicable access control policies. Ownership should be given to the following assets:

- A business process;
- A defined set of activities;
- An application; or
- A defined set of data.

3.4 ACCEPTABLE USE OF ASSETS

All employees, contractors, and third party users will follow rules for the acceptable use of information and assets associated with information processing facilities, including:

- Rules for electronic mail and Internet use (Computer Use Policy);
- Guidelines for the use of mobile devices, especially outwith Council premises.

3.5 INFORMATION CLASSIFICATION

To ensure that information assets receive an appropriate level of protection, such information assets will be classified to indicate the need, priorities, and expected degree of protection when handling the information. It should be recognised that some items may require additional levels of protection or special handling.

An information classification system will be established and used to define an appropriate set of protection levels, and to communicate the need for special handling measures. Where doubt exists as to the level of sensitivity of information, or what protective measures are appropriate, staff should seek advice from the Council’s Information Security Officer.

It will be the responsibility of Departments to determine the classification of an item of information, and for periodically reviewing that classification. All such classifications (and any changes) will be agreed with the Information Security Officer.

3.5.1 Classification of Highly Sensitive Data

Some information will be regarded as particularly sensitive and will require to be given additional levels of protection both for storage and transmission. It will be the responsibility of Departments to identify data that is of a particularly sensitive nature, and to agree with the Council’s Information Security Officer where and how it should be handled.

3.6 INFORMATION LABELLING AND HANDLING

An appropriate set of procedures will be defined for information labelling and handling in accordance with the classification scheme. Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label in the output.

From time to time, Council employees may receive information classified under the Government Protective Marking Scheme (GPMS). The GPMS is a protective marking regime that exists within Her Majesty’s Government; for example such information may carry a term such as PROTECT, RESTRICTED, or CONFIDENTIAL, and is likely to originate from organisations such as the Police and Government departments.

Note that it is the responsibility of the sender of such information to satisfy him or herself as to how the Council will handle information that carries such a protective marking. Advice on the appropriate handling of information carrying a GPMS marking can be obtained from the Council’s Information Security Officer.

4 HUMAN RESOURCES MANAGEMENT

4.1 GENERAL

The Moray Council and its constituent departments will ensure that personnel security is addressed at the relevant stages of the employment process.

4.2 RECRUITMENT

Council departments should take appropriate steps to ensure that specific responsibilities for managing and/or adhering to aspects of the Council's Information Security Policy are included in staff job descriptions. It is recommended that new recruits are made explicitly aware of their responsibilities to:

- Implement and act in accordance with the Council's Information Security Policy;
- Protect assets from unauthorised access, disclosure, modification, destruction or interference;
- Execute particular security processes or activities;
- Accept responsibility for any actions taken;
- Report all security events or potential events or other security risks to the Information Security Officer.

Recruits must be suitably screened, in particular for posts requiring access to information or information systems that may be deemed sensitive.

4.3 DURING EMPLOYMENT

Departmental management must ensure that employees, volunteers, contractors and third party users apply security in accordance with this and related Council policies. To this end, departmental management should ensure that all users:

- Are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems;
- Are provided with guidelines to state security expectations of their role within the organisation;
- Are motivated to fulfil the security policies of the Council.

4.4 TERMINATION OR CHANGE OF EMPLOYMENT

Departmental management must ensure that duties related to employment termination or change of employment are clearly defined and assigned. Such duties include responsibility for the return of Council assets and the removal of access rights (to offices and buildings as well as information assets and systems).

[This page is intentionally blank]

5 PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 GENERAL

Appropriate control mechanisms will be established to prevent unauthorised access, damage and/or interference to the Council's information assets and information processing facilities. In addition, suitable measures must be in place to prevent loss, damage, theft or compromise of assets and interruption to the Council’s activities.

5.2 SECURE AREAS

5.2.1 General

Photography, recording or video equipment must not be allowed within secure areas unless authorised by the appropriate departmental manager.

5.2.2 Data Centre

A secure data centre environment for housing all major corporate information systems hardware, data storage and communications equipment will be established within the Council's office premises. This facility will be air conditioned with fire detection and security access. As such it will provide a proper environment for the management of the Council's ICT assets.

The consumption of food and drink will not be permitted within the main computer room within the Council's data centre.

Only ICT Services staff and authorised visitors will be permitted access to the Council's data centre. Visitors will be accompanied at all times by a member of ICT Services staff.

5.2.3 Secure Areas within Council Premises

Departments must consider appropriate protection for information and information processing facilities. They should give consideration to:

- Physical security perimeter;
- Physical entry controls;
- Securing rooms, offices and facilities;
- Secure working areas;
- Protection against external and environmental threats;
- Public access, delivery and loading areas.

Where practicable, Council premises should have “staff-only” areas where the processing of information is undertaken, in order to limit the access of unauthorised individuals into areas where sensitive information may be processed or stored. Contractors and other third-parties should be supervised at all times in secure areas.

Secure and protected accommodation will be established throughout the Council's office premises for the location of other critical elements of the ICT infrastructure such as telephone exchanges, corporate applications and file servers, and key components of the corporate WAN and associated LANs. Accommodation for ICT infrastructure will only be accessible to authorised staff.

5.2.4 Secure Areas for Handling Highly Sensitive Information

Information systems, or PCs/terminals that are used to access information classified as highly sensitive (as defined in 3.5.1), must wherever possible be located in secure accommodation with appropriate access controls.

5.3 SECURITY OF ICT EQUIPMENT

Equipment associated with the storage, processing or display of information intended for internal consumption will be sited or protected such as to reduce the risks associated with environmental hazards and opportunities for unauthorised access. Wherever possible, such equipment will not be sited in public areas, or only after appropriate technical controls have been implemented.

Where equipment requires additional security, and cannot be located in secure areas, consideration may be given to such equipment being sited in areas where staff require only occasional access. The actual security measures implemented should reflect the sensitivity of the information that is stored, processed or displayed.

In addition to normal office environmental precautions against theft, fire and health and safety hazards, consideration will be given to additional issues associated with information processing equipment, such as air conditioning and electrical supply requirements and potential damage from water ingress.

Particular attention should be paid to ensure that:

- Equipment is sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access;
- Equipment is protected from power failures and other disruptions caused by failures in supporting facilities;
- Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage;
- Equipment should be correctly maintained to ensure its continued availability and integrity;
- Security should be applied to off-site equipment taking into account the different risks of working outside the Council's premises;
- Equipment, information or software should not be taken off-site without prior authorisation.

5.4 SECURITY OF EQUIPMENT OFF-PREMISES

Security should be applied to off-site equipment taking into account the different risks of working outside the Council's premises. Authorisation from the appropriate departmental manager will be required before equipment is taken off-site. Whilst off-site, such equipment will be protected by the user from the risk of theft and will not be left unattended in public places.

Any item of Council ICT equipment authorised for use out with Council premises, including PC equipment and laptop computers, will be subject to the same guidelines for use as ICT equipment within the workplace.

Staff who are issued portable devices, such as laptops, PDAs, mobile phones or "smartphones", must be made aware of the increased risk of theft and the consequences arising from the loss of data held upon the device, especially given that such data may carry high or sensitive classifications.

Council ICT equipment held off-site by a member of staff will be returned to the appropriate Council department if and when the member of staff leaves Council employment, or when the equipment is no longer required. Equipment will not be held off-site for any period of time longer than is necessary. All equipment that is to be held off-site will require to be signed for.

5.4.1 Insurance of Equipment

The Council provides reinstatement based insurance cover for all computer equipment including laptop PCs and ancillary/peripheral equipment owned, hired, leased, or loaned to the Council and for which it holds itself responsible whilst such equipment is in the UK. Cover is provided for most risks of physical damage including, but not limited to, fire, lighting, aircraft, explosion, riot, civil commotion, storm, flood, earthquake, transit, accidental damage and breakdown.

It should be noted however that the Council carries an excess of £5,000 and so consequently the loss of an individual item, for example a laptop, would fall into the excess. Therefore all staff must endeavour to ensure the physical safety of equipment in their possession and to take all reasonable precautions against such risks as theft.

5.5 SECURE DISPOSAL OR RE-USE OF EQUIPMENT

All redundant ICT equipment will be disposed of by arrangement with ICT Services.

All items of equipment containing storage media (such as computer hard drives) should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten in order to make the information non-retrievable. Standard delete or format functions must not be used.

Damaged devices containing sensitive data will require a risk assessment to determine whether the items should be physically destroyed rather than being sent for repair or discarded.

6 COMMUNICATIONS AND OPERATIONS MANAGEMENT

6.1 GENERAL

The Moray Council will ensure the correct and secure operation of processing facilities. Core electronic communication and IT-based information processing facilities are managed by the Council's ICT Services section.

6.2 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

ICT Services will ensure that operating instructions and incident response procedures are in place for information processing routines and facilities. Where resources permit, consideration will be given to separating duties where conflict of interest may occur – for example, segregating policy development from implementation by system administrators. It is recommended that other Council departments and services which manage their own applications follow this approach. All departments should ensure that:

- Operating procedures are documented, maintained, and made available to all users who need them;
- Changes to information processing facilities and systems are controlled (for example, significant changes are identified and recorded, changes are planned and tested, and that there is a formal approval procedure for proposed changes);
- Unless otherwise agreed by the Information Security Officer, staff duties are separated where potential conflicts of interest could occur – for example by ensuring that the same individual cannot both authorise a change and implement it;
- Development, test and operational facilities are separated.

6.3 THIRD PARTY SERVICE DELIVERY MANAGEMENT

The Council should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. In the case of outsourcing, it is the Council that is ultimately responsible for information processed by an outsourcing party.

Where the Council or Council departments have contracted a service to a third party organisation, it is recommended that the appropriate level of information security is implemented and maintained and reflected within all third party service delivery agreements, and in agreement with the Information Security Officer.

It is recommended that the services, reports and records provided by a third party should be regularly monitored and reviewed, and that audits should be carried out regularly. Monitoring and review of third party services should ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly, including notifying the Information Security Officer.

Responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team.

6.4 SYSTEM PLANNING AND ACCEPTANCE

In an effort to minimise the risk of systems failures, prior to any new information system being implemented, it is recommended that an assessment is made to ensure that adequate capacity and resources are in place to deliver the required system performance. Projections of future capacity requirements should be made, to reduce the risk of system overload.

Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance and use.

6.5 PROTECTION AGAINST MALICIOUS AND MOBILE CODE

ICT Services will ensure that all desktop computers and appropriate servers under its management are protected against malicious software, in a manner proportional to the perceived risk. At a minimum, antivirus software will be installed on all desktops, and updated on a regular basis.

Where practicable, at least two software products from different vendors will be deployed across the information processing environment for the purposes of protecting against malicious software. Such diversity of products is intended to provide a greater assurance of detection in the event that one of the products fails to detect a particular item of malicious software.

To further the Council's protection against malicious software, the download and/or installation of unauthorised software on any Council computer is prohibited.

Mobile code is software code which transfers from one computer to another and then executes automatically, performing a specific function with little or no user intervention. Examples of mobile code include JAVA and ActiveX.

Where the use of mobile code is authorised, the configuration should ensure that the authorised code operates according to the defined security policy, and that unauthorised code is prevented from being executed.

6.6 HOUSEKEEPING

ICT Services have procedures in place for the routine backing-up of information held in central data stores. These include mechanisms for backing-up, back-up tape/media storage, and for restoring information from a back-up. A fault logging mechanism is in place for all information systems managed by ICT Services.

It will be the responsibility of the individual PC user to ensure that important data files are stored on their local fileserver for automatic overnight backing up.

Where prior agreement has been given by ICT Services for departments or services to implement their own data storage facilities, it is recommended that they follow 'best practice' for backing up information as defined by ICT Services, and document the process they have in place. Advice on back-up routines and how best to document them is available from ICT Services.

6.7 NETWORK SECURITY MANAGEMENT

The secure management of networks requires careful consideration to dataflows, legal implications, monitoring and protection. The Council's voice and data networks, including the associated communications equipment, will be managed centrally by ICT Services by a dedicated team. As such, ICT Services will be responsible for ensuring the security of the Council's voice and data networks is addressed.

No connection to the corporate data network will be permitted without the prior approval of the Council's Head of ICT Services or delegated officer.

Although the primary security controls will be applied at the application level, data networks will be managed in such a way as to prevent unauthorised logical and physical connection, and to detect unauthorised connection should this occur. This will include the enablement of unused network connection points only when a legitimate requirement has been identified, the disabling of network connection points when they are no longer required, and restricting the use of diagnostic tools such as LAN monitors and 'sniffers'.

Data communications protocol filtering mechanisms will also be employed to restrict network access to authorised users.

Subject to overall cost considerations, the Council's WAN and associated LANs will be designed and configured in such a way that the consequential effect of any single component or link failure will be minimised.

6.8 MEDIA HANDLING

ICT Services will work with departments and services in order to put in place documented routines to securely handle computer media and output. This includes the:

- Management of removable computer media. Departments must be clear in stating what forms of removable media are permitted to be used and whether removable media can be removed from Council premises;
- Disposal of media. Departments must ensure that media (paper records and printouts, magnetic tapes, hard disks, floppy disks, CD-ROMs, USB pens, etc.) are stored and disposed of securely and safely. Departments should contact the Information Security Officer for advice and guidance where required.
- Information handling procedures. This is particularly important for sensitive information (for example where information is confidential or financial in nature or where an individual can be identified). Consideration should be given to, amongst other things,

how media is handled and labelled, whether or not to apply access restrictions to prevent access by unauthorised individuals, and ensuring that input data is complete and that processing is properly completed.

- Management of the security of system documentation. System documentation may contain a range of sensitive information (e.g. descriptions of application processes, procedures, data structures, remote access mechanisms, infrastructure topology, authorisation processes) and so should be protected against unauthorised access.

6.9 EXCHANGE OF INFORMATION AND SOFTWARE

In order to prevent the loss, modification or misuse of information exchanged between the Council and third party organisations, such exchanges must be controlled and efforts made to ensure their compliance with any current legislation.

Council employees should satisfy themselves that, before sharing Council information of a sensitive nature which identifies an individual (or individuals) or may affect Council business with another organisation, the officer concerned establishes that they are permitted to do so, particularly from a legal and ethical perspective, and in particular adhere to the provisos of the Data Protection Act (1998).

As stated in 2.4 (*Authorisation Process for ICT Facilities*) above, where it is considered necessary or beneficial to make information regarding the technical infrastructure available to a third party, such information will be marked "*Confidential - Restricted*" and vetted by the Information Security Officer prior to release. Where appropriate a Non-Disclosure Agreement (NDA) may be sought before the release of such information.

6.9.1 Exchange Agreements

Where regular exchanges of information occur, particularly where the information is deemed to be sensitive, Council departments are advised to examine the value of formal agreements.

Copies of formal and informal data sharing agreements should be lodged with Legal Services and the Information Security Officer.

6.9.2 Electronic Messaging

The use of email services other than those provided by ICT Services is prohibited. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls must be considered by Council departments.

To this end, ICT Services will implement the technical controls as resources permit. Any information leaving the Council should be acknowledged as having been forwarded from a named source. Email leaving the Council must be traceable to a known individual.

6.9.3 Physical Media in transit

All departments must ensure that media containing information is protected against unauthorised access, misuse or corruption during transportation beyond the Council's boundaries. This means that all electronic data leaving Council premises on mobile media (such as USB pen drives, laptop computer hard drives, floppy disks, and CDs or DVDs) should be encrypted (see 8.4), and staff made aware of best practice in protecting this information.

6.10 ELECTRONIC COMMERCE SERVICES

With increasing delivery of services to the public by electronic means, the Council needs to carefully consider the security implications associated with the use of electronic commerce services including on-line transactions. In addition, the integrity and availability of information electronically published through publically available systems (e.g. the World Wide Web) should also be considered.

6.10.1 On-Line Transactions

Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorised interception, unauthorised alteration, unauthorised disclosure, and unauthorised duplication or replay.

The extent of the controls adopted will need to be appropriate for the level of risk associated with the form of on-line transaction.

All on-line transactional systems involved in the handling or processing of payment card details (such as debit/credit cards) **must** comply with the Payment Card Industry Data Security Standard (PCI DSS).

6.10.2 Publically Available Information

The integrity of information being made available on a publically available system should be protected to prevent unauthorised modification and avoid potential embarrassment for the Council. Publically available systems should be subject to regular vulnerability scans (penetration testing) as per Section 11.3.

There should be a formal approval process before information is made publically available. In particular, it should be noted that information on a publically available system may also need to comply with laws, rules, and regulations in the jurisdiction in which the system is located.

6.11 MONITORING

In order to detect unauthorised information processing activities, systems will be monitored and information security events recorded.

Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring. Since audit logs may contain intrusive and personal data, appropriate privacy protection measures will be taken, and all monitoring activities will comply with all relevant legal requirements. Logging facilities and logging information should be protected against tampering and unauthorised access.

The activities of system administrators and system operators, including all privileged users, will be logged. Such logs should be reviewed on a regular basis. System administrators should not have permission to erase or de-activate logs of their own activities (also refer to 6.2).

Where possible, the date and time settings on all applications software and ICT equipment will be set/adjusted automatically, and synchronised to a central time source. Where this is not practicable, the Council's ICT users will be responsible for periodically checking the date and time settings on all applications software and ICT equipment under their control, as this will greatly assist audit checking.

7 ACCESS CONTROL

7.1 GENERAL

The Moray Council recognises the value of the information contained within its manual and electronic information systems. To this end, it will ensure that appropriate measures are put in place to control access to the information, information processing facilities and business processes under its control to appropriate persons or groups of persons.

7.2 ACCESS CONTROL POLICY

Logical access (for instance, to information and business processes) and physical access (for example, to buildings and facilities) must be controlled on the basis of business and security requirements.

It is the policy of the Council to restrict access to information systems to those staff and authorised agents of the Council who require such access to enable them to undertake their duties. Council departments and services, in conjunction with ICT Services, must determine who will authorise access to systems and put a clear authorisation process in place. A similar system must be used to authorise changes to access rights. A documented mechanism for informing ICT Services of access requirements should be in place.

Each multi-user software application will have a user access control policy clearly defined by ICT Services in conjunction with the departmental ‘owner’ of the system. This policy will define:

- The access rights of each user or group of users;
- The security requirements of individual departments and support applications;
- The relevant policy for information dissemination and entitlement;
- Adherence to relevant legislation e.g. Data Protection Act.

7.3 USER ACCESS MANAGEMENT

ICT Services will work with Council departments to establish procedures to control the allocation of access rights to information systems and services. These procedures will cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Where Council departments have delegated responsibility for their systems, they must implement similar procedures.

The allocation of privileged access rights, which allow users to override system controls, must be limited. ICT Services will ensure that only key administrators can affect privileged system and network controls. Privileged access will only be granted where such access could not compromise the operation of other information systems, or where such privileges would not allow that member of staff to access other critical or sensitive systems or information.

The procedures for registration and de-registration of users should include:

- The use of unique user IDs to enable users to be linked and held responsible for their actions;
- Checking that the user has authorisation from the system “owner” for the use of particular information systems or services;
- Checking that the level of access granted is appropriate to the business purpose (see 7.2 above) and is consistent with the Council’s Security Policy e.g. does not compromise segregation of duties (see 6.2);
- Ensuring that users understand the conditions of access;
- Ensuring that access is not provided until authorisation procedures have been completed;
- Maintaining a record of all persons registered to access systems;
- Maintaining a record of all privileged users;
- Immediately removing or blocking access rights of users who have changed roles or jobs or left the organisation;
- Periodically checking for redundant user IDs and accounts;
- Periodically checking and reviewing privileged access accounts (to be undertaken more frequently than for non-privileged accounts);
- Ensuring that redundant user IDs are not issued to other users.

The use of generic or shared user IDs is to be discouraged and will only be permitted with the approval of the Information Security Officer.

The Council's Personnel Services section will be responsible for notifying ICT Services to cancel user accounts of staff who leave the Council, or where staff change job function, to have any user access rights modified in accordance with their new role.

7.4 User Password Management

ICT Services will work with Council departments to ensure that good password management practices are followed at all times. This includes:

- Ensuring that users are made aware of the need to keep passwords confidential at all times;
- Establishing processes whereby users are forced to change passwords on a regular basis;
- Establishing minimum standards for the strength and complexity of passwords (it is recommended that passwords should be a minimum of eight characters, and include upper/lower case letters as well as numbers);
- Where users are required to maintain their own passwords that they are initially provided with a secure temporary password which they are forced to change immediately on first use;
- Establishing procedures to verify the identify of a user prior to providing a new, replacement or temporary password;
- Providing temporary passwords in a secure manner (e.g. avoiding the use of clear text email messages);
- Instructing users and system administrators not to store passwords on computer systems in an unprotected form;
- Always changing default vendor passwords following the installation of systems or software;
- Account passwords should not be embedded within automated log-on procedures.

7.5 User Responsibilities

Users should be made aware, through the continuous dissemination of good practice guidance and induction training, of the need for effective security. It is particularly important that they are made aware of their responsibilities for maintaining effective access controls, particularly the use of passwords for accessing information systems and the security of ICT equipment. The following good practice guidelines should be in place:

- Users reminded to manage passwords and **on no account divulge them to other individuals** – including colleagues and staff from ICT Services;
- Unattended computers are protected by means of a password-protected screensaver or password-protected monitor power-save function that is enabled after a period of inactivity (10 minutes is recommended);
- Users must log-off all central computers, servers and office PCs when a session is finished (i.e. not just switching off the PC or terminal screen);
- Laptop computers and mobile devices are secured in a lockable cabinet at the end of each working day.

In addition, where sensitive or critical business information is handled on paper or on electronic media, departments should consider implementing clear desk policies.

7.6 Network Access Control

In order to ensure the protection of network services, the Council will control access to both internal and external networked services. It is recommended that the following controls be implemented:

- Users should only be provided with access to the services that they have been specifically authorised to use;
- Appropriate authentication methods are used to control access by remote users and devices;
- The Council's computer network is logically segmented into separate network domains according to the nature of the information being stored or processes performed;
- Limit the capability for users to connect to the Council network, particularly from other networks, according to the requirements of the business they need to perform;

- Appropriate network routing controls are put in place to ensure that only approved computer connections and information flows can occur;
- Control physical and logical access to diagnostic and configuration ports on equipment.

Facilities exist to allow secure Council-wide access to the Internet and World Wide Web (WWW) from networked PCs, including the provision of a central firewall and proxy server(s). ALL access to the Internet, regardless of the service being used, will be provided via these central facilities; access to the Internet via any other means (e.g. modem) is strictly forbidden.

All Internet access will be permitted only to authenticated network users. Access to Internet facilities will not be permitted for 'anonymous' access, nor will access be restricted only by network node address.

7.7 OPERATING SYSTEM ACCESS CONTROL

Good security practices should be used to restrict access to operating systems to authorised users. Such practices include:

- Implementing a secure log-on procedure to control access to operating systems e.g. the use of a secure transport layer such as SSH for username and password transmission, the use of banner messages, and limiting the number of unsuccessful log-on attempts;
- Recording successful and failed system authentication attempts;
- Recording the use of special system privileges;
- All administrators should have a unique user ID for their personal use only;
- Password management and quality standards are enforced e.g. enforcing password length and complexity;
- The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled;
- Inactive sessions should be shut down after a defined period of inactivity.

7.8 APPLICATION AND INFORMATION ACCESS CONTROL

Wherever possible, it is recommended that access controls be utilised in particular software systems to prevent unauthorised access to any information which those systems may hold. This includes the application of granular access controls which permit access only to those parts of the system which the user requires.

Consideration should be given to the isolation of systems processing information that is especially sensitive in nature.

7.9 MOBILE COMPUTING AND TELEWORKING

When using mobile computing and communication facilities (e.g. laptops, notebooks, PDAs, mobile phone and smart phones) special care should be taken to ensure that business information is not compromised. Care should be taken when using mobile computing facilities in public places, meeting rooms, and other unprotected areas outside of Council premises.
In addition to the general requirements set out in this policy, the following controls should be implemented:

- Mobile computing equipment should be physically protected against theft, and particular care should be taken if equipment is to be left unattended e.g. in a meeting room, conference facility, hotel room, public transport;
- Where equipment carries important, sensitive and/or critical business information, all information held on the equipment should be encrypted;
- Processes should be established to ensure that the currency of virus protection and intrusion protection ("personal firewall") software is maintained;
- Users should be made aware of the additional risks of mobile computing, especially in using wireless networks which may lack security.

[This page is intentionally blank]

8 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

8.1 GENERAL

The Moray Council recognises the need to ensure that security is built into new and proposed systems, and is assessed as part of the normal system lifecycle. As such, appropriate consideration of the requirements for information systems security will be given prior to the development or procurement of ICT systems.

8.2 SECURITY REQUIREMENTS OF SYSTEMS

ICT Services in conjunction with Council departments will ensure that security issues are assessed prior to the development or procurement of new information systems, or enhancements made to existing systems. It is significantly cheaper to implement and maintain controls introduced at the design stage than those included during or after implementation. It is recommended that departments and services follow an accepted framework for analysing security requirements and identifying controls, risk assessment and risk management. ISO/IEC TR 13335-3 provides such guidance on the use of risk management processes to identify requirements for security controls.

A formal testing and acquisition process should follow the purchase of a product. Contracts with the supplier should address the security requirements.

8.3 CORRECT PROCESSING IN APPLICATIONS

The Council acknowledges the need to ensure that data entered into systems is valid, as is information subsequently derived from these systems. To this end, efforts must be made wherever possible to ensure that controls are in place to check data at the point of entry. All applications, including those developed in-house or by 3rd parties, should check for:

- Out-of-range values;
- Invalid characters in data fields;
- Missing or incomplete data;
- Exceeding upper and lower data volume limits (e.g. buffer overflow conditions).

A more complete selection of controls is outlined in ISO 27001:2005. Further advice is available from the Council’s Information Security Officer.

In addition to ensuring the validity of input data, data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Typically, systems and applications are constructed on the assumption that having undertaken appropriate validation, verification and testing, the output will always be correct. However, this assumption is not always valid i.e. systems that have been tested may still produce incorrect output under some circumstances.

Where possible, controls for ensuring the authenticity and integrity of messages within applications should be identified and implemented.

In order to ensure integrity, all input data will be automatically validated by software applications systems.

In order to guard against the corruption of data, regular system checks will be run against software application databases.

8.4 CRYPTOGRAPHIC CONTROLS

Where appropriate, consideration will be given to the adoption of data encryption techniques for sensitive and critical business information.

Where cryptographic measures are implemented, care should be taken to protect the confidentiality of the private key, particularly where digital signatures are used. Physical protection should be used to protect equipment used to generate, store and archive keys.

A policy governing the use of cryptographic systems and techniques, including the use of digital signatures and the management of cryptographic keys, will be incorporated in this document at a later date. In the meantime, advice on the use of cryptography is available from the Information Security Officer.

8.5 SECURITY OF SYSTEM FILES

System files are those which form part of an application or operating system. ICT Services will control access to system files by limiting the ability to modify or delete application and operating system files to specific system administrators. In particular:

- The updating of operational software, operating systems, applications, and program libraries will only be performed by trained administrators upon appropriate management authorisation;
- Operational systems should only hold approved executable code, and not development code or compilers;
- Applications and operating systems should only be implemented after extensive and successful testing;
- A configuration control system should be used to keep control of all implemented software as well as the system documentation;
- A rollback strategy should be in place before changes are implemented;
- Test data should be carefully selected, and protected and controlled;
- Access to program source code should be restricted;
- Old versions of software should be archived, together with any required information and parameters, for as long as the data is held in archive.

Live operational data will not be used for the purposes of program testing. Where extracts from databases are to be used for testing, prior authorisation will be required and documented, with all personal information removed or modified prior to its use.

Printed output test systems will be clearly marked “TEST ONLY” to ensure that such output is not inadvertently introduced into business processes.

8.6 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

The implementation of changes should be controlled by the use of formal change control procedures. Such procedures should be documented and enforced in order to minimise the corruption of information systems.

Wherever practicable, application and operational change control procedures should be established and integrated with one another (see also 6.2).

The change control process should include a technical review of operating system changes, with specific checks to ensure that system security is not being compromised. It is recommended that an individual or group be assigned the responsibility for monitoring vulnerabilities and vendors’ releases of patches and fixes (see 8.7).

Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

Particular care will be taken when upgrading ICT operating systems with specific checks to ensure that systems security is not being compromised.

The following controls should be considered to limit the opportunity and risk for information leakage should be prevented e.g. as may be achieved through the use and exploitation of covert channels:

- Scanning outbound media and communications for hidden information;
- Regular monitoring of personnel and system activities, where permitted under existing legislation;
- Monitoring resource usage in computer systems.

8.7 TECHNICAL VULNERABILITY MANAGEMENT

Timely information about technical vulnerabilities of information systems being used should be obtained, the Council’s exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. A current and complete inventory of assets (see 3.2) is necessary for effective vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current deployment state, and the individual(s) within the organisation responsible for the software.

ISO 27002:2005 contains a comprehensive guidance for establishing an effective management process for technical vulnerabilities. However, the following items are particularly important:

- Establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any co-ordination activities required;
- Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and technology assets;
- Upon identifying a potential technical vulnerability, the associated risks should be identified and the actions to be taken (such actions could involve patching of vulnerable systems, and/or the application of other controls);
- Wherever possible, patches should be tested prior to application in live environments, and facilities should be provided to achieve this;
- An audit log should be maintained for all procedures undertaken;
- The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;
- Systems at high risk should be addressed first.

[This page is intentionally blank]

9 INFORMATION SECURITY INCIDENT MANAGEMENT

9.1 GENERAL

The Moray Council recognises the need to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

9.2 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES

All employees, contractors, volunteers and third-party users of Council information systems and services are required to note and report any information security events or incidents.

Some examples of information security events and incidents include:

- Loss of service, equipment or facilities;
- System malfunctions or overloads;
- Human errors (e.g. unintentionally deleting a critical directory and all files contained therein);
- Non-compliance with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware;
- Access violations.

Information security events should be reported through the appropriate channels as quickly as possible. Normal practice will be to immediately alert the Council's ICT Helpdesk, as this point of contact will always be available during normal office hours.

Where the ICT Helpdesk system proves unsuitable, a system for recording events and actions as well as providing feedback will be established by the Information Security Officer.

Malfunctions or other anomalous system behaviour may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

The Council's normal disciplinary process may be invoked for dealing with employees, contractors or third-party users who commit security breaches.

All employees, contractors, volunteers and third-party users of Council information systems and services are required to note and report any observed or suspected security weaknesses in systems or services. These must be reported either directly to the Information Security Officer or via line management.

Under no circumstances should an employee, contractor volunteer or third-party user attempt to prove or exploit a suspected weakness, as this is liable to be interpreted as a potential misuse of the system. Such actions could also cause damage to the information system and may result in legal liability for the individual performing the testing.

[This page is intentionally blank]

10 BUSINESS CONTINUITY MANAGEMENT

10.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

The Council has a need to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.

To that end, comprehensive disaster recovery plans and associated operational procedures should be developed and maintained for the cost-effective recovery of critical information systems in the event of partial or total failure of the relevant operational system platform. These plans and procedures will include the specification of timescales within which operational services will be restored.

There should be a managed process for developing and maintaining disaster recovery plans across the Council. This planning process should include:

- Identification and prioritisation of critical corporate and departmental systems, including telephony services;
- Determination of the potential impact of various types of disaster on corporate and departmental systems;
- Identification and agreement of all responsibilities and emergency arrangements;
- Identification and sourcing of all required resources, including ICT facilities;
- Documentation of agreed procedures and processes;
- Appropriate education of relevant staff in the execution of the agreed emergency procedures and processes;
- Testing and updating of plans.

[This page is intentionally blank]

11 COMPLIANCE

11.1 GENERAL

This Corporate Information Security Policy is intended to ensure that measures are put in place to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and of any security requirements.

11.2 COMPLIANCE WITH LEGAL REQUIREMENTS

The design, operation, use, and management of information systems are subject to statutory, regulatory and contractual security requirements. The following non-exhaustive list provides a sample of those items of legislation that The Moray Council acknowledges as impacting on security requirements:

- Copyright Designs and Patents Act 1988;
- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Freedom of Information (Scotland) Act 2002;
- Civil Contingencies Act 2004;
- Sexual Offences Act 2003;
- Criminal Justice (Scotland) Act 2003.

In order to meet the demands of legislation, the Council will ensure that:

- Intellectual property rights are not infringed i.e. measures are taken to prevent the use of unlicensed software;
- Important records are protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements;
- Data protection and privacy is ensured as required in relevant legislation;
- Users are deterred from using information processing facilities for unauthorised purposes;
- Cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.

All Council staff and authorised agents will conform to the terms of software licence agreements. No software will be copied or installed on to an ICT system without the authorisation of the Council's Head of ICT Services.

The copyright of all software applications systems developed by Council staff or authorised agents, using Council resources will rest with the Council.

11.3 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE

It is recommended that all departments regularly review the compliance of information processing within their area of responsibility with this and any other supporting policies, in addition to any other standards and security requirements.

It is also recommended that information systems themselves are regularly checked for compliance with security standards. This includes conducting vulnerability scans and penetration testing.

11.4 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

Council information systems may be subject to audits carried out by the Council's Internal Audit function and occasionally by external parties e.g. Audit Scotland. It is recommended that audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business processes. It is suggested that the following guidelines are followed:

- Audit requirements are agreed with appropriate management;
- The scope of the checks should be agreed and controlled;
- The checks should be limited to read-only access to software and data;
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

- Resources for performing the checks should be explicitly identified and made available;
- Requirements for special or additional processing should be identified and agreed;
- All access should be monitored and logged to produce a reference trail; the use of time-stamped reference trails should be considered for critical data or systems;
- All procedures, requirements, and responsibilities should be documented;
- The person(s) carrying out the audit should be independent of the activities audited.

Access to information systems audit tools should be protected to prevent possible misuse or compromise.

Appendix A TERMS AND DEFINITIONS

[This page is intentionally blank]

Accreditation The process to ensure that the security policy has been implemented to reduce risk for an IT System to an acceptable level.

Asset Anything which has value to the Council and needs to be protected.

Assurance The confidence that may be held in the security provided by a system, product or process.

Availability Ensuring that authorised users have access to information and associated assets when required.

Code of Connection A list of security controls with which an organisation must be compliant before a proposed connection can be activated.

Compliance To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations.

Confidentiality Ensuring that information is accessible only to those authorised to have access.

Control Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature.

[**NOTE**: *Control* is also used as a synonym for safeguard or countermeasure]

Data Custodian An individual who has been identified as being responsible for a specific set or sets of information held within the Council.

Denial of Service An incident in which a user or organization is deliberately deprived of the services of a resource they would normally expect to have.

Firewall Data communications barrier that is trusted to limit the data that passes across it by implementation of network access control rules.

Guideline A description that clarifies what should be done and how, to achieve the objective set out in policies.

Information Processing Facilities Any information processing system, service or infrastructure, or the physical locations housing them.

Information Security Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security Event An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Information Security Incident The act of violating an explicit or implied security policy, indicated by a single or a series of unwanted or unexpected information security events.

Such an act may involve (but is not limited to):

- attempts (either failed or successful) to gain unauthorized access to a system or it's data;
- unwanted disruption or denial of service;
- the unauthorized use of a system for the processing or storage of data;
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Information Security Policy The set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed.

Integrity Safeguarding the accuracy and completeness of information and processing methods

Malware Malicious software designed to infiltrate or damage a computer system without the owner's informed consent. Malware includes:

- Viruses: a computer program that infects a computer system without the permission or knowledge of the owner, and invariably intended to cause some level of harm or disruption to that computer system;
- Worms: similar to a virus, except that a worm is self-replicating and can spread via a network to other vulnerable computer systems;
- Trojan Horses: a computer program that appears to perform a desirable function (e.g. screen saver) but in fact performs undisclosed malicious functions;
- Rootkits: software intended to take fundamental control of a computer system in a subversive fashion without the knowledge or consent of the owner;
- Spyware: software installed in a stealthy manner to intercept or partially take control of the user’s interaction with a computer system, without their consent, often with the purpose of surreptitiously passing personal, sensitive or confidential information to an unauthorised individual.

Protective Marking A protective marking is a label – usually a word or phrase contained within the header or footer of a document – that indicates the level of protection that should be applied to that document (or the information contained within it). The level of protective marking can be taken as an indication of the sensitivity of the information.

Examples of protective marking used within the GPMS (lowest first) are NOT PROTECTIVELY MARKED (NPM), PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET.

Risk The likelihood of a threat occurring and being successful in exploiting a vulnerability and causing a breach in security.

Risk Analysis The systematic use of information to identify sources and to estimate the risk.

Risk Assessment Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

Risk Evaluation The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk Management All the processes involved in identifying, assessing and judging risks, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

Risk Treatment The process of selection and implementation of measures (controls) to modify risk.

Third Party That person or body that is recognised as being independent of the parties involved, as concerns the issue in question.

Threat A weakness of an asset or group of assets that can be exploited by one or more threats.

Vulnerability A weakness of an asset or group of assets that can be exploited by one or more threats.

Appendix B LIST OF ABBREVIATIONS

[This page is intentionally blank]

A/V	Anti-Virus
ADS	Accreditation Document Set
BCS	British Computer Society
BS	British Standard
CA	Certificate Authority
CERT	Computer Emergency Response Team
CESG	Communications-Electronics Security Group (www.cesg.gov.uk)
CoCo	Code of Connection
COSLA	Convention of Scottish Local Authorities
CPNI	Centre for the Protection of National Infrastructure (www.cpni.gov.uk)
CSIA	Central Sponsor for Information Assurance (www.cabinetoffice.gov.uk/csia)
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPA	Data Protection Act
DPO	Data Protection Officer
EDI	Electronic Data Interchange
FAST	Federation Against Software Theft
FTP	File Transfer Protocol
GPMS	Government Protective Marking Scheme
GSi	Government Secure Infrastructure (collective name for GSI, GSX, xGSI, etc.)
GSI	Government Secure Intranet (GSi Community)
GSX	Government Secure Extranet (GSi Community)
HMG	Her Majesty’s Government
IA	Information Assurance
ICO	Information Commissioner’s Office
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
INFOSEC	Information Security
IS	Information System
ISCJIS	Integration of Scottish Criminal Justice Information Systems
ISMS	Information Security Management System
ISO	Information Security Officer (also International Standards Organisation)
ISPD	Information Security Policy Documentation
ITSEC	IT Security Evaluation and Certification Scheme
JANET	Joint Academic NETwork (the UK’s Education and Research Network)
LAN	Local Area Network
NDA	Non-Disclosure Agreement
OGC	Office of Government Commerce
PCI DSS	Payment Card Industry Data Security Standard
PDA	Personal Digital Assistant (also known as “palmtops” or “pocket PCs”)
PKI	Public Key Infrastructure
SLA	Service Level Agreement
SoA	Statement of Applicability
SOCITM	Society of IT Managers
UPS	Uninterruptible Power Supply
WAN	Wide Area Network
WWW	World Wide Web

[This page is intentionally blank]

Appendix C CONTACT DETAILS

[This page is intentionally blank]

Contact Details for the Information Security Officer

Name: Mike Alexander, ICT Project Leader

Address: Finance & ICT Services
Council HQ
High Street
ELGIN
Moray
IV30 1BX

Email: mike.alexander@moray.gov.uk

Phone: 01343 563445 (Direct)
Fax: 01343 563221

Contact Details for the ICT Service/Support Desk

Address: Finance & ICT Services
Council HQ
High Street
ELGIN
Moray
IV30 1BX

Email: helpdesk@moray.gov.uk

Phone: 01343 563333 (Direct)
Fax: 01343 563226

[This page is intentionally blank]