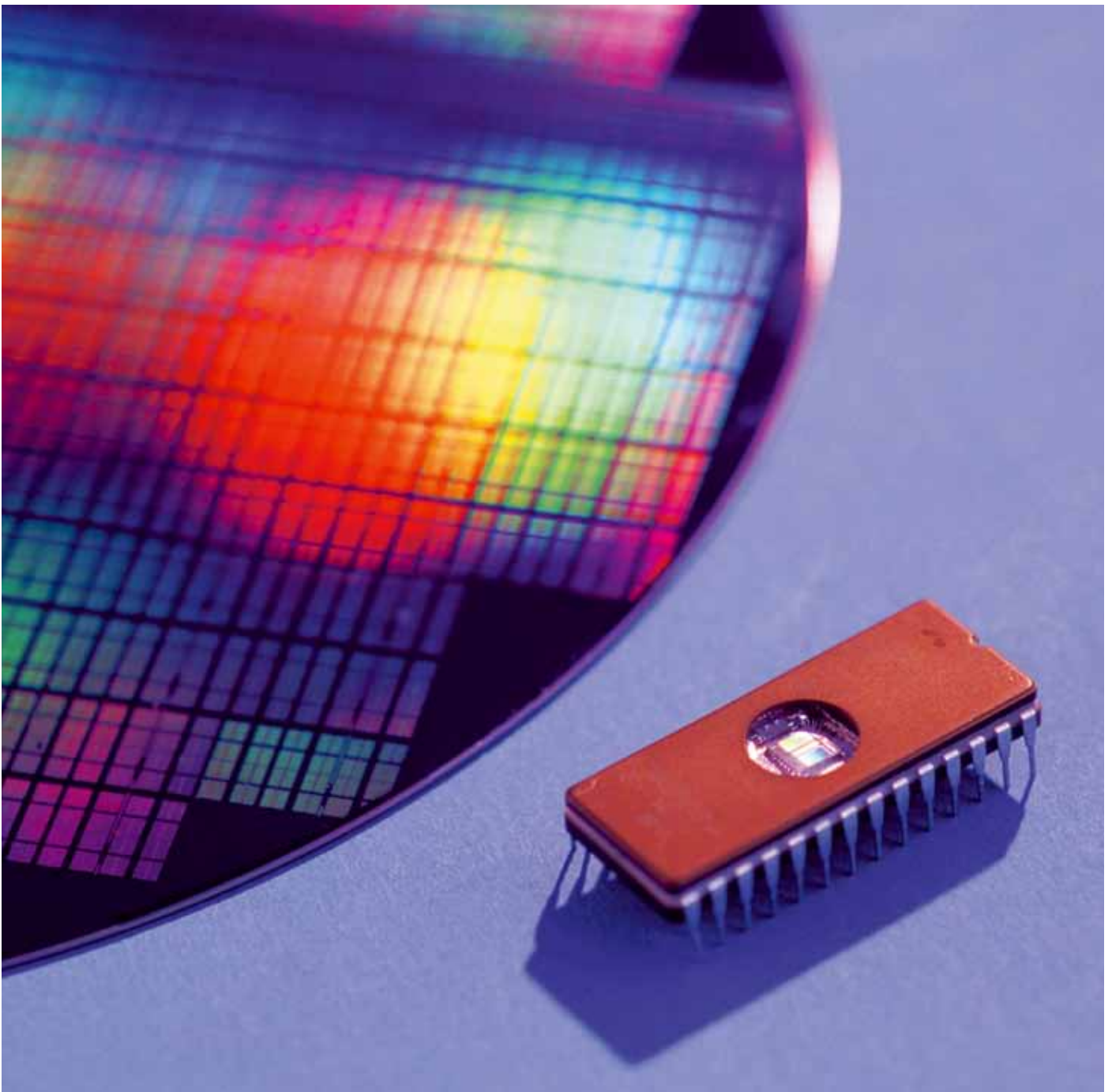


Information Security Policy



AGRI-FOOD & BIOSCIENCES INSTITUTE (AFBI)

INFORMATION SECURITY POLICY

Reference:	AFBI POL 07/09
Board Approval:	27 May 2009
Version:	1.2 (August 2011)
Author:	Biometrics & Information Systems Branch

Version Control

Version 1.0	May 2009	
Version 1.1	January 2010	• List of current post holders modified
Version 1.2	August 2011	• List of current post holders modified • Layout enhancements

1	INTRODUCTION	4
2	POLICY OBJECTIVE	4
3	SCOPE OF THIS POLICY	4
4	INFORMATION SECURITY POLICY	6
4.1	Policy Status	6
4.2	Risk Assessment	6
4.3	Security Documentation	6
4.4	IT System Accreditation	6
4.5	Physical Security	6
4.6	Incident Reporting	6
4.7	Technical Security	6
4.8	Education and Training	7
4.9	Systems Development	7
4.10	Business Continuity Management	7
4.11	Sanctions	7
4.12	Compliance	7
5	DEFINITION OF SECURITY MEASURES	8
5.1	Introduction	8
5.2	Identification and Authentication	8
5.3	Logical Access Controls	8
5.4	Accounting	9
5.5	Audit	9
5.6	Reliability of Service	9
5.6.1	Security Testing	9
5.6.2	Software Integrity	9
5.6.3	Protection Against Malicious Software	9
5.6.4	Software Distribution	10
5.6.5	System Input / Output Controls	10
5.6.6	Content Scanning	10
5.6.7	Data Confidentiality over Networks	10
5.6.8	Network Access Controls	10
5.6.9	Message Security	10
5.6.10	Mobile Code Protection	10
5.6.11	Anti-spamming Controls	10
5.6.12	Preservation of Message Sequencing	10
5.6.13	Operations Controls	10
5.6.14	Network Administration Controls	11
5.6.15	Software Maintenance Controls	11
5.6.16	Hardware Maintenance Controls	11
5.6.17	User Controls	11
5.6.18	Document / Media Controls	11
5.6.19	Recovery Options for Hosts	11
5.6.20	Business Continuity Planning	11
5.6.21	Back-up of Data	12
5.6.22	Capacity Planning	12
5.6.23	Equipment Failure Protection	12
5.7	Physical and Personnel Security	12
5.7.1	Site / Building Physical Security	12
5.7.2	Accommodation Moves	13

5.7.3	Room / Zone Physical Security.....	13
5.7.4	Theft Protection.....	13
5.7.5	Physical Equipment Protection	13
5.7.6	Terrorist / Extremist Warnings	13
5.7.7	Delivered Item (DI) Protection	13
5.7.8	Bomb Detection	13
5.7.9	Internal and External Bomb Protection	13
5.7.10	Fire Protection.....	14
5.7.11	Water Protection	14
5.7.12	Power Protection.....	14
5.7.13	Environmental Protection.....	14
5.7.14	Personnel	14
5.7.15	Data Protection Legislation	14
5.7.16	Incident Handling	15
5.7.17	Compliance Checks	15
6	ADMINISTRATION OF SECURITY	16
6.1	Roles, Responsibilities and Functions.....	16
6.2	Senior Information Risk Owner (SIRO)	16
6.3	Responsibilities.....	16
6.4	Senior Responsible Owner (SRO).....	16
6.5	Accreditor.....	17
6.6	Security Manager.....	17
6.7	Users	17
6.8	Managers.....	18
6.9	Security Consultants.....	18
6.10	Accreditation Authorities.....	18
7	GUIDANCE	18
8	VALIDITY OF THIS POLICY	18
9	REFERENCES	18
10	CURRENT POST HOLDERS – AUGUST 2011.....	19
	APPENDIX A: SAFEKEEPING OF PORTABLE AFBI ASSETS GUIDELINES	20
1	Staff Responsibilities	20
2	Care Of Assets In The Office	20
3	Taking Assets Out Of The Office.....	20
4	In Transit.....	20
5	Taking Assets Home	20
6	Asset Registers	20
7	Asset Marking.....	21
8	Action In The Event Of Theft Or Loss	21
9	Further Information	21
	APPENDIX B: AFBI REMOVABLE STORAGE MEDIA GUIDELINES	22
1	Malicious Software	22
2	Marking and Storing Removable Media	22
3	Loss of Removable Media.....	23
4	Further Information	23

1 INTRODUCTION

This document defines the Information Security Policy for the Agri-Food & Biosciences Institute (AFBI) network. The establishment of, and adherence to, an Information Security Policy is an essential component for ensuring the security of AFBI's business. This policy is the basis of the security standards which in turn establish the foundations for building the procedures and controls necessary for each business area to secure its information systems. Clear, understandable policy statements protect AFBI, its information assets and the organisations with whom AFBI interacts.

The term "information system" is used throughout this policy and is defined as the hardware, system and application software, communication components, physical environment and, primarily, information assets which together form a business domain. It should be noted that a domain may consist of one or more information systems.

AFBI Information Systems is headquartered at Newforge Lane, Belfast and is managed by AFBI Biometrics & Information Systems Branch (BISB) staff located there. The underlying AFBI network is accessible from eight locations throughout Northern Ireland.

This Information Security Policy applies to all business functions within the defined scope and covers all information systems which support those business functions. It has been developed in line with the provisions of HMG incorporating BS ISO/IEC 27001.

This document, therefore:

- Sets out AFBI's policy for the protection of the confidentiality, integrity and availability of its information systems;
- Establishes the baseline security responsibilities for information security;
- Provides reference to other related documentation.

This policy is not protectively marked on the grounds that it contains no protectively marked information or any facts which could compromise information systems security.

Information processed, stored and transmitted by AFBI Information Systems has been assigned a protective marking of RESTRICTED. The network itself therefore attracts a protective marking of RESTRICTED.

Specific policy requirements are given in detail later in this document.

2 POLICY OBJECTIVE

The objective of this policy is to ensure adequate security of AFBI's information systems, all of which adhere to AFBI's overriding business objectives, particularly:

- To preserve Confidentiality by protecting assets against unauthorised disclosure
- To preserve Integrity by protecting assets from unauthorised or accidental modification
- To retain Availability by ensuring that assets are available as/when required

3 SCOPE OF THIS POLICY

This policy is owned by AFBI and applies to all IT resources and equipment managed, supported, owned or leased by AFBI, and to all staff - permanent and temporary, contractors and their employees and anyone else with access to AFBI IT resources and network services.

The number of identified authorised users of AFBI Information Systems is circa 650.

An “authorised user” of AFBI Information Systems is defined as any AFBI staff member or contracted (non-AFBI) other, including agency staff, student and visiting worker, who has approval to access AFBI Information Systems to input, store or process information. All authorised users shall have Baseline Standard security clearance as defined in the HMG Manual of Protective Security (MPS) or shall be compliant with the AFBI Visiting Worker Information Security Policy (VWISP).

There may be instances where, for business reasons, it is not possible or practical to grant either formal clearance (for example, where a third party is contracted to undertake an ad hoc maintenance job) or apply the VWISP. Such instances shall be kept to an absolute minimum, and the party concerned (e.g. the contractors) must be closely supervised throughout.

Third party contractors granted long-term access shall have their access restricted on a need-to-know basis. Contract staff required to work on HMG systems for a significant period shall have Baseline Standard security clearance. AFBI Senior Responsible Owner (SRO) advice in this regard shall be sought.

4 INFORMATION SECURITY POLICY

The overall AFBI Information Security Policy statement is:

“AFBI’s information systems will be available when needed, will be accessed only by legitimate users and will contain complete and accurate information. The information systems will also be able to withstand, or recover from, threats to their confidentiality, integrity and availability.”

To satisfy this overall policy statement, AFBI will implement security measures, commensurate with the value of AFBI’s assets, to protect its information systems with priority given to those systems which are considered to be critical to the business.

The following statements represent the minimum information security policy applicable to all of AFBI’s information systems.

4.1 Policy Status

This policy is subordinate to HMG’s Information Security Policy (as defined in the Manual of Protective Security), the NICS Information Security Policy and the NICS Community Security Policy and Code of Connection.

4.2 Risk Assessment

All risk assessments will be conducted using the HMG Infosec Standard No 1.

Risk assessments will cover all information systems that are used to support business processes. Risk assessments will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

4.3 Security Documentation

The SYOPS must be approved by the AFBI SRO, prior to the implementation of the information system.

All staff will be made aware of the contents and implications of the SYOPS.

4.4 IT System Accreditation

The SRO will be supported by the Security Manager in ensuring that information systems do not pose an unacceptable security risk to AFBI.

4.5 Physical Security

All AFBI assets must be uniquely identified.

All AFBI assets must be recorded in an effective configuration management system.

The Security Manager will retain a register of all information systems, including their assets, which fall within the scope of this policy.

Physical assets, such as computer hardware, must be located with due consideration given to their value in security terms and following an assessment of the relevant risks.

4.6 Incident Reporting

All actual, attempted or suspected security breaches must be reported to the Security Manager and relevant security incidents will be reported in accordance with the requirements of GOVCERTUK.

All incidents reported to the Security Manager will be investigated.

4.7 Technical Security

There must be measures in place to protect AFBI’s information systems from viruses and other malicious software.

All contracts with third party organisations must consider necessary security requirements and must take into account the terms of this information security policy.

All information systems will be monitored for potential security breaches.

All use of the Internet and E-mail will be made in accordance with the provisions of the NICS policy CSC 02/03 entitled, "Internet and Email Usage Policy".

4.8 Education and Training

All users of information systems will be provided with the necessary security guidance, awareness and, where appropriate, formal training to enable them to effectively discharge their security responsibilities.

4.9 Systems Development

All business cases or feasibility studies for new projects must include estimated costs for information system security (including business continuity).

4.10 Business Continuity Management

Business Continuity Plans will be produced for AFBI information systems.

4.11 Sanctions

All staff must be informed that irresponsible or improper actions which breach this policy, any other AFBI policies or frameworks, or SYOPS, may result in disciplinary action.

Where a member of staff is found to have broken the law then the matter will be reported to, and dealt with by, the appropriate authorities.

4.12 Compliance

AFBI will comply with all laws, statutory requirements and legislation which are relevant to its information systems. This should include, but is not limited to, the following

- Official Secrets Act 1989
- Human Rights Act 2000
- Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Civil Evidence Act 1968 and Police and Criminal Evidence Act
- Wireless Telegraphy Act 1949
- Communications Act 2003
- Human Rights Act 1998
- Telecommunications Regulations 2000
- Civil Contingencies Act 2004

The SRO and Security Manager reserve the right to carry out checks on, or commission an independent assessment of, the actual implementation of security measures based on the claims made in any security operating procedures.

5 DEFINITION OF SECURITY MEASURES

5.1 Introduction

This section describes the specific measures which shall be taken to achieve a level of security which is commensurate with the value of the AFBI network and its data. Each of these measures is expressed as a policy statement. Together with the implementation of appropriate technical countermeasures and SYOPS, the policy statements below satisfy the security requirements of the AFBI network and its information.

There have been no exceptional risks identified, and the general risks outlined in the HMG Infosec Standard No. 1 may be assumed. The risks are not negligible, but they are adequately countered by the security measures defined in this policy and the supporting SYOPS documents.

5.2 Identification and Authentication

User IDs shall ensure that activities can be traced to individuals.

Passwords shall be sufficiently long so that they are difficult to guess or determine from the encrypted form.

Passwords shall be stored in a form that no-one, not even the Network Administrator, may see the password chosen by the user.

Passwords shall be generated in a manner which makes them difficult for unauthorised people to guess.

Users shall follow good security practices in the selection and use of passwords.

Passwords shall be changed frequently to assist in ensuring that the confidentiality of the password continues to be maintained.

Passwords shall be distributed to users in such a manner that the confidentiality of the password is maintained.

The log-on dialogue shall not assist unauthorised users in any attempt to gain unauthorised access.

Access by remote users shall be subject to authentication.

5.3 Logical Access Controls

The owner of a file or program shall be provided with the facility to specify who is allowed to access the file or program.

The time that a workstation can remain inactive shall be minimised to reduce the opportunity for an unauthorised person to masquerade as a legitimate user.

Assets shall be accounted for to help ensure that adequate security protection is maintained.

There shall be a formal registration and de-registration procedure for access to all multi-user information networks and services.

Access to privilege functions shall be restricted to those people who have a need to use such functions.

The user's access rights shall be reviewed in order to maintain effective control over access to data and IT services.

Application systems shall:

- control user access to data and application system functions;

- provide protection from unauthorised access for any utility software;
- not compromise the security of other systems with which IT resources are shared.

Access to the audit trail shall be safeguarded to prevent any possible misuse or compromise.

Clear policies and guidelines are required to control the business and security risks associated with electronic office systems.

5.4 Accounting

Sufficient information shall be recorded to enable a thorough review of any suspected incident to be completed.

The time events occur may be significant in investigating any security incident. It is therefore important that all clocks of connected systems are working to a common standard.

The Accounting Log shall be retained for a period commensurate with business requirements. The condition of the Accounting Log shall be assured.

The Accounting Log shall have sufficient capacity.

5.5 Audit

Auditing is closely related to Accounting but is concerned solely with the security relevant events which take place on the network. A range of facilities for analysing accounting logs shall be provided.

The audit trails shall be reviewed to ensure that users are only performing processes that they have been explicitly authorised to carry out.

When incidents are detected or suspected, they must be investigated in a thorough manner which can not be compromised.

Audit requirements and activities involving checks on operational networks shall be carefully planned and agreed, to minimise the risk of disruptions to business processes.

Access to network audit tools i.e. software or data files, shall be safeguarded to prevent any possible misuse or compromise.

5.6 Reliability of Service

5.6.1 *Security Testing*

Acceptance criteria shall be established against which suitable tests shall be carried out, prior to acceptance of the system, to provide the required level of security.

Tests shall be conducted prior to acceptance of the system to provide the required level of security.

5.6.2 *Software Integrity*

The integrity of software shall be maintained in live use.

5.6.3 *Protection Against Malicious Software*

Procedures shall minimise the potential for the introduction of malicious software into the IT network.

The IT network shall be monitored for potential malicious software activity.

Any identified malicious software shall be isolated and removed.

5.6.4 Software Distribution

Software integrity shall be preserved whilst it is being distributed in order to ensure that no unauthorised amendments have been made.

Software shall be exported in a manner that will help the party receiving the software to check its integrity.

5.6.5 System Input / Output Controls

The classification / protective marking of the information needs to be exported with the information in order that the receiving system can impose an equivalent level of access control.

5.6.6 Content Scanning

E-mail messages shall be checked in order to detect cases where people are misusing such facilities.

The web sites that users are visiting shall be monitored in order to detect cases where people are misusing such facilities.

5.6.7 Data Confidentiality over Networks

The confidentiality of information in transit over networks shall be protected.

5.6.8 Network Access Controls

The application shall be identified to the network.

Mutual Authentication shall be used to verify the communicating entities.

User access shall be segregated across networks, especially when connected to third party networks.

Connection to the Internet needs to be secured.

Care shall be taken to protect the integrity of electronically published information.

5.6.9 Message Security

Submission acknowledgement shall be used to prove that a message was sent.

5.6.10 Mobile Code Protection

External organisations must not be able to track which sites users have visited previously.

5.6.11 Anti-spamming Controls

Mechanisms and procedures shall be in place to detect cases where large quantities of unwanted messages are being received and help deal with such messages.

5.6.12 Preservation of Message Sequencing

A mechanism shall be used to ensure that messages are delivered in sequence.

5.6.13 Operations Controls

There must be formal procedures to cover all operator actions.

Operational staff must maintain a log of their activities.

Faults must be reported and corrective action taken.

Personnel procedures must be in place to ensure that no undue reliance is placed on any individual.

Operator activity must be monitored to minimise accidental errors and malicious actions.

Network operations shall be controlled.

Network managers should implement controls to ensure the security of data in networks, and the protection of connection devices from unauthorised access.

The risks from using an external contractor to manage information processing facilities must be identified and appropriate controls agreed with the contract and incorporated into the contract.

5.6.14 Network Administration Controls

Formal management responsibilities and procedures are necessary to ensure satisfactory control of all changes to equipment, software or procedures.

Periodically, it is necessary to change the Operating System (e.g. when installing a new version). When such changes occur the security of the system shall be reviewed to ensure that it has not introduced any adverse affects.

The System Managers Accounts are, on most IT systems, the most powerful accounts on the system. Access to these accounts shall be controlled.

As far as possible, vendor supplied software packages shall be used without modification. In circumstances where it is deemed essential to modify the software package, the modification must be strictly controlled in order to maintain the integrity.

5.6.15 Software Maintenance Controls

The identity of software maintenance engineers shall be checked to reduce the risk of unauthorised people gaining access to the information.

When software is being maintained there is a risk that errors may be made which could lead to a loss of availability, disclosure or modification of information, so such work shall be checked.

5.6.16 Hardware Maintenance Controls

All key equipment shall be supported by a maintenance contract.

Access by maintenance staff must be controlled.

5.6.17 User Controls

The work user's conduct shall be checked to ensure that it is both accurate and authorised.

5.6.18 Document / Media Controls

An information classification scheme shall be used to define an appropriate set of protection levels and communicate the need for special handling measures.

5.6.19 Recovery Options for Hosts

Hosts shall be available when required.

5.6.20 Business Continuity Planning

Business continuity plans shall be prepared.

Business continuity shall begin by identifying events that can cause interruptions to business processes.

Plans shall be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes.

Business continuity plans need to be tested to ensure that they are workable.

Business continuity plans need to be maintained to ensure that they continue to be workable.

Organisations shall have plans in place that will assist them in handling any crisis.

5.6.21 Back-up of Data

Back-ups of data shall be taken to ensure the continued availability of data.

Suitable back-up technology shall be used.

5.6.22 Capacity Planning

Procedures shall be regularly activated to help minimise the risk of system failure because of overloading.

Software facilities shall be available to help ensure that the risk of system failure because of overloading is minimised.

Acceptance criteria for new information systems, upgrades and new versions should be established.

5.6.23 Equipment Failure Protection

The availability of information shall be maintained by ensuring proper equipment usage.

The availability of information shall be maintained by providing equipment support.

The availability of information shall be maintained by providing a resilient equipment architecture.

5.7 Physical and Personnel Security

5.7.1 Site / Building Physical Security

The construction of the building often provides the first line of defence against an external attacker trying to gain access. It must be of sufficient strength to either prevent or deter likely attackers from forcing unauthorised entry.

The building's doors can be one of its vulnerable access points so these doors must be sufficiently strong to either prevent or deter an attacker from forcing unauthorised entry.

Staff passes shall be used both as a means of identifying staff when entering the building and differentiating between staff and visitors once in the building.

Control must be exercised over who may enter the building.

Windows, particularly those on the ground floor or other parts of the building which it is easy to gain access to, can be one of the vulnerable access points. These must be protected to prevent or deter an attacker from forcing unauthorised entry.

The perimeter of the site must be the first line of protection against an unauthorised person attempting to gain physical access to a site.

Security lighting shall be installed in order to allow: guards to see intruders before they reach their objectives, conceal guards from intruders, deter intruders and hinder intruders from their purpose.

Control must be exercised over the entry of visitors in to the building to reduce the risk of them gaining unauthorised access to information held in the building.

Control must be maintained over the entrances to the building to ensure that only authorised people may enter.

Guards will be employed to provide a deterrent to criminals and to others who might plan a covert attack.

5.7.2 Accommodation Moves

The confidentiality of Commercially Sensitive information shall be protected whilst it is in transit.

5.7.3 Room / Zone Physical Security

The room must be designed to reduce the risk of unauthorised access. The level of protection offered by a room depends on the strength and structure of the walls, floor and ceiling.

The access to keys to those rooms which are kept locked when unattended must be controlled in order to maintain the security of the room.

Additional controls and guidelines shall be required to enhance the security of a secure area.

Equipment installed in user areas, e.g. workstations or file servers, requires specific protection from unauthorised access when left unattended for an extended period.

5.7.4 Theft Protection

There shall be measures in place to detect occurrences of theft.

There shall be measures in place to prevent the theft of assets.

5.7.5 Physical Equipment Protection

The physical security of equipment processing, storing or transmitting information shall be maintained.

Equipment shall be sited or protected to reduce the risk from environmental threats and hazards, and opportunities for unauthorised access.

5.7.6 Terrorist / Extremist Warnings

When an indication is given that the level of threat is temporarily increased, it will be necessary to increase individual vigilance and to increase the level of surveillance and checking.

5.7.7 Delivered Item (DI) Protection

An isolated delivery and loading area shall be used to reduce the opportunity for the delivery of an improvised explosive device to critical areas.

5.7.8 Bomb Detection

It is essential that as much information on a telephone warning of a bomb is gathered as soon as possible. This will help to establish credibility of the warning and should also help with any subsequent investigation.

Staff must be given clear instructions on the correct action to be taken when a suspected package is found or a warning has been received.

Relevant staff shall be able to identify a suspicious package or device and take appropriate actions.

5.7.9 Internal and External Bomb Protection

The positioning of buildings, roads and car parks within a site shall be carried out in such a manner as to reduce the risks from explosive devices.

In order for the physical protection measures to be effective, a site survey shall be conducted to identify vulnerable points so that improvements can be made or additional surveillance can be provided at these points.

5.7.10 Fire Protection

Measures shall be in place to detect a fire at an early stage.

Measures shall be in place to ensure the safety of personnel in the event of a fire.

Measures shall be in place to prevent a fire occurring.

Measures shall be in place to ensure that if a fire breaks out it can be controlled.

5.7.11 Water Protection

Measures shall be in place to control the flow if water penetration occurs.

There shall be measures in place to prevent unwanted water entering the building / room.

5.7.12 Power Protection

Power equipment shall be installed according to all relevant regulations.

The system shall be provided with a conditioned power supply.

The system shall be provided with a resilient power supply.

Procedures shall be provided to manage the power supply during emergency conditions.

5.7.13 Environmental Protection

The correct operating environment shall be provided for the IT equipment.

The facilities that support the working environment need to be managed to ensure that they are operating correctly and are being well maintained.

5.7.14 Personnel

Applications for employment shall be screened.

The terms and conditions of employment must state the employee's responsibilities for information security.

Job descriptions shall be clearly defined.

Users shall sign a Confidentiality Agreement.

Disciplinary processes shall be in place to deal with security breaches.

5.7.15 Data Protection Legislation

The organisation must have a clearly defined Data Protection Management Structure.

The Data Protection Officer shall provide the Data Protection Commissioner with a notification of arrangements for personal data processing.

A number of countries making up the European Economic Area have introduced legislation placing controls on the processing and transmission of personal data. Such controls impose duties on those collecting, processing or disseminating information.

The Data Protection Officer shall ensure that Data Subjects' rights are enforced in relation to the processing of their personal information.

The Data Protection Officer shall ensure that all staff receive Data Protection awareness training.

Regular reviews shall be undertaken of the personal information and the reasons for its processing.

5.7.16 Incident Handling

Security incidents must be detected, any damage managed and lessons learnt disseminated.

Security weaknesses must be reported to enable analysis of security incidents.

Procedures shall be established for reporting software malfunctions.

There shall be mechanisms in place to enable the types, volumes and cost of incidents and malfunctions to be quantified and monitored.

Adequate evidence shall be gathered that would be able to support an action against a person or organisation.

5.7.17 Compliance Checks

All relevant statutory, regulatory and contractual requirements shall be explicitly defined.

Legal restrictions on the use of software in respect to intellectual property rights shall be adhered to.

Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect to intellectual property rights.

Checks shall be made to ensure that security measures are implemented as required and used properly to avoid security breaches and non-fulfilment of statutory, regulatory and contractual requirements.

6 ADMINISTRATION OF SECURITY

6.1 Roles, Responsibilities and Functions

It is important is that responsibilities are clearly assigned and that individuals are held accountable.

This policy shall be updated to reflect changes in personnel.

6.2 Senior Information Risk Owner (SIRO)

The appointment at board level of a SIRO is critical as it sends a clear message to the organisation that the ownership of information risk is considered a strategic responsibility in the same way as financial and legal risks to the business are. The role of the SIRO or Information Assurance (IA) Champion is to understand how the strategic business goals of the organisation may be affected by failures in the secure use of the organisation's information systems.

6.3 Responsibilities

The board, but principally the SIRO on behalf of the board, is responsible for ensuring that:

- a) An organisational structure is established for the delivery of effective IA. This should include an effective process for achieving security awareness and accountability;
- b) Funding is available to train staff who have IA responsibilities to meet recognised professional IA standards (ITPC, IISP, CISSP etc);
- c) IA requirements are addressed in strategic planning and are accepted as an integral part of the business;
- d) Security policies (are produced to) ensure consistency across the organisation and compliance with relevant laws, regulations and IA standards;
- e) Contingency planning in the form of disaster recovery, business continuity and forensic readiness plans are produced and comply with recognised National and International Standards and good practice guidance;
- f) There is an assurance process to monitor and maintain the effectiveness of the corporate IA policies and plans;
- g) All risk management decisions are justified and accountable in the context of the business requirement and there is a clear understanding of the potential business impact;
- h) An escalation process is established to resolve conflict with or exceptions to corporate IA requirements (business objectives and risk tolerance);
- i) Where an information system crosses organisational boundaries, or connects to a multi-organisational service, controls and reporting mechanisms are in place to support the wider IA governance requirements;
- j) Staff with delegated authority are in place to monitor and manage risk and are aware that they are accountable to the board.

6.4 Senior Responsible Owner (SRO)

The SRO is responsible for managing the information risk for specific programmes or projects to ensure they meet the objectives agreed with the SIRO and Board level business owners. The SRO must understand the IA risks to the programme or project and how it may impact the strategic goals of the programme or project. The SRO is also responsible for ensuring that information risk management processes are carried out

within the programme or project. The SRO cannot assume ownership of any corporate risks that are incurred outside the scope of their particular programme or project.

6.5 Accreditor

The role of the Accreditor is to act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting the business requirement and to formally accredit that system on behalf of the board. Although it is necessary for the Accreditor to have an understanding of ICT related technology, the role does not require a deep technical knowledge. Indeed, it is necessary for the Accreditor to step back from the technical detail and consider risk management in the round to ensure the physical, personal, procedural and technical controls are balanced. It is important therefore, that the Accreditor has access to people who have a professional technical understanding of the technologies involved, to support the accreditation process. To support this requirement, funding should be identified at the outset for any specialist technical advice and services such as Technical and IA Consultants, IT Health Checks and assurance services.

Accreditors are accountable for their decisions and actions in their role as IA risk assessors and risk managers. They can be called to account for their business actions in a legal proceeding but are not liable in law. This standard supports the need for accountability in the business process and the traceability of risk management decisions.

6.6 Security Manager

The Security Manager's role is to provide the day to day security management of the information system, responsibilities could include:

- a) Implement the Risk Management plan.
- b) Verify that appropriate security testing is conducted and documented.
- c) Ensure that the accreditation support documentation is developed and maintained.
- d) Review the accreditation management plan and the re-accreditation schedule and plans.
- e) Ensure that any proposed system changes are formally reviewed and that implemented system modifications do not adversely affect the security of the system.
- f) Ensure contingency plans are produced and tested.
- g) Ensure the activities of the users comply with security policies and procedures.
- h) The Security Manager should not be the system administrator.

6.7 Users

All users must accept a level of responsibility for information risk ownership when using the organisation's information systems. This includes:

- Safeguarding assets, particularly information, in their care.
- Understanding and abiding by the provisions of all AFBI policies and frameworks governing the use of IT resources.
- Preventing the introduction of malicious software on AFBI's IT systems.
- Reporting any actual, attempted or suspected breaches of security.

However, it is the responsibility of the SIRO and those with delegated responsibility for IA to ensure that all users are aware of the risks and that they formally acknowledge their

acceptance of the corporate security policies and user guidance specific to the system they are using.

6.8 Managers

Line Managers are directly responsible ensuring that

- AFBI's assets used by staff are used in a secure manner under the terms of this policy
- their staff are aware of their security responsibilities
- their staff have had appropriate security training

6.9 Security Consultants

Unless prior authorisation is given, all contact with external security consultants or other computer security authorities shall be made through the Security Manager.

6.10 Accreditation Authorities

As AFBI Information Systems is RESTRICTED, re-accreditation will be required either on the expiry of any previous Accreditation Certificate, or at the Accreditor's request, whichever is earlier.

Preparation of the accreditation documentation for accreditation shall be the responsibility of the AFBI SRO and the AFBI Security Manager.

Internal accreditation from the DARD Accreditor shall be sought on behalf of the AFBI SRO.

External accreditation, which is a requirement for connection to the NICS Public Service Network RESTRICTED domain (NIGOV.NET), shall be sought from the NICS Accreditation Panel.

7 GUIDANCE

Detailed advice on how to determine and implement an appropriate level of security of AFBI's information systems is available from the AFBI Accreditor and the AFBI Security Manager.

8 VALIDITY OF THIS POLICY

This policy is reviewed annually by the AFBI Accreditor acting under the authority of the Chief Executive. Associated information security standards are subject to an on-going development and review programme.

9 REFERENCES

Related documents include:

- HMG Infosec Standard 1, "Technical Risk Assessments"
- HMG Infosec Standard 2, "Risk Management and Accreditation of Information Systems"
- HMG Manual of Protective Security (MPS)
- DARD IT Security Policy
- NICS Information Security Policy
- NICS Community Security Policy and Code of Connection

10 CURRENT POST HOLDERS – AUGUST 2011

Senior Information Risk Owner (SIRO)	Seamus Kennedy, AFBI CEO
Senior Responsible Owner (SRO)	David Armstrong, AFBI Head of ICT
Accreditor	David Kilpatrick, AFBI Head of Biometrics & Information Systems
Security Manager	John Ward, AFBI Head of IT Infrastructure & Support

APPENDIX A: SAFEKEEPING OF PORTABLE AFBI ASSETS GUIDELINES

The purpose of this Memo is to advise staff on measures which should be taken to minimise the risk of loss or theft of assets which are attractive and easily transportable, for example laptop computers, digital cameras, mobile phones, blackberries, petty cash etc.

1 STAFF RESPONSIBILITIES

Staff who have use of and access to such an asset should be advised that they are responsible for its safekeeping and for the security of any information it contains.

2 CARE OF ASSETS IN THE OFFICE

Equipment assets should not be left lying on desks or in offices when it is not being used. When not in use, and particularly outside working hours, they should be stored in suitable locked metal or wooden furniture. Equipment which holds protectively-marked material should be handled in accordance with the highest protective marking.

3 TAKING ASSETS OUT OF THE OFFICE

Equipment, information or software should not be taken off-site without authorisation. Where necessary and appropriate, equipment should be logged out and logged back in when returned. Spot checks should be undertaken to detect unauthorised removal of property. Individuals should be made aware that spot checks will take place.

Assets such as laptops, digital cameras etc should therefore only be taken out of the office by staff who have been given permission to do so and only when needed for business purposes. Heads of Branches may wish to consider putting in place a system to log such items 'in' and 'out'.

4 IN TRANSIT

Assets such as laptops and digital cameras should be placed securely in the boot of the vehicle before the journey starts - they should not be placed on seats or in footwells even on short journeys. Other assets such as mobile phones and blackberries should be kept in bags or pockets. Assets should not be left in unattended vehicles.

Particular care should be exercised when using public transport (i.e. bus, train, taxi etc.). The asset should remain in the officer's possession and not be left on luggage shelves or bays.

Where possible, consideration should be given to using a carrying case other than that of the manufacturer. This may reduce attention being drawn to a laptop, camera etc.

5 TAKING ASSETS HOME

Assets should only be taken home by staff who have been given permission to do so and only when needed for business purposes. Staff should be given advice about the measures required to protect the asset and any information it holds, particularly where protectively marked material is involved. Portable assets should be stored at home as they should be in the office i.e. they should not be left lying around but should be locked away when not in use and handled in accordance with the highest protective marking of any material which the asset holds.

6 ASSET REGISTERS

Branches holding such assets should consider setting up and maintaining an asset register if they have not already done so. The register should be frequently audited (spot checked). Details on the register should include:

- Asset number

- Serial Number of the asset (or other unique identifier e.g. IMEI Number for mobile telephones, Vehicle or plant Identification Number etc.)
- Description (model, colour, size etc)
- Purchase date and supplier
- Value
- If the asset has been “marked” the location of the mark on the item

7 ASSET MARKING

A wide range of easy-to-use methods to mark assets is available and should be considered especially for valuable assets and those holding protectively marked information. Visibly marking property makes it less attractive to thieves, helping to protect it.

8 ACTION IN THE EVENT OF THEFT OR LOSS

The police must be informed as soon as a theft or loss of any asset taken outside the office is discovered or suspected and an incident (serial) number obtained from PSNI. Such incidents, and incidents of actual or suspected theft or loss within offices, should also be reported to the AFBI Personnel Manager. In the event of the loss or theft of a mobile phone or a PDA (e.g. Blackberry) the AFBI Security Manager should be advised so the Service Provider is instructed to block the handset and SIM card. Refer to CESG Security Procedures for Blackberry Users.

9 FURTHER INFORMATION

If you have any queries on any aspect of this advice please contact the AFBI IT Security Manager, John Ward, on 028 90255626.

APPENDIX B: AFBI REMOVABLE STORAGE MEDIA GUIDELINES

There are many forms of removable storage media. This is defined as physical media that can be physically inserted into the computer or removed from the computer. This would include floppy disks, flash, CDs, DVDs, tape, firewire and USB devices. This list is not exhaustive as other technologies become available. Examples of USB devices include memory sticks, external hard drives, printers, cameras, mobile phones, iPods, MP3 players and watches.

Staff must ensure that appropriate care is taken in protecting any personal data on staff, customers or citizens on removable storage media. Staff should consider carefully the implications if the data was lost and based on a risk assessment determine if it should be held on removable media at all. If it must, staff should consider if password protection or encryption is appropriate. If encryption is deemed appropriate, staff should contact the Security Manager (John Ward, ext 55626). Any bulk transfer of data should be sanctioned at Head of Branch level or above.

There are two sources of removable storage media and these are AFBI and non-AFBI. Non-AFBI includes but is not restricted to media that is owned by yourself, family and external organisations.

- AFBI media must only be connected to AFBI computers. It must not be connected to other computers except for WORM* media that contains non-protectively marked information.
- Non-AFBI media should not be connected to AFBI computers. If there is a requirement to connect Non-AFBI media, it must be scanned by BISB first.

**WORM media is media such as CDs and DVDs that are Write Once Read Many Times. This negates the ability of malware to copy itself onto removable media.*

If AFBI media has been connected to a non-AFBI computer then it must be taken to the BISB Service Desk for scanning before being connected to an AFBI computer.

If an external company needs to connect a USB stick for a presentation or demonstration of a product then they should bring a laptop with them and only connect their USB device to their own laptop.

If you need to work on a document out of the office then you can:

- use your AFBI laptop (if you have one).
- borrow a branch laptop.

1 MALICIOUS SOFTWARE

Malware is software that is developed for the purpose of doing harm. This includes computer viruses, worms, and Trojan horses.

Malware will use removable storage media to spread themselves and steal data & passwords.

The rules above are designed to ensure that malware is not passed from other computers to AFBI computers and that departmental data is not stolen.

A computer infected with malware will also steal the data from media connected to it.

2 MARKING AND STORING REMOVABLE MEDIA

All removable storage media should be labelled to identify the information and the highest protective marking of the data on the disk or device.

If Restricted information has been stored on them, then the device needs to be treated as Restricted even if the information is “deleted” as only the link to the information is deleted not the actual information itself.

3 LOSS OF REMOVABLE MEDIA

All loss of removable storage media (including theft) must be reported to the Security Manager.

4 FURTHER INFORMATION

For further advice please contact the AFBI IT Security Manager, John Ward on 028 90255626.