Policy & Guidelines - Information Security Policy

	Name
Author	G.I.S.O.
Checked by	Data Protection & Information Security Officers [DPISOs]
Approved by	Chief Officer's Group
Distribution	1) DPISOs.
	2) Staff via Intranet

Document Reference	IS/001

Version	Date	Change	No.
0.1	03/01/2001	Draft Document	
0.2	14/02/2003	Amendments following consultation with InfoSec Committee	
0.3	18/02/2003	Included clearer definitions of Confidentiality, Integrity & Availability	
1.0	06/05/2003	First Issue	
2.0	18/09/2006	Draft Document	
2.0	01/11/2006	Chief Officers Group for approval.	
2.0	28/03/2007	Issue.	

Table of Contents

1 OVERALL POLICY

It is Isle of Man Government* policy to ensure that all of its systems and the information they contain [information assets] are made secure from threats, whether internal or external, deliberate or accidental; while enabling those who are authorised to access the information to carry out their legitimate business.

This policy and associated standards and procedures aims to emphasise three principal properties relating to the security of information:-

- **Confidentiality** – must be able to share information among individuals and organisations that need the information, while not allowing access by individuals or organisations that do not have a need to know the information.

- **Integrity** – must be sure that information has not been corrupted, degraded or undergone any unauthorised modification. It is important that the information is accurate.

- **Availability** – information must be available to those who need it, when they need it and kept from those who do not need the information.

All breaches of information security, actual or suspected, shall be reported to departmental Data Protection & Information Security Officers [DPISOs], and investigated by them or brought to the attention of the Government Information Security Officer where required.

Business Continuity Plans for critical information systems shall be produced, maintained and tested for effectiveness at appropriate intervals.

2 ORGANISATION & RESPONSIBILITIES

2.1 IOM Government

IOM Government has an established senior management framework through which to initiate and control the implementation of information security within the organisation.

The Chief Officers Group shall accept overall responsibility for all matters relating to information security and will be responsible for:-

- the review and approval of corporate information security policies.
- reviewing and acting on matters arising from corporate security incidents.
- the co-ordination and response to information security threats and vulnerabilities

This Policy is mandatory and applies to all individuals whether employed on a permanent, part-time, temporary or locum basis, as well as third party and contract employees.

All elected members are to be made fully aware of this policy and of their duties and responsibilities to ensure the confidentiality, integrity and availability of information.

Where appropriate the policy should also be communicated externally, e.g. to contractors.

2.2 Government Information Security Officer (GISO)

The GISO will be responsible for:-

- the annual review and amendment [if required] of corporate information security policies.
- maintaining appropriate contacts with external authorities and within Isle of Man Government
- ensuring the day-to-day monitoring of security issues, and the consideration of issues.

2.3 Internal Audit

Internal Audit are responsible for examining and evaluating the adequacy and effectiveness of security controls, and for reviewing risk assessment records and risk treatment plans.

2.4 Line Management

Managers shall monitor their workplace to ensure that the confidentiality, integrity and availability of information is maintained, and where risks to information assets are identified they shall ensure that these are reported and that so far as is reasonably practicable action is taken to minimise or remove the risks.

Management duties include the following:

- ensuring that employees, contractors and visitors are made aware of their information security responsibilities.
- providing adequate training, information, instruction and supervision to staff to ensure that information is used in a secure manner when completing duties
- taking immediate and appropriate steps to investigate and rectify any risks to information security arising from the work activity
- bringing to the prompt attention of senior management any information security issue that requires attention.

2.5 Employees

All employees have a duty to co-operate with management to ensure the security of information and must work in accordance with information and training provided, refraining from intentionally mis-using or interfering with information systems, and reporting any security incidents or weaknesses without delay

IOM Government reserves the right to take disciplinary action against any employee who deliberately infringes the confidentiality, integrity or availability of information.

3 INFORMATION SECURITY MANAGEMENT SYSTEM

3.1 Policies & procedures

Where necessary, separate information security policies shall be developed by Departments detailing local, or system specific information security requirements. Departmental policies must be developed and read in conjunction with corporate information security policy documents.

A number of supporting policies and procedures have been developed at a corporate level and these will be implemented by all Departments. Corporate policies include Email and Internet policies, a Copyright policy, Information Classification Guidelines and Incident Reporting Guidelines.

British Standards “BS ISO/IEC 17799:2005 BS7799-1:2005, Information technology – Security techniques – Code of practice for information security management” will be referenced as “best practice” in the implementation of information security within IOM Government.

3.2 Regulatory compliance

All individuals whether employed on a permanent, part-time, temporary or locum basis, as well as third party and contract employees are required to comply with relevant legislation and regulations including:-

- Official Secrets Act 1920
- Copyright and Design Rights Acts 1991
- Computer Security Act, 1992
- Public Records Act 1999
- Data Protection Act, 2002
- Code of Practice on Access to Government Information – July 1996.

- Council of Ministers Instruction On The Security & Privacy of Government Documents – Nov 1996.
- IOM Government Financial Regulations.
- Code of Best Practice for the Maintenance of Information Security
- IOM Government Electronic Communications Policies

3.3 Risk Assessment/Risk Treatment

A corporate Risk Management Policy [May 2006] has been developed, and risk analysis shall be carried out by Departments on all business critical IOM Government information systems.

The results of the risk analysis shall be used to identify measures that can reasonably be taken to manage the risks, removing them or reducing them to an acceptable level.

Where any residual risks remain the "owners" of the information systems shall document their acceptance of the risks.

3.4 Security Awareness

It is IOM Government policy that all staff and contractors, whether full-time, part-time or temporary will be made aware of their responsibilities to protect the confidentiality, integrity and availability of information assets.

Normal management arrangements will ensure that a basic level of security awareness training is provided to all employees. In this respect managers and supervisors will play a key role, as it will be at this level of management that the most effective forms of staff instruction take place.

3.5 Security Incident Reporting

It is IOM Government policy to operate continuous monitoring and incident reporting of security aspects of each information system.

All significant security incidents, and security weaknesses shall be reported to the Government Information Security Officer [GISO] in accordance with Financial Regulations (FD15) and the procedures documented in the Incident Reporting guidelines.

*** NOTE: For the purposes of this document "IOM Government" is taken to comprise all of the Departments, Statutory Boards and bodies or offices of Government.**