GAMBLING COMMISSION

Information Security Management System (ISMS) Policy

June 2017

Version 1.1

Version History			
Version	**Date**	**Detail**	**Author**
0.1	18/02/2015	First draft	Andy Turton
0.2	20/02/2015	Updated following feedback from P2	Andy Turton
1.0	29/04/2015	Approved	Andy Turton
1.0	28/05/2016	Reviewed – No changes	Luke Traat
1.1	02/06/2016	Reviewed – No changes required	Luke Traat

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
5.2	Information Security Policy

RACI Matrix

A RACI matrix describes the participation by various roles in completing tasks or deliverables for a project or business process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes.

R	Andrew Turton
A	IAG
C	IAG
I	All Commission staff

R – Responsibility Those who do the work to achieve the task.

A – Accountable The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible.

C – Consultable Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.

I – Informed Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Contents page

Purpose

1. The purpose of this policy is to set out the Commission's aims and objectives for the management of information security. Information Security is defined as the preservation of confidentiality, integrity and availability of information.

2. The scope of the Information Security Policy covers the storage, access and transmission of information in the course of Commission business. It therefore applies to the conduct of staff, contractors, suppliers and others with access to that information (wherever the information or they are located) as well as the applications, systems, equipment and premises that create, process, transmit, host, or store information, whether in-house, personally owned or provided by external suppliers.

3. The Commission is committed to preserving the confidentiality, integrity and availability of all our key information assets in order to effectively deliver strategic goals and to maintain our legal and contractual compliance and reputation. The information security framework (comprising this policy, supporting policies, processes and tools and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing and for reducing information-related risk to acceptable levels.

4. This policy is owned by the Information Asset Group (IAG) who will:

   - Systematically examine the organisation's information security risks, taking, account of the threats, vulnerabilities, and impacts;
   - Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
   - Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.
   - Monitor the development of the ISMS to ensure continual improvement.

Individual responsibilities

All users

5. All individual users of Commission information systems and those handling or having access to Commission information outside of those systems shall be responsible for:

   a) Complying with all relevant information security, policies, practices and procedures including any external accountability;

   b) Ensuring that they request, where necessary, and receive adequate and relevant information security awareness training to enable them to undertake their roles; and

   c) Reporting information security incidents via the defined and approved channels.

6. Violation of information security policies may be grounds for disciplinary action up to and including dismissal.

Senior Information Risk Owner (SIRO)

7. The SIRO is ultimately responsible for managing the organisation's information risks, including maintaining an information risk register. The SIRO shall:

   a) Ensure that this policy and the information security objectives are compatible with the strategic direction of the Commission

   b) Own the risks associated with the information security objectives and ensure that control action owners are identified, including identifying key Information Assets and nominating Information Asset Owners

   c) Authorise acceptance or mitigation of significant information security risks that deviate from agreed standards

Information Asset Owners (IAOs)

8. IAOs are senior members of staff and form an integral part of the Information Assurance framework. IAOs shall:

   a) Lead and foster a culture that values, protects and uses information for the public good

   b) Know what information an asset holds, and what enters and leaves it and why

   c) Know who has access and why, and ensure their use of the asset is monitored

   d) Understand and address risks to the asset, and provide assurance to the SIRO

   e) Ensure the asset is fully used for the public good, including responding to access requests

Departmental Security Officer (DSO)

9. The DSO is required to manage day to day security arrangements, working to the corporate standards set out in the Security Policy Framework and risk assessment requirements of Cabinet Office and the Office of the Government SIRO. The DSO shall:

   a) Be responsible for maintaining security policies and guidance

   b) Monitor compliance to the ISMS

   c) Support IAG reviews

   d) Investigate security breaches

   e) Support IAOs in meeting their responsibilities

   f) Support in the accreditation of relevant systems

Information Technology Security Officer (ITSO)

10. The ITSO is responsible for managing IT related security issues. The ITSO shall:

    a) Support IAOs in their understanding, and mitigation of, IT related security risk

    b) Investigate security breaches

    c) Support in the accreditation of relevant systems

Information security objectives

11. The following are the Commission’s on-going security objectives:

    - Information is only accessible to authorised persons from within or outside the organisation and levels of access are determined by IAOs or by delegated authority
    - Confidentiality, Integrity and Availability of information and systems is maintained
    - Business continuity plans are established, maintained and tested
    - All personnel are trained on information security and are informed that compliance with the policy is mandatory
    - All breaches of information security and suspected weaknesses are reported and investigated and appropriate actions taken
    - Relevant procedures exist to support the policies in place
    - Regular audits of the processes and policies are conducted to ensure continuous review and improvement of the ISMS
    - New systems or services are deployed in a controlled and secure manner
    - As far as is possible the Commission avoids breaches of legal, regulatory and contractual requirements.

12. IAG will also identify specific security objectives that are reviewed annually. These are used to develop the ISMS, including the monitoring of:

    - Internal risks to confidentiality (such as printer checks and clear screen / clear desk compliance)
    - Risks which will impact on service delivery to external stakeholders (including the availability of eServices)
    - Risks to the availability of services and information (including business continuity testing)