An Garda Síochána

Policy Document

ICT Information Security Policy

Effective Date	12th November 2019
Version No.	1.0
Approved by	Garda Executive
Introduced by	[HQ Directive 056/ 2019]
Policy Owner	Executive Director, Information & Communications Technology

1. Purpose

Information resources in all its forms are vital business assets of An Garda Síochána and shall be adequately protected against all risks. The purpose of this policy is to define the organisation's approach to managing its information security objectives, as well as to set forth requirements that all personnel shall adhere to when utilising An Garda Síochána information resources. The Information Security Policy will act as the umbrella for all of An Garda Síochána Information Security procedure documents, to set out management and governance responsibilities within An Garda Síochána Information Communication and Technology Section, (Garda ICT).

2. Scope

This policy applies to all An Garda Síochána staff utilising An Garda Síochána information resources. This also applies to Police Officers from the Police Service of Northern Ireland (PSNI) seconded to An Garda Síochána in accordance with Section 53, Garda Síochána Act 2005.

3. Policy Statement

An Garda Síochána is committed to the development and implementation of Information Security policies and procedures that reflect best practice. To maintain best practice and consistency of application across the organisation, all managers, supervisors and all Garda Staff are expected to meet the standards outlined, and be accountable for any deviation from those standards defined in the Information Security policy and its accompanying procedure documents.

The Executive Director of Garda ICT is accountable for maintaining and governing 'Information Security' within An Garda Síochána, as well as executing the Information Security policies and procedures.

Garda ICT are responsible for the following under the ICT Information Security Policy:

- Establishing and maintaining an Information Security Management System (ISMS) that defines and audits Information Security processes across An Garda Síochána.
- Developing and maintaining the Information Security policies, procedures and guidelines for An Garda Síochána.
- Assessing and managing Information Security risk, through the development of people, processes and technology solutions that are implemented across the organisation.
- Defining and maintaining the minimum standard security controls.
- Managing compliance with, and exceptions to, Information Security policies, procedures and guidelines.
- Governing the design and operation of technology that enforces Information Security controls.
- Driving awareness and developing training on Information Security topics.
- Managing Information Security threats, incidents and breaches in accordance with the Information Security Incident Management Procedures.

Garda ICT will aim to do this, in part, by regulating all areas relating to An Garda Síochána information resources and information processing facilities, by governing and maintaining the following information security areas:

- Acceptable Use
- Encryption
- Asset Management
- Information Security Business Continuity Management
- Information Security Incident Management
- Access Control & User Identity Management
- IT Operations (ICT Management, Malware Protection, Backups, Vulnerability Management, Logging & Auditing)
- Printer Management

- Mobile Devices
- Physical & Environment Security

This policy and its accompanying procedure documents do not override any applicable data privacy and data protection laws and regulations to which An Garda Síochána is subject. It covers electronic data, computer systems, data networks, servers and personal computers (stand-alone or network-enabled), located at An Garda Síochána and non-Garda locations. This includes systems that are under the jurisdiction and/or ownership of An Garda Síochána, and all personal computers and/or servers authorised to access An Garda Síochána's data networks. The policy applies to, but is not limited to core policing systems, applications, databases, operating systems, source code, assets, mobile devices, computers, laptops, servers, networks, interfaces and middleware.

Violation of these policies may result in disciplinary and/or legal action.

The requirements stated in the associated procedure documents are minimum standards. It is always acceptable to implement measures that are more stringent than what is documented. Exceeding the minimum standards does not warrant an information security exception.

All alleged breaches of the guidelines outlined in this policy will be investigated and may result in: withdrawal of all information communication and technology facilities, disciplinary actions, and/or initiation of criminal or civil proceedings.

4. Compliance

Compliance with An Garda Síochána Information Security Policy and accompanying Procedures is mandatory for all members of An Garda Síochána, Garda Staff, and to Police Officers from the Police Service of Northern Ireland (PSNI) seconded to An Garda Síochána in accordance with Section 53, Garda Síochána Act 2005.

Staff may be held accountable for alleged infringements caused by any violations of the Information Security Policy and Procedures.

5. Related Documents

- Code of Ethics
- Data Protection for An Garda Síochána

6. Legal & Human Rights Screening

This document has been Legal and Human Rights screened in terms of the respective obligations placed on An Garda Síochána for the subject area concerned.

7. Ethical Standards & Commitments

Every person working in An Garda Síochána must observe and adhere to the standards and commitments set out in the Code of Ethics for An Garda Síochána and uphold and promote this Code throughout the organisation.

1. Policy & Procedure Review

This document and associated Policy will be reviewed 12 months from its date of effect and every three years thereafter or as appropriate.

2. Disclaimer

This document is not intended to, nor does it represent legal advice to be relied upon in respect of the subject matter contained herein. This document should not be used as a substitute for professional legal advice.

10. Policy & Procedure Document Feedback

The Policy and Governance Coordination Unit maintains a Policy Issues Log. Where there are potential issues regarding the implementation of the Procedures set out in this document, please forward an outline of same through the relevant Divisional Office to the Section mail-box policy.governance@garda.ie. Divisional submissions will be recorded in the Policy Issues Log and forwarded to the Policy Owner for whatever action deemed necessary.

*(**Please note** that where there is an urgent issue arising regarding the implementation of this Policy document and accompanying Procedure documents, it should be clearly flagged as urgent / important and also reported directly to First Line Supervisors/Managers to ensure it is addressed).*