Malta NSO

National Statistics Office
Uffiċċju Nazzjonali tal-Istatistika

ISU-POL-001: Information Security Policy

8 November 2022

1. Overview

1.1. This overarching Information Security Policy introduces the information security policies, procedures and guidelines that are or shall be in place, and the main information security responsibilities established, within the National Statistics Office.

2. Abbreviations

DPO: Data Protection Officer
ISMS: Information Security Management System
ISP: Information Security Policy
NSO: National Statistics Office
SoA: Statement of Applicability

3. Definitions

3.1. **Information Security Management System:** A set of interrelated or interacting elements of an organisation designed to establish information security policies, objectives, processes and controls to achieve those objectives.

3.2. **Information Asset:** A body of information defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.

3.3. **Supporting Assets:** All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described above, including:

- Premises; e.g. offices, data centres, storage facilities, recovery sites, etc.;
- Hardware; e.g. servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices;
- Media; e.g. optical disks, USB storage keys and paper;
- Software; e.g. operating systems, commercially available software applications and others developed internally by the NSO or external suppliers.

3.4. **Data Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

3.5. **Data Integrity:** The property that information is accurate and complete.

3.6. **Data Availability:** The property that information is accessible and usable upon demand by an authorised individual or entity.

3.7. **Information Security Incident:** A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

3.8. **Information Security Control:** Any administrative, management, technical or legal method that is used to manage information security risk. Controls are safeguards or countermeasures, including things like practices, policies, procedures, programs, techniques, technologies, guidelines and organizational structures.

3.9. **Asset Owner:** An individual who is recognised by the NSO as the person responsible for an Information Asset or a Supporting Asset.

3.10. **Control Owner:** An individual who is recognised by the NSO as the person responsible for an Information Security Control linked to an Information Asset or a Supporting Asset.

4. Policy Objectives

4.1. To direct the design, implementation and management of an effective ISMS, which ensures that the information assets of the NSO are properly identified, recorded and protected at all times.

4.2. To ensure the confidentiality, integrity and availability of the NSO's information assets and supporting assets (including information systems), as defined within the NSO's Inventory of Assets.

4.3. To ensure that all vulnerabilities, threats and risks to information assets and the supporting assets are formally identified, understood, assessed and controlled in accordance with the NSO's documented Risk Assessment and Risk Treatment Procedure; see [1].

4.4. To ensure that the NSO's employees, contractors and third-party users comply with this Information Security Policy (ISP) and all other applicable ISMS documentation, through the provision of effective information security training, awareness and ongoing monitoring activities.

4.5. To ensure that the NSO is able to maintain compliance with all applicable legislation and contractual requirements, and with any supporting management system certifications.

4.6. This policy is meant for internal purposes but can be made available to external parties (particularly entities who work closely with the NSO) upon request and authorisation from the Director General or Director for Data Resources, IT and Methodology.

5. Scope

5.1. The scope of the NSO's ISP shall include the following:

5.1.1. **Information Assets:** All information assets owned by the NSO or entrusted to the NSO by a stakeholder under an agreement which specifically details the NSO's responsibility for that data, or information assets held, processed or stored on the NSO's premises or stored at approved off-site premises or locations. For example, all data stored within the NSO's server computers, and all data printed on NSO documents.

5.1.2. **Supporting Assets:** All supporting assets that contribute to the collection, storage, processing, and transfer of the information assets as described in point 5.1.1, including:

- Premises; e.g. offices, data centres, storage facilities, recovery sites, etc.
- Hardware; e.g. servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices
- Media; e.g. optical disks, USB storage keys and paper
- Software; e.g. operating systems, commercially available software applications and others developed internally by the NSO or external suppliers

5.1.3. **Documentation and Records:** All policies, processes, procedures, work instructions and records related to the management, use, control and disposal of the information assets and their supporting assets as detailed above.

5.1.4. **All Company Personnel:** Permanent, temporary, full-time and part-time employees, authorised contractors and any third-party users of information systems.

6. Policy Statements

6.1. The NSO shall be committed to the protection of the information assets and supporting assets as defined within the scope of this policy.

6.2. The NSO has created its ISMS in accordance with the international standard on Information Security Management—ISO/IEC 27001:2013 [2]—which shall be followed in all information security-related activities, and it shall seek to retain compliance against this standard.

6.3. To effectively manage and deliver its ISMS, the NSO shall establish the following, among other constructs:

6.3.1. **Inventory of Assets:** Define and maintain a comprehensive Inventory of Assets, including all information assets and supporting assets as defined within Section 5 of this policy. The Inventory of Assets shall detail a named owner for each asset, who shall fully understand his/her responsibilities for the protection of the asset in accordance with the documented Asset Management Procedure see [3].

6.3.2. **Access Control Management:** Ensure that all information assets and their supporting assets are protected by the restriction of access so as to ensure the maintenance of their confidentiality, integrity and availability. Access to information assets and the related supporting assets shall be in accordance with the NSO's Access Control Policy (see [4]), and shall be restricted to the minimum required to undertake authorised business activities, according to the NSO's principle, which states that *"access is forbidden unless it has been specifically and formally pre-authorised".*

6.3.3. **Information Classification and Handling Guide:** Ensure that all information assets shall be classified and handled in accordance with the NSO's Information Classification and Handling Procedure (see [5]), which details how information assets of different sensitivity levels shall be managed, handled, processed, encrypted, stored, transmitted, dispatched and disposed of when no longer required. This guide also details the appropriate levels of personnel screening or clearances necessary to access information of different classifications.

6.3.4. **Acceptable Use Practices:** Ensure that all personnel, contractors and third-party users comply with the NSO's Acceptable Use Policy (see [6]), which details how information assets and their supporting assets should be used in an acceptable manner and in accordance with all ISMS-related policies and processes. This policy shall detail the acceptable methods of use of information processing systems, networks—including, for example, the internet, computer hardware and telephone systems—and other resources within the scope of this policy.

6.3.5. **Risk Management Programme:** Perform regular risk management activities (e.g. risk identification, assessment and treatment) relating to all information assets and their supporting assets as detailed within the NSO's Risk Assessment and Risk Treatment Procedure; (see [1]). The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and a risk treatment plan shall be defined to ensure that the appropriate controls are implemented as appropriate to address any unacceptable risks that have been identified. Risk assessments will be based on the Statement of Applicability (SoA) which specifies the ISO/IEC 27001:2013 [2] controls that have been selected, the reasons for their selection and their implementation, and includes a justification for any control that is not selected.

6.3.6. **Information Security Incident Management:** Provide a mechanism for: (a) the prompt identification, reporting, investigation and closure of information security incidents within the NSO, in accordance with the Information Security Incident Policy (see [7]), (b) the analysis of reported incidents to identify the root cause of issues, taking advantage of any improvement opportunities which may be identified, and (c) notifying affected parties and regulators (where applicable) of the incident and the related rectification measures and controls that may be implemented.

6.3.7. **Remote Access Management:** Legitimate remote access shall only be granted in accordance with the Mobile Device and Teleworking Policy (see [8]) to bona-fide personnel, contractors and third-party users, using NSO-approved devices. Remote connections shall be used strictly in accordance with the

Acceptable Use Policy; (see [6]). Remote access shall be regularly reviewed and any connections that are no longer required shall be removed immediately.

6.3.8. **Business Continuity Management:** Ensure that information security is a key consideration within the Business Continuity Management Policy (see [9]), so that the security of the NSO's information assets is not compromised, even when faced with a wide variety of unplanned business interruptions.

6.3.9. **Information Security Training Programme:** Develop a regular training and education programme in accordance with the Information Security Training Policy (see [10]), which shall be mandatory for NSO staff in specific grades, contractors and third party users, and which details their individual responsibilities to fully adhere to the requirements of the ISMS policies, processes and work instructions as defined in Section 5 of this policy.

6.3.10. **Data Protection Management:** Ensure that the ISMS includes a Personal Data Protection Policy (see [11]) that enables the NSO to comply with all applicable data protection laws and regulations.

6.3.11. **ISMS Management, Monitoring and Review:** Continually monitor, review and improve the NSO's ISMS in accordance with the Information Security Committee Management Review Policy (see [12]), by undertaking regular reviews, internal audits—in accordance with the Internal Audit Procedure (see [14])—and other related activities, as well as by taking prompt corrective actions and implementing improvements in response to the findings and opportunities emerging from these activities.

6.3.12. **Legislative Compliance Mechanism:** Ensure that, at all times, the NSO's ISMS enables compliance with the applicable Maltese and EU legislation.

7. Responsibilities

7.1. **Employees, Contractors and Third-Party Users:**

7.1.1. All information security policies forming part of the NSO's ISMS are designed to be congruent with and possibly more restrictive than, the Government of Malta ICT (GMICT) policies. Any party who notices any undue conflicts between the GMICT policies and the NSO's information security policies has a duty to inform the Director of Data Resources, IT and Methodology and/or the Head of IT and to comply with the NSO's information security policies unless s/he is explicitly authorised not to, in writing.

7.1.2. Within the NSO, all employees, contractors and third-party users shall understand their role in ensuring the security of information assets (and the related supporting assets) in accordance with the Information Security Training Policy as detailed in Section 6. NSO staff must be familiar with the ISP and any other documents that regulate the ISMS (see [15]). There are, however, additional responsibilities defined to enable the ISMS to operate efficiently and in accordance with the requirements of ISO/IEC 27001:2013 [2] as detailed below.

7.2. **Directors**

The Director General and all Directors shall be responsible for the following activities in relation to the NSO's ISMS:

7.2.1. Agreeing the business need for the ISMS, and communicating their ongoing commitment to it;

7.2.2. Agreeing to and reviewing this policy;

7.2.3. Setting and reviewing the NSO's Information Security Objectives, including the scope of the NSO's ISMS;

7.2.4. Assigning appropriate resources necessary to manage and operate the ISMS effectively;

7.2.5. Agreeing the level of acceptable risk in line with the Risk Assessment and Risk Treatment Procedure [1];

7.2.6. Approving any decisions not to address any unacceptable residual risks, as may be necessary;

7.2.7. Having ultimate responsibility for actions related to information security incidents or breaches;

7.2.8. Instituting any disciplinary action resulting from information security incidents or breaches.

7.3. **Director of Data Resources, IT and Methodology:**

The Director of Data Resources, IT and Methodology, who reports directly to the Director General, is responsible to lead the NSO on all matters relating to information security and have functional responsibility for the NSO's ISMS, including:

7.3.1. Ensuring that the Office implements and maintains and ISMS in-line with the ISO/IEC 27001:2013 [2] standard and that there is an appropriate structure of ISMS policies, processes and work instructions;

7.3.2. Overseeing the information security risk management programme which covers information security risk assessments, risk treatments and internal audits;

7.3.3. Preparing and communicating the SoA;

7.4. **Head of Information Security:**

The Head of Information Security, who reports directly to the Director of Data Resources, IT and Methodology, shall lead the NSO on all matters relating to information security, and be responsible for the daily operations relating to the ISMS, including:

7.4.1. Reviewing the information security risk management programme, including information security risk assessments, risk treatments and internal audits;

7.4.2. Carrying out regular assessments of the organisation, using a top-down risk-based approach, to ensure the continual improvement of the organisation, and implementing corrective and preventive actions;

7.4.3. Monitoring information security trends at the national and international levels, as well as keeping all stakeholders informed about such issues;

7.4.4. Coordinating the development of a training and awareness programme on information security and privacy matters for NSO employees and other users;

7.4.5. The overall management and functionality of the NSO's business continuity plan;

7.4.6. Ensuring that appropriate records are created and maintained for all ISMS activities;

7.4.7. The facilitation of the provision of information security training and awareness to IT suppliers and contractors;

7.4.8. Monitoring the performance of the ISMS and reporting information security updates to the Director of Data Resources, IT and Methodology and the Information Security Committee.

7.5. **Head of IT:**

The Head of IT, who reports directly to the Director of Data Resources, IT and Methodology, shall, in line with the requirements emerging from the NSO's ISMS, be responsible for:

7.5.1. The overall management of the information security controls in the production processes;

7.5.2. The design and review of technical security controls, including with respect to the NSO's computer networks;

7.5.3. Supporting reviews and internal audits, and supporting or performing risk assessments within their area of responsibility.

7.6. **Information Security Committee:**

The Committee composed of the Director General, all Directors, Head of IT, Head of Legal, Head of Procurement, Support and Resources and Head of Human Resources and Staff Development shall be set up to review the objectives, inputs and outputs of the ISMS and its effectiveness and alignment with the ISP (see [12]).

7.7. **Head of Legal:**

The Head of Legal, who also occupies the role of DPO within the NSO, shall be responsible for keeping a list of applicable legal and regulatory compliance as well as supplier and third-party agreements and ensuring full adherence to the Data Retention Policy [see 13].

7.8. **Head of Human Resources and Staff Development:**

The Head of Human Resources and Staff Development shall be responsible for keeping all personal files and their contents up to date, including the registration and de-registration of employees as well as to facilitate training and awareness sessions on Information Security to NSO staff.

7.9. **Head of Procurement, Support and Resources:**

The Head of Procurement, Support and Resources shall be responsible to coordinate and manage security of the premises and record any visits made by external staff, and facilitating asset management and procedures.

7.10. **Heads of Unit/Domain Managers:**

Employees in charge of specific domains shall be responsible for:

7.10.1. Ensuring that their team members are aware of, and remain compliant with all relevant information security policies, processes and work instructions, and that they receive appropriate training;

7.10.2. The facilitation of the provision of information security training and awareness to applicable third-party users;

7.10.3. Supporting the performance of reviews, internal audits and risk assessments within their area of responsibility, as well as engaging to facilitate the design of ISMS constructs as may be needed from time to time.

7.11. **Asset Owners:**

As per the Asset Management Procedure, designated Asset Owners shall be responsible for:

7.11.1. Assessing the value of their asset/s to the NSO;

7.11.2. Undertaking detailed risk assessments relating to their assets, including the identification of controls, and assessing the controls' effectiveness, in line with the Risk Assessment and Risk Treatment Procedure [1];

7.11.3. Addressing any unacceptable risks in line with the Risk Assessment and Risk Treatment Procedure [1];

7.11.4. Assisting in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of their asset/s;

7.11.5. Reviewing and authorising the levels of access relating to their asset/s, which are granted to others as per the Access Control Policy [4];

7.11.6. Contributing to the Acceptable Use Policy [6], specifically in relation to the use of their asset/s.

7.12. **Control Owners:**

As per the Asset Management Procedure, Control Owners shall be responsible for:

7.12.1. How their assigned control/s are selected, implemented and operated;

7.12.2. Understanding which asset/s rely upon each of their assigned controls;

7.12.3. Providing feedback to asset owners on the operation of each control, to assist them in undertaking accurate risk assessments of their asset/s;

7.12.4. Assisting in the investigation, resolution and closure of any information security incident which actually, or potentially, indicates the failure of a control.

8. References

[1] ISU-PRO-001: Risk Assessment and Risk Treatment Procedure

[2] ISO/IEC 27001: Information Technology – Security Techniques: Information security management system-requirements

[3] ISU-PRO-004: Asset Management Procedure

[4] ISU-POL-003: Access Control Policy

[5] ISU-PRO-002: Information Classification and Handling Procedure

[6] ISU-POL-004: Acceptable Use Policy

[7] ISU-POL-005: Information Security Incident Management Policy

[8] ISU-POL-012: Mobile Device and Teleworking Policy

[9] ISU-POL-007: Business Continuity Management Policy

[10] ISU-POL-008: Information Security Training Policy

[11] ISU-POL-019: Personal Data Protection Policy

[12] ISU-POL-010: ISCM Review Policy

[13] ISU-POL-021: Data Retention Policy

[14] ISU-PRO-009: Internal Audit Procedure

[15] ISU-POL-001-A1: Statement of Acceptance of ISMS Documents

9. Document Control

9.1. This policy needs to be formally reviewed by the Policy Owner at least once a year to address any of the following issues:

9.1.1. A change in business activities, which will or could possibly affect the current operation of the NSO's ISMS.

9.1.2. A change in how the NSO manages or operates its information assets and/or their supporting assets.

9.1.3. An identified shortcoming in the effectiveness of this policy, for example as a result of a reported information security incident or an audit finding.

9.2. The current version of this policy, together with its previous versions, shall be recorded below.

Version History		
Version	**Description**	
1.0	Date Live:	21 June 2019
	Version Notes	Updating of referenced documents in section 8 in line with OBS02 & updating of responsibility of monitoring and reporting of information security updates to the committee in section 7
2.0	Date Live:	28 September 2019
	Version Notes	Inserted Clauses 7.5-7.8 to include the responsibilities of the ISC, Head of Legal, Head of Human Resources and Staff Development and Head of Procurement, Support and Resources. Included Clause 4.6 to specify (in-line with MCCAA recommendations) that the Policy may be made available to external entities upon request and internal clearance.
2.1	Date Live:	27 November 2020
	Version Notes	Updated references to documents listed in section 8, removed reference to Head of Information Security and assigned these responsibilities to the Director of Data Resources, IT and Methodology. Point 7.3.9 has been removed and point 7.3.10 is relabelled as 7.3.9 Included reference to ISU-POL-001-A1 (Statement of Acceptance of ISMS Documents) in Clause 7.1.2
2.2	Date Live:	9 February 2022
	Version Notes	Corrected part of Section 6.3.9 so that it is in-line with ISU-POL-008: Information Security Training Policy given that training is limited to specific grades.
2.3	Date Live:	8 November 2022
	Version Notes	Shift in responsibilities from the Director of Data Resources, IT and Methodology and the Head of IT to the Head of Information Security.

Version 2.3	
	Full Name & Role
Policy Owner:	Silvan Zammit (Director of Data Resources, IT and Methodology)
Reviewed by:	Mark Tonna (Head of Information Security)
Reviewed by:	Ivan Salomone (Head of Information Technology)
Approved by:	Etienne Caruana (Director General)