Malta NSO

National Statistics Office
Uffiċċju Nazzjonali tal-Istatistika

ISU-POL-013: Supplier Security Policy

26 October 2024

1. Overview

1.1. The NSO relies on external parties for the delivery of some aspects of its ISMS, for example the provision of data centres or monitoring software. ISO27001:2013 requires a specific policy to be implemented which clearly communicates the NSO's information security requirements and how these are to be addressed by its suppliers. The policy should specifically document how risks related to a supplier's access to the organisation's information assets and information-processing facilities are to be identified and managed.

2. Abbreviations

ISMS: Information Security Management System
NSO: National Statistics Office
OSINT: Open Source Intelligence

3. Definitions

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

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

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

3.4. **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 life cycles.

3.5. **Supporting Asset:** All supporting assets that contribute to the collection, storage, processing and transfer of the Information Assets 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.

3.6. **Open-Source Intelligence:** Refers to the process of collecting, analyzing, and utilizing publicly available information from a variety of sources to support decision-making, security operations, or organizational objectives. OSINT sources include, but are not limited to:

- Publicly accessible websites (news articles, social media, blogs, forums)
- Government publications (reports, press releases, statistical data)
- Academic papers and journals
- Commercially available data (market research, financial reports)
- Media broadcasts (television, radio, podcasts)

OSINT does not involve accessing or collecting classified, confidential, or private information through illicit means. Focus strictly on legally and ethically gathering information from open, publicly available sources.

4. Policy Objectives

4.1. The NSO uses the services of various carefully selected third-party organisations to deliver some aspects of the NSO's operations. To ensure that these are aware of and can comply with the information security requirements of the NSO, this policy details the security activities which need to accompany the use of outsourced services.

5. Scope

5.1. The NSO's Supplier Security Policy encompasses third-party organisations, especially IT-related suppliers or subcontractors, and potentially other service providers. It applies to those responsible for managing, processing, storing, or deleting NSO Information Assets, or for maintaining information-processing facilities that ensure the security of these Information Assets.

6. Policy Statements

6.1. General Statements

6.1.1. The NSO shall maintain an active Information Security Management System, which protects the confidentiality, integrity and availability of Information Assets, as well as the facilities and systems which support their security. If it is necessary for the Office to outsource any services to a third party, such parties shall be required to comply with the requirements detailed in this policy.

6.1.2. The assessment of third-party organisations prior to their formal engagement by the NSO shall include a review of the maturity of their own information security capabilities. An OSINT exercise may be conducted on the contracting authority, individual or entity. The procurement body are informed with the result and such details are filed for future reference. During the procurement process, specific references to information security risks must be made to anticipate and address potential issues (see [1]). When possible, preference shall be given in the selection process to those third parties who have formal ISO27001 or equivalent certification and can demonstrate experience in safeguarding Information Assets and processing facilities through their previous work.

6.1.3. The ongoing information security capability of contracted third-party organisations, mainly selected IT related suppliers and/or subcontractors, shall be periodically (at least once a year) re-assessed by the NSO to ensure that no risks have emerged (see [1]).

6.1.4. The NSO and its third-party suppliers shall agree the protective markings, classifications and acceptable use of data, systems, networks and facilities that are to be entrusted either in whole or in part to the third party. The third party shall fully comply with such requirements, and shall ensure that its personnel understand their responsibilities in this regard.

6.1.5. Third-party suppliers shall ensure that all dealings with the NSO remain strictly private and confidential and are not disclosed without the prior written permission of the NSO.

6.2. Event Notifications

6.2.1. Third-party suppliers shall be required to maintain regular communications with the NSO whilst they fulfil the contracted requirements for the delivery of goods and services, and shall be required to promptly notify the NSO of any of the following activities:

- Any identified security breaches within their own organisation;
- Any changes to the status of their ISO27001 certification, where applicable;
- Any changes to directors, key personnel, ownership or operating locations.

6.3. **Audit and Inspection Clause**

6.3.1. The third-party supplier shall unreservedly agree to on-site inspections and audits by the NSO to ascertain that its information, assets and systems are being properly protected. Where possible, reasonable notice of such an inspection or audit shall be given, and any attempts by the third party to avoid or unreasonably delay such activities shall be considered by the NSO, which may lead to the termination of the services.

6.4. **End of Service Requirements:**

6.4.1. At the end of the contract for delivering goods or services to the NSO:

- The NSO shall arrange to promptly revoke access to all premises, facilities and systems to which the third-party supplier had been granted access;
- The third-party supplier shall fully adhere to NSO's requirements for returning all NSO's Information Assets, including providing evidence of the secure and permanent erasure of NSO data from the third-party supplier's systems and backup media;
- The third-party supplier shall be obliged to remind all its personnel of the ongoing requirement to confidentiality and the obligations of the non-disclosure agreement.

7. Responsibilities

7.1. The **Head of Information Security** shall be responsible for ensuring that this Supplier Security Policy remains current, aligned with NSO's business activities and security objectives, and is fully communicated to and understood by those third-party suppliers detailed within the scope of this policy. In the absence of the Head of Information Security, this responsibility lies with the Head of Information Technology.

7.2. The **Director Data Resources, IT and Methodology** shall be responsible for ensuring that the requirements of this policy, enhanced by specific clauses relating to the provision of goods or services by the supplier, are included in contractual documentation.

7.3. The **Third-party supplier** shall make its personnel aware of the requirements of this policy and shall ensure their full compliance with it. The NSO reserves the right to suspend or terminate the services of the third-party supplier in the event of a proven failure to fully follow the requirements of this policy.

8. References

[1] ISU-DOC-006 - Contractors and Subcontractors checklist

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**	
1.04	Date Live:	26 October 2024
	Version Notes:	Reference is made to OSINT in 6.1.2
1.03	Date Live:	26 April 2024
	Version Notes:	Reworded Clause 5.1 to emphasize the role of IT-related service providers. Version history changed to descending order.
1.02	Date Live:	12 June 2023
	Version Notes:	Logo and template updated. Shifted owner from Head of Information Technology to Head of Information Security throughout the document. Added reference to ISU-DOC-006 - Contractors and Subcontractors checklist in Clause 6.1.3.
1.01	Date Live:	27 November 2020
	Version Notes:	Amended point 6.1.2 to reflect that preference to information security shall be given when selecting third parties when possible. The responsibilities of the Head of Information Security have been assigned to the Head of IT.
1.00	Date Live:	6 June 2019
	Version Notes:	First version of the policy.

Version 1.04	
	Full Name & Role
Policy Owner:	Mark Tonna (Head of Information Security)
Reviewed by:	Ivan Salomone (Head of Information Technology)
Reviewed by:	Silvan Zammit (Director of Data Resources, IT and Methodology)
Approved by:	Etienne Caruana (Director General)