InterPARES Trust Project Report

Title:	**Checklist for Developing or Revising Policies for Managing Security Classified Information Assets**
Status:	Final Draft
Version:	2.1
Date submitted:	09 May 2017
Last reviewed:	30 May 2017
Author:	InterPARES Trust Project
Writer(s):	Ineke Deserno, Eng Sengsavang, Marie Shockley, Shadrack Katuu, Julia Kastenhofer
Research domain:	Transnational Team 03

Document Control

Version history			
Version	Date	By	Version notes
1.0	17 Aug 2016	I. Deserno, E. Sengsavang	Initial draft checklist
1.1	19 Aug 2016	All	Draft checklist
1.2	25 Aug 2016	All	Draft checklist
1.3	17 Sep 2016	All	Draft checklist following comments from Jens Boel (UNESCO) and Adele Torrance (UNESCO)
1.4	8 Oct 2016	All	Draft checklist following comments from Transnational Team Meeting, 28-29 Sept 2016
1.4a	17 Oct 2016	All	Draft checklist following initial consideration of comments from IAEA staff
1.5	14 Jan 2017	All	Draft checklist following comments from IAEA staff, April Miller (World Bank), Andrea Damini (European Commission), Donna Kynaston (World Health Organization) and Grant Mitchell (International Federation Red Cross and Crescent Societies)
1.6	23 Apr 2017	All	Draft checklist following comments from Natascha Khramtsovsky, Maria Caravaca (ICCROM), Patricia Franks (San Jose State University) and Alicia Barnard
2.0	9 May 2017	All	Final draft checklist submitted for approval at Transnational Team meeting on 15 May 2017, Geneva, Switzerland
2.1	30 May 2017	All	Final draft checklist incorporating comments from Transnational Team meeting, 15 May 2017, Geneva, Switzerland

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets

PURPOSE and SCOPE

This checklist is designed to support organizations in the development or revision of policies and procedures for managing security classified information assets (SCIAs), especially digital information, to ensure the reliability, authenticity, confidentiality, integrity and availability of security classified records and their long-term preservation. The checklist aims to support best management of SCIAs throughout their lifecycle: from creation or receipt, active and controlled business uses, to the secondary uses of SCIAs, including where applicable eventual declassification, disclosure, archiving or destruction. While various professionals will bring their own respective issues to the table in the process of policy-making, this checklist is not intended to cover comprehensively every one of those issues. Instead, the checklist promotes a long-term approach to SCIA management that especially complements information security concerns with those of records management and archival requirements. For this reason, the checklist focuses on protecting the confidentiality of SCIAs and managing changes in their classification status, in addition to ensuring that information and records management best practices and procedures are applied to SCIAs. It is assumed that organizations managing SCIAs already have implemented a general security framework that includes required security clearances for individuals handling SCIAs, broad physical and technological access controls, and other organizational security measures.

The checklist is an open tool that may be used by anyone involved in drafting or advising on policies and procedures related to the management of SCIAs, for example: administrative; management; information security; information technology; legal; information and knowledge management; and records management or archival staff. Moreover, the checklist is applicable to many different types of organizations that create and handle SCIAs, including inter- and non-governmental, governmental, public, and private organizations. The checklist will be especially relevant in the development of policies and procedures that focus on SCIAs and their management. In addition, the tool may be useful when developing other types of policies and procedures that impact SCIAs, such as declassification, access, and digital preservation policies. The term “policy” is used throughout the checklist to refer potentially to multiple policies and procedures within an organization that address the issues in question. The checklist uses terminology from the InterPARES Trust Terminology Database, and key terms used are defined below. In addition, a minimum set of descriptive metadata for managing and preserving security classified information assets is proposed in Annex 1, and categories of roles and responsibilities are provided in Annex 2.

BACKGROUND

The checklist is developed from a study of existing policies of 17 international organizations, ranging from large international organizations within the United Nations (UN) structure, to smaller regional organizations in both North America and Europe. The organizations cover a wide range of functions, from humanitarian assistance, development and financial agents, to security organizations and research organizations.

Staff from participating organizations contributed an assemblage of policies and procedures rather than a single policy, which helped to draw a fuller picture of the matrix of existing policies and procedures supporting the management of SCIAs within organizations. In addition to policies dealing specifically with SCIAs, the texts analyzed for this checklist include policies for access to information, organizational security, data privacy and digital preservation. The policies addressed a range of information management issues, such as control and handling, storage and transmission, data privacy, classification and declassification, and public access.

DEFINITIONS

Declassification – The process of removing the security classification from a record or other information asset.

Declassification authority – The person(s) or body(ies) with the authority to declassify an information asset.

Disposition – Records' final destruction or transfer to an archives as determined by their appraisal.[1]

External disclosure – Policies and procedures related to the release of organizational information assets to parties external to an organization.

Information asset – Information, data, documents or records created or received by an organization or person in any format. In the checklist, we use the abbreviation SCIA to mean "security classified information asset(s)."

Internal disclosure – Policies and procedures related to the release of organizational information assets to parties within an organization.

Public disclosure – The process of making a document or other information assets available to the public.

Reclassification – The process of decreasing or downgrading, or increasing the security classification level of a record or other information asset.

Reclassification authority – The person(s) or body(ies) with the authority to reclassify an information asset.

Record – A document made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference.[2]

Security classification authority – The person(s) or body(ies) with the authority to determine the security classification of an information asset.

Security classified information asset (SCIA) – Information asset of an organization that is security classified and therefore controlled/managed through specific policies and procedures.

---

[1] InterPARES Trust. *InterPARES Trust Terminology Database*. "Disposition." http://arstweb.clayton.edu/interlex/term.php?term=disposition

[2] InterPARES Trust. *InterPARES Trust Terminology Database*. "Record." http://arstweb.clayton.edu/interlex/term.php?term=record

Information security classification – 1. The process of applying designated levels of access control and protection on an information asset in compliance with organizational policy, including corresponding measures for management and control of the information asset, based on a security assessment of the degree of negative impact that disclosure of the information would have on an organization, the work of an organization, and/or third parties. 2. The term may also refer to the security classification levels themselves, which vary across organizations, for example Restricted, Confidential, etc.

Sensitive but unclassified information asset (SUIA) – An information asset without a security classification, to which access is controlled due to the risk that disclosure could harm individual, management, political or commercial interests of the organization or other relevant parties. The policies and procedures for managing SUIAs are controlled but may be distinct from those policies and procedures governing the management of security classified information assets (SCIAs).

Withheld date – The date an SCIA item proposed for downgrading, declassification or public disclosure has not been authorized to be downgraded, declassified and/or publicly disclosed.

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets					
	Question	**Y**	**N**	**N/A**[3]	**Notes**[4]
1.	**Scope and Definition**				
1.a.	Does the scope of the policy address the rationale for classifying information assets not only to protect the organization itself, but also more broadly to protect the work of the organization and third parties for which the organization is accountable, according to its mission and core activities (e.g. case file subjects, program beneficiaries)?				
1.b.	Does the policy provide a clear definition of the information assets that it covers?[5]				
1.c.	Does the policy cover procedures for classification, declassification, and reclassification?				
1.d.	Does the policy enable security classifications to be applied to a single information asset, a group of information assets, and a cluster of information asset groups (e.g. a database)?				
1.f.	Does the policy apply retroactively to SCIAs that were classified prior to the development of the policy?				
2.	**Roles and Responsibilities**				
2.a.	Are the roles and responsibilities of the parties involved in various aspects of managing the SCIAs throughout their lifecycle clearly identified and defined? See **Annex 1** for an example of Categories of Roles and Responsibilities.				
2.b.	Is there an information security coordinator within the organization responsible for addressing questions related to SCIAs for each phase of the lifecyle?				

[3] The 'N/A' column means 'not applicable' or 'not known.'
[4] Use this column for notes, or when there is neither a 'yes' nor 'no' answer.
[5] For example, does the policy cover SCIAs that are created *or* received by the organization?

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets					
	Question	**Y**	**N**	**N/A[3]**	**Notes[4]**
2.c.	Have all concerned employees (as records creators or users) been informed and trained in order to ensure that they fully understand the SCIA policies in place and can confidently perform their own part within the overall framework of roles and responsibilities?				
3.	**Creation**				
3.a.	Are the levels of information security classifications and the criteria for applying them clearly defined and distinguished?				
3.b.	Is a list of information asset categories (e.g. intelligence analyses, political analyses, etc.) and the rationale for classifying the information asset categories provided?[6]				
4.	**Records Management**				
4.a.	In addition to a security framework,[7] are SCIAs placed within an information or records management framework? For example, are the organization's information and records management tools applicable to SCIAS, such as file classification schemes and records retention and disposition schedules; and are SCIAs contextualized within a records lifecycle?				
4.b.	Does the policy clearly indicate that the rationale for disposition of an SCIA should be based on an assessment of the value of the SCIA and/or the procedures defined in the records retention schedule, rather than on the security of the classification?				
5.	**Handling and Control**				

[6] If the answer is no, you may consider creating such a list or providing examples of information asset categories to guide users of the policy.

[7] "Framework" refers to the entirety of documents, procedures and processes that support a given function.

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets					
	Question	**Y**	**N**	**N/A**[3]	**Notes**[4]
5.a.	Does the policy establish a link between registration metadata in a classified information register and the SCIAs themselves?				
5.b.	Does the policy ensure identification and retrieval of SCIAs throughout their lifecycle through metadata, control, and handling procedures?				
5.c.	Does the policy address the security classification of systems that hold or convey classified information, for example registries or electronic records management systems?				
6.	**Metadata**				
6.a.	Does the policy provide sufficient provisions for the preservation of descriptive and technical metadata, including metadata related to information classifications?				
6.b.	Does the policy establish a minimum set of metadata for SCIAs? See **Annex 2** for a recommended minimum set of metatdata.				
6.c.	Does the policy establish provisions for the retention of audit trail records throughout the lifecycle of SCIAs?				
6.d.	Does the policy distinguish between the security classification of the content versus the metadata of SCIAs? For example, does the policy consider whether certain kinds of metadata, but not all metadata of SCIAs should also be classified?				
7.	**Information Security**[8]				
7.a.	Does the policy address physical security requirements of SCIAs such as storage area, personnel and equipment?				

[8] The information security standard consulted for this checklist is the ISO 27001:2013 and ISO 27002:2013.

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets					
	Question	**Y**	**N**	**N/A[3]**	**Notes[4]**
7.b.	Does the policy establish controls and procedures to ensure integrity and mitigate against corruption or tampering of SCIAs, including in automated systems, during internal and external transmission and in storage?				
7.c.	Does the policy address the protection of systems that hold or convey classified information, for example registries or electronic records management systems, through procedures such as security audits?				
7.d.	If the policy requires or enables security encryption or other security mechanisms for digital data, are there provisions for long-term access and preservation of the SCIAs by maintaining corresponding decryption mechanisms over time?				
8.	**Digital Information Assets and Long-Term Preservation**				
8.a.	Is the policy applicable to all formats and media, including audiovisual and digital formats?				
8.b.	Does the policy cover SCIAs not in the physical custody of the organization, but still under the control of the organization, for example SCIAs managed using third-party cloud computing services?				
8.c.	Does the policy acknowledge changes resulting from the process of copying SCIAs from one digital medium to another?[9]				
8.d.	Does the policy acknowledge changes resulting from the process of transforming SCIAs from one format or format version to another?[10]				

[9] Also known as 'refreshing.' InterPARES 3 Project. Terminology Database. "Refreshing." http://interpares.org/ip3/ip3_terminology_db.cfm?letter=r&term=513

[10] Also known as 'conversion.' InterPARES 3 Project. Terminology Database. "Conversion." http://interpares.org/ip3/ip3_terminology_db.cfm?letter=r&term=194

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets					
	Question	**Y**	**N**	**N/A[3]**	**Notes[4]**
8.e.	Does the policy acknowledge changes resulting from the process of moving or transferring SCIAs from one system to another?[11]				
8.f.	Does the policy cover changes to systems handling SCIAs resulting from routine system updates or upgrades?				
8.g.	Does the policy address the acknowledged changes to the medium, format, or systems of SCIAs with mechanisms that ensure SCIAs maintain their authenticity, confidentiality, reliability, integrity and usability over time?				
8.h.	Does the policy ensure that any contractual services engaged by the organization that impact SCIAs enable users to be compliant with the policy?				
9.	**Reclassification and Declassification**				
9.a.	Are the criteria, timeframe and method for reclassification and declassification of SCIAs clearly indicated?				
9.b.	If your organization distinguishes between declassification and public access, then does the policy reflect that?				
9.c.	Is there a systematic process for downgrading and declassification of SCIAs after a certain lapse of time?				
9.d.	Is there a process to update the access permissions to SCIAs following reclassification or declassification of SCIAs?				
9.e.	Does the policy specify whether an appeals process is in place for unsuccessful downgrading or declassification requests, with clearly defined roles?				

[11] Also known as 'migration.' InterPARES 3 Project. *Terminology Database*. "Migration." http://interpares.org/ip3/ip3_terminology_db.cfm?letter=r&term=501

Checklist for Developing or Revising Policies for Managing Security Classified Information Assets					
	Question	**Y**	**N**	**N/A[3]**	**Notes[4]**
10.	**Public Access and Disclosure**				
10.a.	Is there a systematic process for public disclosure of SCIAs after a certain lapse of time, to ensure that the majority of records do not remain security classified indefinitely?				
10.b.	Are the criteria, timeframe and method for public disclosure clearly indicated?				
10.c.	Is there a process to update the public access permissions to SCIAs following the disclosure of the SCIAs?				
10.d.	Is there a process to transfer the SCIAs from the protected environment to a more accessible environment, following successful disclosure of SCIAs for public access?				

Annex 1. Minimum Descriptive Metadata for Managing and Preserving Security Classified Information Assets

1. Information security classification
2. Classification authority
3. Eligible date for downgrading and declassification
4. Reclassification/declassification date
5. Reclassification/declassification authority
6. Eligible date for public disclosure
7. Public disclosure date
8. Public disclosure authority
9. Withheld date (if applicable)
10. Reasons for withholding (if applicable)
11. Audit trail of persons who accessed the information/document
12. Version history

Annex 2. Categories of Roles and Responsibilities

Each of the roles outlined below represent general descriptive designations (e.g. Information Security Coordinators, etc.) related to their functions, and not necessarily their real position titles, which will vary across organizations. Additionally, within organizations there may be more than one person fulfilling a role or fulfilling specific aspects of a role.

1.0 Senior Management

- Are responsible for the protection of SCIAs within the organization. This includes SCIAs gathered or generated by the organization, as well as those received from member parties in the case of international organizations;
- Appoints the organization's Information Security Coordinator(s) or ISC(s);
- Approves the organization's procedures and information security classification levels;
- Acts as the final authority on the application of information security classification levels for their area of functional responsibility, in consultation with the ISC(s), in cases of disagreement or uncertainty among staff;
- Coordinates regulatory compliance in the management of SCIAs;
- Approves, on a case-by-case basis, any exceptions to this procedure.

2.0 Information Security Coordinator(s) (ISCs)

- ISCs are responsible for all institution-wide information security issues and provide guidance regarding information asset classification and protection. Specific duties of ISCs include, but are not limited to:
- Ensure effective controls for the protection of classified information assets are implemented – technically as well as administratively;
- Support qualified staff and originators (if possible) in determining the level of classification of an information asset;
- Maintain the organization's information security policy;
- Provide assistance for the protection of classified information assets.

3.0 Information Asset Originators

- Classification decisions should be made by staff with knowledge of the contents of the information asset and the classification criteria. In most cases this will be the originator of the information asset.
- The originator is the staff member who creates an information asset (such as a document). This staff member is thus the first person within the institution to encounter the information asset and to determine the proper classification. For example, a staff member drafting a document should make a determination of the classification level based upon its content and the classification criteria.
- In case of uncertainty about the classification level, the responsible supervisor in the hierarchy should be consulted.

4.0 Initial Classifiers

- A majority of the time the Initial Classifier is the information asset originator. However, in the situation where the organization receives the information asset, and therefore is not the originator, the receiver within the institution is the initial classifier and must make the classification determination based on the institution's classification definitions.
- The initial classifier could be a staff member receiving information directly from an member party, or could be the archives and records management unit as the initial recipient of official information received.

5.0 Information Asset Stewards

- The institution is the owner of all information assets that are created by its staff. The organization is responsible for ensuring an asset's confidentiality, authenticity, reliability, integrity, and availability.
- The information asset steward (hereinafter referred to as steward) is responsible for the classification and proper handling of the information assets.
- The originator of the SCIA may in some cases also be the designated steward. However, in most cases, stewardship is vested in the supervisor of the administrative unit in which the information asset originates.

6.0 Authorized Derivative Classifiers

- In the case of a question or difference of opinion regarding the security classification of an information asset, the Authorized Derivative Classifier is a staff member who is authorized and certified to determine the security classification of an information asset, over and above the decisions of the initial classifier and Information Asset Steward.
- The Authorized Derivative Classifier bases their information security classification assessments on defined organizational guidance and policies.

7.0 Declassification and Reclassification Authorities

- Declassification and Reclassification Authorities are the issuers of authorized declassification and/or reclassification decisions resulting from the proper enactment of declassification/reclassification policies and procedures of the organization.
- In many cases there will be several parties involved in declassification/reclassification decisions and procedures, such as designated staff members, committee members and/or member state parties.
- Declassification and Reclassification Authorities are distinct from any of these roles in that they are authorized to issue the final declassification decision on behalf of the organization. In some cases they may be a committee of representatives rather than a single person or staff member, or they may be a combination of a committee and one or several designated staff members.
- In many organizations, the original classifier may also act as a Declassification and Reclassification Authority.

8.0 Users of Information Assets

- Users of information assets must protect the information asset in accordance with the requirements outlined in organizational policies governing SCIAs. This includes the security requirements for handling, storing, marking, protection from unauthorized or incidental viewing, and for reporting security incidents to the SC.
- Before sharing SCIAs with another staff member, the user is responsible for ensuring the recipient is authorized to receive such information and is aware of the protection requirements.
- It is also the responsibility of the users of SCIAs to bring to the attention of their supervisors, and the ISC, situations where information is not being adequately protected or where the current procedures do not provide sufficient or consistent guidance.
- Each user is encouraged to raise issues on appropriateness of classification if he or she believes the SCIA is not correctly classified.

9.0 Information Asset Custodians

- The information asset custodian is a staff member or an organizational unit that has been assigned the responsibility for safekeeping of information assets, such as recordkeeping and information management staff/units, and information technology staff who have technical responsibility for supporting systems in which SCIAs are managed. All information asset custodians are responsible for complying with relevant information asset policies.
- This might happen on a temporary or permanent basis. The custodian must ensure that the information is protected in accordance with the requirements set in the relevant policies governing the management of SCIAs.