ITSRM

IT Security Plan (ITSP) Template v2.0

Template Instructions

Text in **ORANGE** represent text that should be defined and recoloured to black ("Automatic")

< Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. >

Text in **BLUE** represent guidelines that should be deleted in the final version

< Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. >

Text in **RED** represent instructions that should be deleted once executed

< Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. >

<This page should be deleted>

SENSITIVE[1]

<This template is already marked according to SN1903; however, it is up to the document owner to ensure the proper marking and handling – detailed instruction and reference are at the bottom of this page>

<DG Name>
<Unit Name>

IT Security Plan[2]

[Subject]

<Please make sure the subject name is aligned with the GovIS2 naming convention>

[GovIS2-ID(s)]

<Provide the exact reference to GovIS2-ID, to indicate the coverage of document: IS-xxx SV-xxx, MO-xxx and make sure that GovIS2 section related records contain the same info>

<If you are starting the ITSRM process now, you should fill immediately the related GovIS2 field of the security section, called "ITSRM Processes Start Date">

[1] Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions: https://europa.eu/!db43PX

[2] Based on ITSP Template v2.0 available on https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM/Publications

Document Control Information

<You can customize this section according to your context and needs, for example adding other roles>

Settings	Value
Document Title:	IT Security Plan for [Subject]
Document Author:	*<This is likely to be the Security Risk Manager>*
Project Manager (PM):	
System Owner (SO):	
Doc. Version:	*<v>*
Date:	*<date>*

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All Reviewers in the list are considered required unless explicitly listed as Optional.

Name	Role	Action	Date

Document history:

The Document Author is authorised to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Short Description of Changes

TABLE OF CONTENTS

<Do not forget to update the Table of Contents once the body of the document is final>

EXECUTIVE SUMMARY

<Provide an executive summary (one page maximum) highlighting the key points of the IT security plan, namely a few information about the IT system and its purpose, the main assets and their value (including the resultant system classification), the main risks, with their inherent risk, residual risk and security measures. The executive summary should provide to the reader the key points of the IT system and its IT security plans and the assurance that risks have been identified and managed>

1. SYSTEM OVERVIEW

<This section aims to provide a system characterization that includes, namely, a description of the system (purpose, information handled, user population etc.), system high-level architecture and compliance requirements/constraints identified for the system. Additional system information (technical documentation, detailed description of the business processes etc.) can be attached to this document in Appendix 2: References and Related Documents.>

1.1. System Description

<System description>

- *<Mention what is the name of the CIS that this IT Security Plan applies to and who is the owner (e.g. name of the responsible DG/Unit). Describe what is the purpose of the system, its main business functionalities, the information handled and the user population. Specify if any parts of the system are out-of-scope of this IT Security Plan and provide a justification if this is the case.>*

<System high-level architecture>

- *<If possible, provide a high-level diagram of the system components and/or business workflows. Also indicate where the system components are located, if in multiple locations>*

1.2. Constraints and Compliance

< This section aims to identify the compliance requirements[3] and constraints imposed on the system, including any assumptions made that put constraints on the risk study. Complete the table below to provide an overview of the main compliance requirements and constraints identified for the system>

- *< The "Compl?" column contains "Yes" if the entry is a compliance requirement and "No" if it is a constraint. The "Exc?" column contains "Yes" if there is an exception from that compliance requirement>*
- *<Some constraints/compliance requirements might impose to implement specific security measures for the system. If this is the case, link the mandatory security measures identified to the related constraint/compliance requirement in the table.>*

Constraint ID	Title	Compl?	Exc?	Mandatory Measures
<Provide constraint / compliance ID (e.g. GDPR)>	*<Provide the full name of the compliance requirement or constraint (e.g. General Data Protection Regulation (EU) 2016/679>*	*<Insert 'Yes' if it is a compliance requirement and 'No' if it is not>*	*<Insert 'Yes' if an exception was raised>*	*<Provide the name/ID of the related mandatory measure imposed by the requirement/constraint (if any)>*

[3] IT Security Policy, Standards, Guidelines and Technical specifications
https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Pages/IT-security-standards-and-guidelines.aspx

Constraint ID	Title	Compl?	Exc?	Mandatory Measures

Table 1 – Constraints and compliance requirements on this IT Security Plan

- *<If any exceptions to the implementation of the security measures imposed by the constraints/compliance requirements (the mandatory measures) were identified, provide a justification, together with an expiration date>*

Constraint ID	Measure ID	Justification	End date

Table 2 – Exceptions in the ITSP from the compliance requirements

1.3. Risk Acceptance Criteria

< According to COMMISSION DECISION of 13.12.2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission, the Risk Acceptance Criteria is one of the key output of the IT risk management process that needs to be documented in security plans drawn by the System Security Officer (article 4, paragraph b)>

<Provide the Risk Acceptance Criteria defined for the CIS by filling-in the table below. The IT Security Plan should refer to a policy/document/decision where the risk appetite is defined and translate this into risk level objectives and risk acceptance criteria.>

ID	Description

Table 3 – Risk Acceptance Criteria

2. IT Security Risk Assessment Results

<This section aims to provide the main outcomes of the asset valuation and the risk analysis performed for the system. It also documents any deviation from the default values defined by the methodology.>

<The System Owner shall monitor and review at least once a year, the IT security needs and risk assessments' results, the residual risks, exceptions and the identified acceptable levels of risks, taking into account changes to the organisation, technology, business objectives and processes, identified threats, effectiveness of the implemented security measures and external events, such as changes to the legal, contractual or regulatory environment or changes in the Commission's IT security policy. The security plan must be updated accordingly, periodically or after any significant change.>

2.1. Risk Assessment Approach

<The objective of this section is to describe the methodology and approach followed to identify and prioritise the risks and to document the stakeholders involved in the different phases of this exercise>

<Methodology and approach>

- ***If ITSRM was used :***
  - *<Please indicate which combination of Methodology and Tools was selected among the ones showed in the below table, using a simple statement like: "The Risk Assessment was performed using the ITSRM methodology version 1.2, and GovSec.RM.">*

Methodology	***Tools***
ITSRM Methodology v.1.2	***GovSec.RM***
ITSRM Methodology v.1.0	***Basic Excel Tool v1.2***
	Basic Excel Tool v1.1.0-beta1
	Basic Excel Tool v1.0.1 r1
	Basic Excel Tool v.1.0

  - *< State which roles (as these are defined in ITSRM were involved for every process/step of the risk study, what was their responsibility (ARSCI) and when each step was completed.>*
    <You may use and tailor/customise the following table to achieve such result>

ITSRM Step	Stakeholder #1	Stakeholder #2	……	Date completed
System Characterization (P1)				*dd/mm/yyyy*
Primary Asset Inventory and Asset Valuation (P2)				*dd/mm/yyyy*
Supporting Assets Inventory (P3)				*dd/mm/yyyy*
System Modelling (P4)				*dd/mm/yyyy*
Risk Identification (P5)				*dd/mm/yyyy*
Risk Analysis and Evaluation (P6)				*dd/mm/yyyy*
Risk Treatment (P7)				*dd/mm/yyyy*

Table 4 – ITSRM Steps and Stakeholders

- ***If other risk management methodologies were used:***
  - *<Provide a high-level description of the processes followed to conduct the assessment.>*
  - *<State which departments/roles were involved and/or responsible for every process of the risk study.>*
  - *<Please remember to mark accordingly the GovIS2 field "ITSRM Methodology" to indicated whether or not ITSRM was used, this will ensure accurate records.>*

2.2. Asset Valuation Conclusions

< System classification>

- *<Provide the overall classification level for the system by filling-in Table 5 – System classification. The overall system classification levels are identified by selecting the highest impact value identified for each security dimension across all Primary Assets. For more information on the system classification, consult the 'ITSRM Mapping CIA levels' of the ITSRM Wiki[4] that facilitate the correspondence between ITSRM values and Legal Basis values>*

	Confidentiality	Integrity	Availability
Maximum Asset Valuation	*<Insert the maximum asset value identified for the system>*	*<Insert the maximum asset value identified for the system>*	*<Insert the maximum asset value identified for the system>*
Classification	*<Provide the classification for confidentiality (e.g. Sensitive Non Classified)>*	*<Provide the classification for confidentiality (e.g. Low)>*	*<Provide the classification for confidentiality (e.g. Medium)>*
Description	*<Provide the description of the classification level chosen (e.g. Information that the Commission must protect because of legal obligations or because of its sensitivity)>*	*<Provide the description of the classification level chosen (e.g. Minor damage to the Commission or other stakeholders)>*	*<Provide the description of the classification level chosen (e.g. Significant damage to the Commission or other stakeholders)>*

Table 5 – System classification

<When you have completed ITSM step P1 and P2, please go in GovIS2 and updated all the relevant security fields for this stage: ITSRM Methodology, GovSec.RM ID, Confidentiality Level, Integrity Level, Availability Level>

< Maximum Tolerable Period of Disruption (MTPD)>

- *<Provide the Maximum Tolerable Period of Disruption for the system. It is the maximum duration after which the down-time of the system would be considered unacceptable.>*

[4] The mapping documents is available on https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM/Publications

2.3. Risk Identification and Analysis Conclusions

< Conclusions of the risk assessment>

- *<Provide the main outcomes of the risk identification and evaluation process (e.g. number of risks identified, number of risks that need to be mitigated etc.). Include a visual representation of the risks identified if possible.>*

- *<Present an overview of the main risks identified by filling-in the table below. To simplify the overview, the risks can be grouped together if they do apply on the same Primary Asset with the same security dimension and threat.>*

ID	Description	Primary Asset	Security Dimension	Inherent risk	Residual risk
Provide the risk ID (e.g. RSC-10428)	*<Provide the description of the risk scenario>*	*<Provide the name of the Primary Asset>*	*<Provide the security dimension>*	*<Provide the inherent risk score (e.g. 20,00)>*	*<Provide the residual risk score (e.g. 20,00)>*

Table 6 – Top Ten risk scenarios by Inherent Risk Level

- *<If all Risk Scenarios have a Residual Risk Level that satisfies the Risk Acceptance Criteria defined in section '1.3 Risk Acceptance Criteria', write the following statement: 'All Risk Scenarios have a Residual Risk Level that satisfies the Risk Acceptance Criteria'.>*

- *<If not all Risk Scenarios have a Residual Risk Level that satisfies the Risk Acceptance Criteria, provide a justification.>*

2.4. Deviations from Default Values

< Deviations>

- *<Record any deviations from the default values of the methodology used for the risk study and provide a justification for these deviations.>*

- *<If no deviations from the values defined by the methodology used need to be recorded, write the following statement: 'No deviations were recorded in this IT Security Plan from the default values from the ITSRM Extended Catalogues, neither for Threat Easiness/Frequency, nor for Security Measure Mitigation Factors'.>*

3. RISK TREATMENT PLAN

<This section describes the risk treatment approach and the action plan defined to treat the risks identified for the system.>

3.1. Risk Treatment Approach

<Risk treatment strategy>

- *<Describe the Risk Acceptance Criteria and the Risk Treatment Strategy defined to ensure that all Residual Risk Levels meet the Risk Acceptance Criteria (e.g. 'all risks above a defined risk threshold should be mitigated'). Refer to the policy/document/decision for the risk appetite and translate this into risk acceptance criteria.>*

<Selected risk treatment options>

- *<Explain which risk treatment options were selected (Risk Acceptance, Risk Sharing, Risk Transfer and Risk Remediation). Explain why these risk treatment options were chosen based on the risk treatment strategy defined.>*

3.2. Selection and Prioritisation Criteria

<Selection and prioritisation strategy>

- *< Define the criteria that define their implementation priority. The Risk Level is a primary factor in prioritising the security measures to be implemented, but other factors (such as complexity of implementation, mandatory time-constrained compliance requirements, low hanging fruit - i.e. measures easy/fast/cheap to implement, measures that mitigate multiple risks) can also be used to prioritise the implementation of security measures and the creation of the implementation timeline in the action plan. Reference the iterative nature of P6-P7 and describe how the measures selected are the best combination between risk, compliance and cost-benefit requirements.>*

3.3. Action Plan

<Action plan>

- *<Present the risk treatment plan to implement the identified security measures, including the deadline, owner and all the relevant information presented in Table 7 – Risk treatment action plan. The action plan can include development activities (measures to be implemented during the development of the system) and/or operations activities (the work to implement any security measure during the operations).>*

ID	Measure	Deadline	Owner	Sophistication	Mandatory?	Mitigated Risks	Priority
	<Name of the measure>						
<Measure ID>	*<Measure description>*	*<Deadline defined for the implementation>*	*<Department or person responsible of the implementation>*	*<Insert the sophistication level (Low/Medium/ High)>*	*<Insert 'Yes' if the measure is imposed by a constraint/ compliance requirement >*	*<Include the risk IDs mitigated>*	*<Insert Low, Medium or high>*

Table 7 – Risk treatment action plan

APPENDIX 1: FULL RISK STUDY

<Provide the file used to complete the risk study.

If the risk study was performed in GovSec.RM, provide an XLS export.

If the risk study was done using the Basic Excel Tool embed it here.

If you used another methodology, you can add as well the related details here >

APPENDIX 2: REFERENCES AND RELATED DOCUMENTS

<Provide any relevant documentation used to complete the risk study and the IT Security Plan (e.g. methodology used if different from ITSRM, System architecture and design, compliance requirements relevant to the system etc.)>

ID	Reference or Related Document	Source or Link/Location

<If you want to refer to ITSRM documents, please point to the main pages e.g.

https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM

https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM/Publications

https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM/Tools>

APPENDIX 3: ITSP APPROVAL NOTE

<According to C(2017) 8841, the System Owner 'shall formally approve the security plans and residual risks; the residual risks shall be formally accepted by the Head of the Commission Department concerned while using criteria documented in the security plan; major residual risks shall be escalated to the ISSB and may have to be flagged in the Directorate-General's Annual Activity Report'>

<As a result, this approval note should be signed by the System Owner to formally approve the IT Security Plan and the residual risks>

<You can save as a separate document the next page and use it as a cover letter for the ARES approval process. You can then remove such Appendix 3 from your final version>

<The text of your approval note can be tailored to your needs>

<When you have completed also this approval step, make sure that all the related GovIS2 security fields are up-to-date: IT Security Plan, IT Security Plan Location, IT Security Plan Date, IT Security Plan Next Update>

EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Department / Unit / Sector

Brussels,
<Unit/Initials of authors>

NOTE FOR THE ATTENTION OF MR/MS <Insert name of the head of the commission department concerned>

Subject: **[Subject]**

The attached IT Security Plan covers the Communication and Information System named

< System name>.

The IT Security was commissioned by **< System Owner>**, created under the coordination of **<Security Risk Manager>**, with contributions from **<Stakeholders involved in the assessment>** and recommendations from **< LISO and any other relevant stakeholder>**.

The plan will be reviewed annually in accordance to C(2017)8841 to ensure it is accurate and adapted when there are significant changes to the infrastructure or application. If such modifications are made, it will be resubmitted for endorsement.
The current versions and annex documents will be always available for consultation in ARES. **<or Insert any location where the IT Security Plan is stored where>**

As System Owner, you are kindly requested to sign this approval note formally endorsing the attached IT Security Plan.

<Insert name of the System Owner and Signature >
……

c.c.: Type the recipient(s) you are copying to. Use Shift+Return to add lines.

<While saving this cover letter to **ARES**, please make sure DIGIT.S is in CC of this communication.

The signed ITSP should be always sent for **INFO** to the virtual entity **ve_digit.bfs1**>