SENSITIVE[1]

University of Harderwijk

Herbal Research Infrastructure

IT Security Plan

Doc Identifier

[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: LINK to handling sensitive information

Document Control Information

Settings	Value
Document Title:	IT Security Plan for the Herbal Research Infrastructure (HRI)
Document Author:	Fetze Alsvanouds
Project Manager (PM):	eduGAIN PM (if exists)
System Owner (SO):	Carl Linnaeus
Doc. Version:	0.2.71828
Date [YYYY-MM-DD]:	2025-03-17

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
0.1	2025/03/10	AARC Policy team	Initial version derived from the eduGAIN ITSP by Sven Gabriel

TABLE OF CONTENTS

Executive Summary 4

1. System Overview 5

1.1. Key Security Roles 5

1.2. User Population 5

1.3. System Description 6

1.4. System high-level architecture 7

1.5. Constraints and Compliance 7

1.6. Risk Acceptance Criteria 8

2. IT Security Risk Assessment Results 9

2.1. Risk Assessment Approach 9

2.2. Primary Assets 9

2.3. Asset Valuation Conclusions 9

2.4. Risk Identification and Analysis Conclusions 10

2.5. Deviations from Default Values 11

3. Risk Treatment Plan 12

3.1. Risk Treatment Approach 12

3.2. Selection and Prioritisation Criteria 12

3.3. Action Plan 12

Appendix 1: Full Risk Study 14

Appendix 2: References and Related Documents 14

Appendix 3: ITSP Approval Note 14

1. EXECUTIVE SUMMARY

This IT Security Plan contains the information about the system provided by the business owner of the Herbal Research Infrastructure (HRI) at the University of Harderwijk, and represents a high level overview of the system, and the outcomes of the Asset Valuation estimated through a Business Impact Assessment (BIA). Since the risk scenarios investigated here are taking in consideration only the threats and vulnerabilities listed in the Detailed Catalogues IT Security Risk Management Methodology v1.2, this version of the IT Security Plan serves primarily as a starting point and will be completed through the analysis of IT Security Incidents handled by the UoH CSIRT.

The HRI is a key research activity at the university, and about the only claim to fame that our university ever will have in the world. The infrastructure, established by Carl Linneaus, has had a profound impact on biology in the world: its services on taxonomic identification and indexing of plant species is of critical importance across the discipline worldwide, and there is no alternative for this service. Its community of users, globally distributed, augments the data provided by the HRI services, and without its contributing users the HRI, and hence the field of biology, will lose species-naming coherence. Without unique non-reassigned naming, research in biology cannot function. At the same time, citizens could also discover new species that will need naming, and more importantly rely on the HRI services to determine the ecological composition of household gardens, without which BBC2 would not have sufficient television programming. Since societal impact is an important measure for continued funding of the HRI, availability of such television programming is essential.

The protection of the HRI hence has to be the highest priority for university management, since the University of Harderwijk has no other assets, not even students. The IT Security Plan should be fully adhered to for continued existence of both HRI and the university itself.

2. 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.

2.1. Key Security Roles

Security role	Name	Contact
System Owner (SO)	Carl Linnaeus	c.linnaeus@uni-harderwijk.nl
Data Owner (DO)	Carl Linnaeus	c.linnaeus@uni-harderwijk.nl
UoH Security Officer	Prof. Fetze Alsvanouds	f.alsvanouds@uni-harderwijk.nl
UoH Security Officer (SSO)	O.S. Beroepsseclegend	abuse@uni-harderwijk.nl
Data Protection Coordinator (DPC)	Aart Staartjes	dataminer@uni-harderwijk.nl
Security Risk Manager (SRM)	**Participants Name**	**Email address**

2.2. User Population

User Group ID	Description	Priority
1	**Flora biologists, discoverers, and reseachers** Biologists supply new taxomomies and data to the HRI, as well as use the HRI to identify plant species and verify the consistency and materials in plant seed banks and dta from other research labs. They augment the databases of the HRI from their homebase institutions as well as during field trips.	High
2	**Citizens** The general citizenry uses the HRI portals to identify species in their gardens. Some attempt to add duplicate data or ‘new species’ because of insufficient flora determination skills.	Medium

3	**Compliance auditors** Auditing companies use the database to identify correct attribution and adherence to the Nagoya Protocol. Some less well-regarded auditing companies and activists may attempt to identify which legitimate researchers are accessing the HRI databases so as to complain about perceived non-compliance, or about interest in data related to GMOs that are to be classified as new species.	Low

2.3. System Description

The HRI is a comprehensive infrastructure for flora-centric research. It consists of

- Taxonomy information and meta-data for seed-bank vaults
- Databases with descriptions of flora for determination, and with genetic structures
- A citizen science portal for lookup and determination of plant species
- A collection submission system for new species
- A research institute for permanent staff and visiting sciensists to conjure up two-part names for plant species and prevent their correlation with any actual generic makeup of the plant involved
- A virtual home for researchers who do not otherwise have access to an identify they can use for access to both the HRI and other ESFRI infrastructures

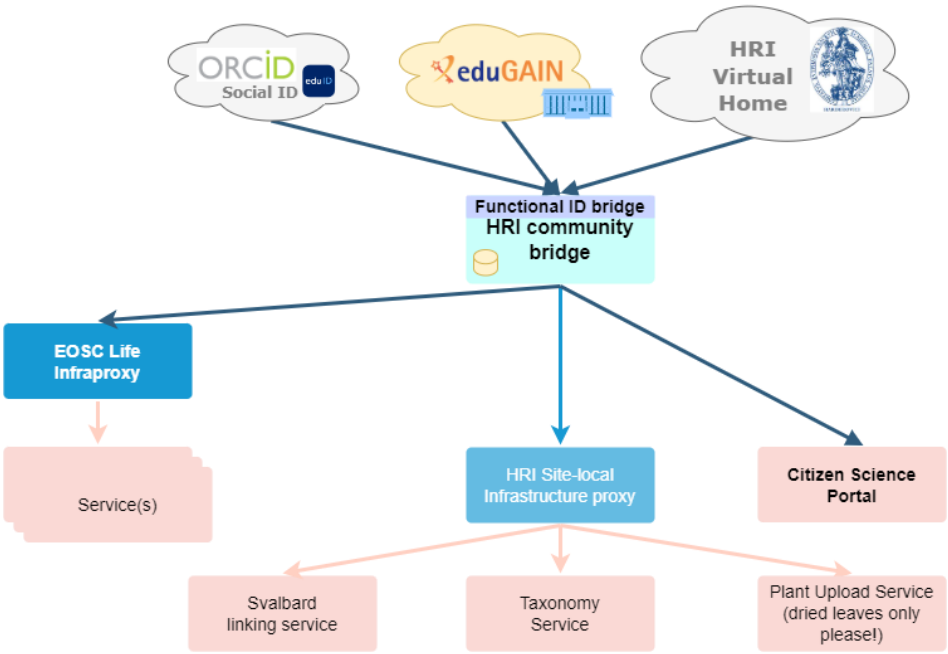
Currently, the HRI databases contain meta-data for 1,280,677 species and their taxonomies. The citizen science portal is being visited by at least 50,7 million people (in the typical spring month of April 2024), of which 50,7 million come from the UK, assuming all BBC viewers watch gardening programmes and proceed to analyse the taxonomy of the plants found there.

The HRI Institute itself in Harderwijk hosts 1 permanent staff member, but attracts 4 million visitors each year, who generate 1.92 billion potential taxonomic names per year. Each of these is curated in the database, althgouh duplicates are removed.

The Virtual Home for herbal researchers accomodates 65535 researchers that also use their HRI account to access useful research infrastructures via the EOSCLife Infrastructure Proxy.

Researchers (doing taxonomic work) and discoverers (who enter new precies data) can use eduGAIN federated access to login. The Virtual Home of the HRI is added to the list of all other eduGAIN IdPs in the login discovery page.

2.4. System high-level architecture



2.5. Constraints and Compliance

This section aims to identify the compliance requirements 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, if an exception is raised short explanation for that is required.*
- *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	Compliance Requirement [Y/N]		Mandatory Measures
CO-nnnn	GDPR: 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)>*

Constraint ID	Title	Compliance Requirement [Y/N]	Mandatory Measures
CO-nnnn	Security Operational Baseline…		
CO-nnnn	SIRTFI 1/2 document		

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>*
- *<SG: The Table 2 (Exceptions) will be completed later, it depends on the security measures catalogue>*

Constraint ID	Measure ID	Justification	End date

Table 2 – Exceptions in the ITSP from the compliance requirements

2.6. Risk Acceptance Criteria

Prelimenary Risk Acceptance Criteria is that any Risk below 5 will be automatically accepted. Depending on the category details this may be adjusted later.

ID	Description

Table 3 – Risk Acceptance Criteria

3. IT SECURITY RISK ASSESSMENT RESULTS

3.1. Risk Assessment Approach

The Risk Assessment was performed using the ITSRM methodology version 1.2.

For the brainstorm session the Basic Excel Tool v1.2, for the Asset Valuation and subsequently the Risk Assessment including the Secundary Assets GovSec.RM were used.

Methodology	*Tools*
ITSRM Methodology v.1.2	*GovSec.RM*
ITSRM Methodology v.1.0	*Basic Excel Tool v1.2*

	Stakeholder #1	**Stakeholder #2**	**…….**	
System Characterization (P1)	SO	SRM		*07/04/2025*
Primary Asset Inventory and Asset Valuation (P2)	SO	SRM		*07/04/2025*
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

3.2. Primary Assets

Ordered by the assets name:

		Description	Type	Owner
PA-1	User Management	This function comprises AAI, Accounting, On/Of boarding of users in a particular role, controlling access to the EOSC EU Node	Function	SO
PA-2	Data Management	Provide dataspace to participants to store data and provide means to control access to the data.	Function	SO

PA-3	Research data objects	Research data sets and results provisioned and obtained by citizen scientists	DATA	SO

< Task-1, create table of PAs, ontact the people identified as the Data and Function owners in the previous task to ensure a correct understanding of the Primary Asset values from a business perspective.>

3.3. Asset Valuation Conclusions

- The values in the System classification table were calculated with the RM-tool

	Confidentiality	Integrity	Availability
Maximum Asset Valuation	1	6	*6*
Classification	Public	high	high
Description	The information handled here is public	Damage Organisation image and reputation Consequential, limited to local/specific public	Damage Organisation image and reputation Moderate negative publicity, limited to local/specific public

Table 5 – System classification

<Asset Value: value of the asset assessed in terms of the maximum Impact (Business or Data Protection) in case of loss of a Security Dimensions (confidentiality, integrity, availability); this is also known as the Security Need.

Asset Value is a tuple with as many components as there are security dimensions envisaged, e.g. (C=2, I=3, A=4).

When you have completed ITSM step P1 and P2, please go in RM-Tool and update all the relevant security fields for this stage: ITSRM Methodology, RM-Tool ID, Confidentiality Level, Integrity Level, Availability Level>

Maximum Tolerable Period of Disruption (MTPD) is 48 hours . This value determines the mapping to the Business Continuity framework. Duration of unavailability from 12 hours to 48 hours is for critical systems.

RTO, RPO needed as well here. DRP/BCP needs to take these values into account. (DR/BC Plan is not part of the ITSP)

- *<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.>*

REST IS FOR THE PARTICIPANTS to sort out, basically the results from the RRisk Asssessment

3.4. 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.>*

3.5. 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'.>*

4. RISK TREATMENT PLAN

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

4.1. 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.>*

4.2. 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.>*

4.3. 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).>*
- *<GF: the part below is to be re-edited with offline MS Word to preferably have landscape orientation section in order to have the measures described more extensively>*

ID	Measure	Deadline	Owner	Sophistication
<Measure ID>	*<Name of the measure>*			
	<Measure description>	*<Deadline defined for the implementation>*	*<Department or person responsible of the implementation>*	*<Insert the sophistication level (Low/Medium/ 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:

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**>