

CRIS Tender 2026

Appendix 1. Requirements

APPENDIX 1. REQUIREMENTS	1
DEFINITION OF CONCEPTS AND ROLES USED IN THIS DOCUMENT	1
FUNCTIONAL REQUIREMENTS	2
<i>R. Basic CRIS functionality</i>	2
NON-FUNCTIONAL REQUIREMENTS	3
<i>A. Architecture & Compliance</i>	3
<i>B. Privacy</i>	4
<i>C. Security</i>	5
EXPLANATORY NOTES	6
1. RECORD TYPES CURRENTLY IN USE	6
2. MINIMUM SET OF MANDATORY FIELDS	7

Definition of concepts and roles used in this document

Concept	Definition
Outputs	Publications, activities, prizes, press/media coverage, datasets, software, artefacts and other resulting works that have been created by TU Delft staff.
Contributor	Contributors to outputs, i.e. authors, editors, supervisors, creators, inventors, etc.
System	The research output administration software system offered by the vendor (CRIS) when implemented, including additional showcasing functionality and intended integrations with other systems.
System Owner	Staff member responsible for policy and decision making about (future) use of the system.
System Admin	User with fullest access to the system's content, functionality and technical setting as designed by the developer. Responsible for effective and efficient configuration and user management.
Library Specialist	User based at the university library with tasks and responsibilities to register TU Delft's research outputs as complete and accurate as possible. Library Specialists typically do the work for one or more faculties.
Faculty Information Coordinator (FIC)	User based at a TU Delft faculty responsible for reporting at a faculty, faculty department or research group level.
Researcher	Scientific staff in one of TU Delft's faculties; including Postdocs and PhD students.
Portal	The web-based public facing interface belonging to the system allowing the public to see, browse, search and download the part of the stored content that has been labelled as 'public'.

Functional Requirements

R. Basic CRIS functionality

The following table contains requirements that should be met by a CRIS system.

No.	Required Function
R.1	The system can store, manage, and exchange high-quality, machine-readable metadata covering a broad range of content types. See section <i>Explanatory Notes: 1. Record types</i> listing of all types currently in use.
R.2	The system's content (sub)types have a (pre-defined) minimal set of mandatory fields which are needed to uniquely identify the work/item described. See section <i>Explanatory Notes: 2. Minimum set of mandatory fields</i> .
R.3	The system allows additional fields to be made mandatory, e.g. a classification field.
R.4	The system supports existing common descriptive practices and standards for bibliographic metadata where and whenever as possible.
R.5	The system presents possible duplicate records with sufficient metadata fields for (manual) evaluation and deduplication.
R.6	The system provides a configurable validation workflow.
R.7	The system offers functionality for bulk edits on workflow statuses and visibility statuses.
R.8	The system offers access to audit logs and import logs.
R.9	The system supports role-based access and includes roles to be tailored to the specific institute's needs.
R.10	The system admin must be able to grant additional access rights to individual users on top of their group rights.
R.11	The system allows users to manually add metadata of publications and other outputs.
R.12	The system supports automated/batch import and updates from external data sources to which the TU Delft subscribes and should include Scopus (Elsevier) or Dimensions (Digital Science).
R.13	The system supports automated synchronization schedules to retrieve new and updated data from external data sources.
R.14	The system allows the TU Delft to define the selection criteria/filter logic, used to import content from the external data sources to achieve the highest level of completeness.
R.15	The system alerts when synchronization fails or data anomalies occur.
R.16	The system provides functionality to validate (accept or reject) items retrieved from external data sources.
R.17	The system is supports using DOI and ORCID as persistent identifiers.
R.18	The system supports manual import of files by users in (at least) the following formats: RIS, Bibtex and CERIF XML.
R.19	Affiliation is used both for the record of a content (sub) type and for the record of a contributor . If the contributor's affiliation changes, for example by an update from the HR system, this must not change the affiliation of the associated "verified" records of content (sub) types.

R.20	The system allows contributors to have multiple affiliations. Affiliations can be connected to both internal and external organisational units.
R.21	The system offers a clear and intuitive interface allowing non-expert users to create ad hoc reports.
R.22	The system allows reporters to select the fields they want to include in the report.
R.23	The system can display alternative metrics derived from Altmetric or PlumX Analytics.
R.24	The system's Portal provides a configurable faceted search.
R.25	The system's portal allows the <i>System Admin</i> to decide to utilise new functionality and when to do so.
R.26	The system's portal offers a way to display the relationships between content and allows online visitors to navigate to related content using hyperlinks.

Non-functional Requirements

A. Architecture & Compliance

A.1	Data exchange must take place by means of web services. The web service must be a RESTful API.
A.2	The system's API provides requested data in a well-structured and consistent format, conform accepted standards, e.g. JSON, XML.
A.3	APIs must transport data using appropriate levels of (TLS) encryption and authentication. For TLS please follow guidelines as published by the Dutch NCSC (IT Security Guidelines for Transport Layer Security (TLS); https://www.ncsc.nl/en/transport-layer-security/tls-security-guidelines)
A.4	The system's API is CRUD capable (Create, Read, Update and Delete).
A.5	The system's API available endpoints and selection filters (attributes) are well documented; easy to access and written in easy-to-understand wordings.
A.6	The system's API uses secure keys to provide access to specified users.
A.7	The message exchange must be event/trigger driven. So-called upsert messages must be used. The application that receives data can independently assess whether an update or an insert is needed.
A.8	It must be possible to use all functionalities of the system with all browsers that have a market share of 5% or more without the use of additional plug-ins.
A.9	The system must support SCIM 2.0 API (or equal functionality)
A.10	In situations in which the supplier is no longer able to provide the Cloud service (for example, in the event of bankruptcy), TU Delft can either have access of the source code of the Cloud services (for example, via ESCROW) or fall back on some other provision to keep the functionality (temporarily) available in order to guarantee the continuity of its processes (as far as possible).
A.11	It must be possible to use the system independently regardless of the time (except for maintenance windows) or device. The users must have the option to use the system from a mobile computer or workstation at the institution or from home.
A.12	The system must support federated single sign-on via SAML or OpenID via SURFconext (see: https://www.surf.nl/en/surfconext-globalaccess-with-1-set-of-credentials)

A.13	The system can deliver the relevant data to the TU Delft data warehouse platform on a regular basis and with acceptable performance. This can be bulk transactions via web services, database extraction files via SFTP or other generic solutions.
A.14	The system's user interface is available in at least English for all users.
A.15	Next to a production environment a test or sandbox environment must be set up and made available to the TU Delft.
A.16	The system must be compliant with Web Content Accessibility Guidelines (WCAG) 2.2, level AA.
A.17	If the system uses Artificial Intelligence (AI) then the supplier has an obligation to ensure that its deployment meets the legal obligations of the EU AI Act (see: https://aiactinfo.eu): • The supplier must state, with reasoning, how each AI feature is classified under the AI Act (prohibited, high-risk, limited-risk transparency, or minimal-risk). • Users must be clearly told when they are interacting with an AI system, such as an assistant or chatbot. • AI-generated or AI-modified content (abstracts, lay summaries, profile texts, keywords) must be marked as such in the interface. • Institutional and research data, including unpublished work, must not be used to train or improve the supplier's or any third party's models without written consent.
A.18	The system should provide functionality to record and handle retention periods by relevant object types.
A.19	The system can migrate content; both information objects and metadata in predetermined formats. Suppliers have to facilitate in exit-scenarios and make a full export of all data available. Migrations will not lead to a loss of context or cohesion of the information objects.

B. Privacy

B.1	The Tenderer makes sure that the Solution provides functionality that enables TU Delft to easily comply with all data subject rights (article 1522 GDPR).
B.2	The Tenderer must sign the Processor Agreement. By registering, the tenderer declares to comply with the provisions of the Processor Agreement.
B.3	The Tenderer must work in accordance with the principles of 'Privacy-by Design' and 'Privacy-by-Default'.
B.4	The Tenderer must act in accordance with the General Data Protection Regulation (GDPR) and other applicable laws and regulations regarding the processing of personal data.
B.5	The Tenderer is obliged to explain the tenderer's data breach and reporting procedures when TU Delft requests this.
B.6	The Tenderer must inform TU Delft of data breaches immediately (within 48 hours).
B.7	The Tenderer stores all personal data processed in the Solution on EU/EEA territory.
B.8	The Tenderer must specify where personal data is stored when data is processed by sub processors. The tenderer performs a data transfer impact assessment (DTIA) when data is processed by sub processors outside the EU/EEA. The tenderer is obliged to share the DTIA with TU Delft as soon as TU Delft requests this.
B.9	The supplier encrypts all personal data, owned by TU Delft, at rest and in transit at all times.
B.10	The Tenderer will support the TU Delft, without additional costs, in performing a Data Protection Impact Assessment (DPIA) on the system.

B.11	The Tenderer appoints a representative in the EU/EEU according to article 27 of the GDPR when the tenderer is not established within the EU/EEA.
B.12	the Tenderer is able comply with TU Delft retention policies and is able to destroy TU Delft personal data upon termination of the contract.

C. Security

C.1	The Tenderer must have a valid internationally recognized certification about the available technical and organizational security measures on the aspects Availability, Integrity, and Confidentiality, for example NEN ISO 27018 or the more general NEN ISO 27001 or equivalent. The Certificate must be issued by an accredited external auditor.
C.2	The supplier sets up a process to prevent the use of technical vulnerabilities. In any case, the process includes: - regularly keeping systems and software up to date (patching) - timely gathering of information about new vulnerabilities (intelligence) - the automated checking of program packages and infrastructural software for known weaknesses - continuous testing of web applications for vulnerabilities (Web application scanning) and performing a penetration test at least once a year - the use of anti-malware (including anti-virus) software from different providers with different engines which are updated daily - restrictions on installing (unauthorized) software
C.3	The supplier is responsible for 24/7 proactive monitoring of the application regarding intrusion detection and (D)DOS detection. The tenderer must immediately notify TU Delft of any breach of the security measures.
C.4	The Tenderer must pursue an active security update policy whereby it strives to implement critical security updates within 5 working days. Security updates for CVSS score higher than 9 (nine) must be implemented within 24 hours.
C.5	The system must have an A-status at https://www.ssllabs.com/ssltest/ .
C.6	The Tenderer must conduct a security audit at least once per year and must provide the results to the TU Delft. In addition, TU Delft is entitled to perform, or to have performed a security audit.
C.7	The supplier carries out a risk analysis at least every year to the threats and vulnerabilities, their consequences for the organization and the likelihood of those consequences. Based on the risk analysis, adequate security measures are established and introduced. The tenderer must provide access to the last two risk analyses related to an audit of their environment/application, if requested by TU Delft.
C.8	The system logs at least the moment of login and the IP address of each user. If logouts are executed these must be logged as well.
C.9	The system logs relevant traffic (sufficient to be able to attribute malicious activities to a certain user and or system: at least accurate timestamp, user, ip addresses, action, status). The log is kept for at least 6 months and can be viewed by authorized persons of the TU Delft.
C.10	The system uses the most recent standard security protocols and algorithms, as described on Forum Standaardisatie: https://www.forumstandaardisatie.nl/open-standaarden/verplicht
C.11	The system provides 2 factor authentication for accounts that are required outside of the federated single sign on (SSO) service.

Explanatory Notes

1. Record types currently in use

Listed are the record types TU Delft wants to use:

- Persons
- Organisation/ Organisational units
- Grants / Awards
- Projects
- Publications
 - Journal contributions (specified, e.g.: (meeting) article, letter to the editor, review)
 - Books (authored, edited)
 - Chapters (in a book, in conference proceedings)
 - Reports
 - Working papers
 - Pre-prints
 - Conference contributions (papers, (extended) abstracts, posters)
 - PhD theses (dissertations)
 - Artefacts
 - Designs
 - Digital/Visual products
 - Websites
 - Online publication (e.g. blog article)
- Patents
- Datasets
- Software
- Equipment/Facilities
- Impact/Case studies
- Funders / Award-giving organisation
- Journals
- Publishers
- Press/Media coverage
 - Interview
 - Media coverage item (online, streaming, print, tv, radio)
 - Press releases
- Events
 - Conferences
 - Workshops
 - Seminars
 - Lecture series
 - Exhibitions
- Activities
 - Editorial work
 - Peer reviewing
 - Talks & presentations
 - Consultancy
 - Memberships
- Prizes and other forms of recognition
 - Prize

- National/international honour
- Fellowship awarded competitively
- Other distinction

2. Minimum set of mandatory fields

For research outputs/academic works, activities, prizes, media content, datasets, software the following fields are mandatory (cannot be empty):

- Type (selected from list)
- Year (when the content was published, made available, took place)
- Title
- Contributor (at least one internal)
- Affiliation of contributor: research group
- Affiliation of the record: faculty, faculty department, research group