European
Commission

Digital Europe Programme (DIGITAL)

Classification of information in Digital Europe projects

Version 1.0
01 November 2021

IMPORTANT NOTICE

This document aims at providing guidance on when and how security-sensitive information produced by Digital Europe Programme projects should be classified. The specific objectives of this document are to:

- inform applicants on when and how information may be designated by an EU classification marking and at which level and help them to draft a comprehensive security self-assessment and security section
- help the granting authority staff to identify potential security sensitive topics in the calls for proposals, as well as to identify potential security issues in ongoing funded projects
- assist the national security experts of the Security Scrutiny Group with conducting the Security Scrutiny of proposals that have been selected for funding.

⚠ This guidance concerns solely protective measures to be taken to preserve the confidentiality of security-sensitive information in Digital Europe Programme projects. Other aspects *(e.g. data protection, ethical issues, dual-use, etc.)* are covered in other parts of the evaluation procedure.

⚠ Projects with classified information must comply with Decision 2015/444 and the Implementing rules on classified grants.

Under the new security rules, all classification markings must now be written in FR/EN format *(e.g. RESTREINT UE/EU RESTRICTED)*.

HISTORY OF CHANGES		
Version	**Publication Date**	**Change**
1.0	01.11.2021	▪ Initial version (new MFF 2021-2027)
		▪
		▪
		▪
		▪
		▪

Table of contents

1. When and for how long must information be classified?

Under Decision 2015/444[1] and the Implementing rules on classified grants[2], information must be classified as EU classified information (EUCI) if its **unauthorised disclosure could adversely impact the interests** of the EU or of one (or more) of its Member States.

There are two types of classified information:

Classified background information — is information already classified by the EU entities, nation states or international organisations, which is used in the frame of a project.

Classified foreground information — is information produced by a project, which is classified as EU Classified Information (EUCI).

> ***Example:*** *some of the information produced by a project could potentially be used to plan terrorist attacks or avoid detection of criminal activities*

To minimise costs and restrictions caused by classifying project information, the classification will be for a limited time — after which classification will be reviewed and possibly downgraded, declassified or extended.

⚠ Classification of information may be combined with other **security recommendations (REC)** *(e.g. limited dissemination, creation of a security advisory group, limiting the level of detail, using a fake scenario, excluding the use of classified information, etc.).*

2. Classification levels

There are four **levels of classification**:

- TRÈS SECRET UE/EU TOP-SECRET **(TS-UE/EU-TS)**

  ⚠ TRÈS SECRET UE/EU TOP-SECRET — projects involving information classified TRÈS SECRET UE/EU TOP SECRET cannot be funded under the Digital Europe Programme.

- SECRET UE/EU SECRET (**S-UE/EU-S**)

  Use this classification for information which could *seriously harm* essential EU or national interests.

  Example: *threatening of life or the serious prejudicing of public order or individual security and liberty*

- CONFIDENTIEL UE/EU CONFIDENTIAL **(C-UE/EU-C)**

  Use this for information which could *harm* essential EU or national interests.

  Example: *inception of damage to the operational effectiveness or security of a Member State or other State's forces or to the effectiveness of valuable security or intelligence operations*

- RESTREINT UE/EU RESTRICTED **(R-UE/EU-R)**

[1] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p.53.)

[2] Commission Decision (EU, Euratom) 2021/259 of 10 February 2021 laying down implementing rules on industrial security with regard to classified grants (OJ L 58, 19.2.2021, p. 55)

Use this for information which could be **disadvantageous** to those interests.

> ***Example:*** *information which could potentially make it more difficult to maintain the operational effectiveness or security of Member States or other State's forces*

3. How to classify information

The classification of information produced by digital projects will normally depend on two parameters:

- the subject-matter of the project, such as:
  - **cybersecurity**
  - **quantum technologies**

AND

- the type of the results and whether it is being done in simulated environments *(e.g. serious gaming, etc.)* or (nearly) operational environments, such as:
  - **threat assessments** (i.e. estimation of the likelihood of a malicious act against an asset, with particular reference to factors such as intention, capacity and potential impact)
  - **vulnerability assessments** (i.e. description of gaps or weaknesses in networks, services, systems, assets, operations or processes which can be exploited during malicious acts, and often contain suggestions to eliminate or diminish these weaknesses)
  - **specifications** (i.e. exact guidelines on the design, composition, manufacture, maintenance or operation of threat substances or countermeasure substances, technologies and procedures)
  - **capability assessments** (i.e. description of the ability of an asset, system, network, service or authority to fulfil its intended role — and in particular the capacity of units, installations, systems, technologies, substances and personnel that have security-related functions to carry these out successfully)
  - **incidents/scenarios** (i.e. detailed information on real-life security incidents and potential threat scenarios):
    - on past incidents (often including details not otherwise publicly available, demonstrating the real-life effects of particular attack methods or security gaps which have since been addressed)
    - on devised scenarios (commonly derived directly from existing vulnerabilities, but normally with a lower level of detail, particularly of the attack preparation phase)).

⚠ These categories are not exhaustive, and may overlap.

3.1 Cybersecurity projects

What?

'**Cybersecurity**' covers a wide range of topics linked to security aspects of the internet and of digital systems, infrastructures, processes and services, such as relevant tools and technologies (e.g. cryptographic techniques, artificial intelligence systems, situational awareness tools) and other relevant technological and procedural measures used to ensure confidentiality, integrity and availability of the concerned information.

Digital systems and infrastructures might include some sensitive information, in particular concerning the security measures used to protect them. In some cybersecurity projects, EU classification might not be required to handle such sensitive information. In other projects, a suitable level of EU classification might be required in view of either the specific domain/sector addressed, or the content/type of the envisaged deliverables or whether the outcomes will be validated in (nearly) operational environments.

The need for EU classification in cybersecurity proposed projects will be examined for each proposal on a case-by-case basis.

How to deal with threat assessments?

Threat assessments prepared by cybersecurity projects may include some sensitive sections and even classified ones.

How to deal with vulnerability assessments?

Particular attention should be paid in the area of vulnerability assessments. For example: The proposed cybersecurity projects may come upon previously unknown vulnerabilities (‘zero-day vulnerabilities’); in this case, responsible disclosure is required and EU classification might be needed.

How to deal with specifications?

In some cases, the specifications prepared during a cybersecurity project might need to be classified. For example, a project for the procurement/establishment of a critical digital infrastructure aiming to improve cybersecurity, where one of the first steps would be the elaboration of technical specifications for such infrastructure.

How to deal with capability assessments?

Classification might be needed e.g when the proposed project plans to handle highly sensitive information/data.

How to deal with incidents/scenarios?

Classification might be necessary for some use-case risk assessments. Depending on the type of use-case and the context of the project, the results of information security risk assessments *(especially if obtained in operational or near operational environments)* may include certain threats and/or vulnerabilities that require classification. For example, in case of critical infrastructures, the operational risks assessment may need to be classified.

3.2 Quantum technologies projects

What?

Quantum Technologies are structured around four distinct but interconnected application domains (Communication, Computing, Simulation as well as Sensing & Metrology), which are complemented by a Scientific and Technological Resources area, which encompasses basic science and cross-cutting activities — engineering, control, software and theory.

A specific deployment initiative is EuroQCI, which is part of the quantum communication domain. The EuroQCI will link critical public communication assets all over the EU, and would make it possible for sensitive information to be transmitted and stored much more securely — using quantum key distribution. It would help to protect the EU’s key digital assets, secure financial transactions, shield national and cross-border critical information infrastructure against eavesdropping.

We assume that in most cases Quantum Technologies proposal do not need any classification. However, in some specific cases, projects in particular under the EuroQCI initiative may need to be classified. In this case, the EU classification levels may need to be determined according to the specific subject- matter, the type of the results and whether the projects outcomes are delivered in simulated environments or in (nearly) operational environments.

The need for classification of Quantum Technology projects will be examined for each proposal on a case-by-case basis.

How to deal with threat assessments?

Threat assessments prepared by quantum communication projects may include some sensitive sections even to the level of need for classification.

How to deal with vulnerability assessments?

Particular attention should be paid in the area of vulnerability assessments. Projects may come upon previously unknown vulnerabilities; in this case, responsible disclosure is required and classification might be needed in accordance with the rules and classification levels foreseen for the specific subject-matter.

How to deal with specifications?

The need for classification of Quantum Technology projects specifications will be examined for each proposal on a case-by-case basis. The classification levels will be selected by the EuroQCI security group in accordance with applicable national, international and EU legislation. Specification data includes:

- Detailed information on the design, characteristics, operation and requirements of, and prototypes for, key functional devices for use in EuroQCI.
- Systems information *(such as the functional or technical architecture, platforms, software and algorithms)*.
- Detailed information on operational processes, including information on communication and interoperability *(such as frequencies used, data rates and communication protocols)*.

Regarding the EuroQCI infrastructure, information should be classified at the same level whether terrestrial or space segments are concerned. Coherence between the level of classified information produced by ESA and by the EU should therefore be ensured.

How to deal with capability assessments?

Classification might be needed *e.g when the proposed project plans to handle highly sensitive information/data*. **How to deal with incidents/scenarios?**

Classification might be necessary for use-case risk assessments. Depending on the type of use-case and the context of the project, the results of information security risk assessments (especially if obtained in operational or near operational environments) may include certain threats and/or vulnerabilities that require classification.