Horizon Europe Cluster 3

Civil Security for Society | WP 2026–2027 Proposal Readiness

Cluster 3 supports projects that strengthen the protection of EU citizens against crime and terrorism, improve border and infrastructure resilience, enhance disaster preparedness, support cybersecurity, and develop socially acceptable security solutions with stronger industrial uptake. The 2026 Cluster 3 info session took place on **4 March 2026**, and the 2026–2027 Cluster 3 work programme was published on **11 December 2025**.

nexuswelt

What a strong Cluster 3 proposal must show

A competitive proposal should not present technology alone. It should demonstrate:

Policy Relevance

Clear alignment with EU security policy frameworks and priorities.

Operational Value

Demonstrated value for practitioners working in security and civil protection.

Preparedness & Resilience

Contribution to preparedness and resilience across EU Member States.

Social Acceptability

Acceptability of the solution to society and affected communities.

Deployment Pathway

A realistic pathway toward deployment, commercialisation, or wider uptake in Europe.

Cluster 3 is explicitly framed around **protection against crime and terrorism**, resilient infrastructure, disaster-resilient societies, cybersecurity, stronger borders, and security innovation with industrial and societal value.

Work package design under the lump-sum logic

For lump-sum topics, work packages must be designed as **meaningful blocks of work with clear completion points**. The following principles apply:

1 Not just one task or a percentage of progress

A work package should not be just one task, a percentage of progress, or a simple time split such as "Year 1 activities."

2 Define around concrete results

Proposals should define work packages around concrete results, deliverables, and completion milestones.

3 Splitting across reporting periods

Splitting a long work package across reporting periods is possible, but only when it supports cash-flow logic rather than compensates for weak proposal structure.

> The Commission's lump-sum guidance states that **payment is linked to completion of work packages** rather than to reimbursement of actual declared costs.

SSH must be embedded, not decorative

What SSH integration means

Social Sciences and Humanities should be integrated wherever the topic requires:

- Societal understanding
- Behavioural insight
- Governance analysis
- Risk perception
- Public trust
- Ethics, adoption, or user acceptance

In practice, SSH should appear in:

- The methodology
- Tasks and deliverables
- Consortium structure

SSH partners should **not** sit outside the core work plan as symbolic contributors.

In Cluster 3, this is especially important where technologies affect people, institutions, public services, emergency response, or societal security outcomes.

Gender dimension in research and innovation content

This point is confirmed. Under Horizon Europe, **integration of the gender dimension into R&I content is a default requirement** unless the topic text explicitly says it is not mandatory. It is evaluated under the **Excellence criterion**.

Problem Framing

Gender should be addressed where relevant in how the problem is defined and scoped.

User Needs

Differentiated user needs by gender must be considered in the design of the solution.

Methodology

Gender-sensitive approaches should be embedded in the research methodology.

Testing & Validation

Testing and validation activities should reflect gender considerations.

Impact Logic

The impact logic should account for differentiated outcomes across genders.

This concerns **research content**, not just the gender balance of the team.

GEP eligibility: what matters

A **Gender Equality Plan** is an eligibility requirement for specific organisation types. Understanding who is in scope is essential for consortium planning.

Organisations required to hold a GEP

- Public bodies
- Higher education institutions
- Research organisations from EU Member States and associated countries

SMEs are not in that mandatory category.

Where a GEP is required, it must:

- Be a **public formal document**
- Include **dedicated resources**
- Include **monitoring measures**
- Include **training measures**

Security is a core design issue in Cluster 3

Cluster 3 proposals must treat security seriously from the proposal stage. The **security self-assessment** is used to identify whether a project raises security concerns, including sensitive or classified content, and whether it may require formal security scrutiny before grant signature.

The official Commission guidance explains that this process is meant to:

Identify security risks

Assess possible use or generation of sensitive or classified information.

Verify proper addressing

Verify whether the issues have been properly addressed in the proposal design.

Define mitigation measures

Define mitigation measures where necessary to manage identified risks.

nexuswelt

Sensitive vs classified information

A good proposal should distinguish clearly between three categories of information:

Public Information	Confidential Sensitive Information	EU Classified Information
Freely accessible, no handling restrictions required.	Requires controlled handling, access restrictions, and defined security procedures.	Subject to formal classification handling rules and designated security responsibilities.

Proposals themselves should not include classified information, but project activities or outputs may involve sensitive handling rules depending on the topic and the design of the action. Where relevant, applicants may need to describe security procedures, access restrictions, classification handling, and designated security responsibilities.

Ethics must be concrete

Ethics should be addressed in **practical, specific language**. If the project raises issues such as the following, the ethics section should explain what the issue is and how it will be managed:

Intrusive data processing

Profiling, monitoring, or sensitive personal data handling.

AI-related risks

Automated decision-making, bias, or algorithmic accountability concerns.

Covert methods

Other serious societal concerns arising from covert or intrusive approaches.

> **Generic wording is weak** and usually creates problems later in evaluation or grant preparation. REA guidance also warns applicants not to forget ethics and security issues when preparing proposals.

The strongest Cluster 3 proposal message

Success comes from combining all of the following elements into a coherent, deployment-oriented European security project:

- **Operational Relevance**
- **Policy Alignment**
- **Strong Methodology**
- **Manageable Lump-Sum WP Design**
- **Real SSH Integration**
- **Credible Gender Dimension**
- **Early Security & Ethics Handling**

> The proposal should read as a **deployment-oriented European security project**, not only as a technical R&D concept.