Terms of Reference
Consultancy: Development of a digital security toolkit

Tailored digital security resource for Civil Society Organizations in high-risk and diverse contexts

Publication date: September 19th 2025
Submission deadline: November 2nd, 2025 EOB
Estimated start date: End Nov. / Early December 2025
Estimated end date: End Q1, 2026
Location: Remote

1. Background and Context

The EU System for an Enabling Environment for Civil Society (EU SEE) is a global consortium of CSOs and networks operating in 86 countries. EU SEE's core mission is to monitor, document, and respond to changes affecting the enabling environment for civil society, through an Early Warning and Monitoring Mechanism. Members of the network operate in diverse digital environments that require varying levels of technical expertise, secure communication skills, and adaptive security practices.

Given that members conduct research on civic space conditions and analyze the operating environment for civil society actors, they require robust digital security processes and tools to protect their research integrity, maintain stakeholder confidentiality, and ensure secure data collection and analysis.

As part of EU SEE commitments to safeguard for the wellbeing of all partners, the consultant will adapt existing resources to the work processes and context of the project to protect EU SEE initiative's and partners' data and online communication.

2. Objectives

The consultant will:

- Analyse EU SEE members' needs and existing processes and tools related to Digital Security. Conduct interviews/surveys and workshops with 10+ EU SEE members (covering diverse regions and threat levels), 2+ key external stakeholders (donor, connected consortium) and with all EU SEE consortium partners, to understand the current behaviours, risks, requirements, needs, gaps, expertise, etc.
- In collaboration with project partners with technical expertise, co-develop a toolkit comprising two coherent elements: 1) a practical, modular tool on digital security, tailored to the risks and capacities of EU SEE members and their local partners in 86 countries; 2) a standardised response guide to security breaches, tailored to the EU SEE consortium. This co-creation will include a testing phase that will take place as part of an online workshop.

- Ensure the toolkit aligns with the standard project processes, security protocols and workflows of the consortium partners and the network members, supporting secure data collection, storage, and sharing. Use real-world examples from EU SEE members' work.
- Address the heterogeneity of contexts: low-bandwidth, internet shutdowns, and any cyberattacks or threats.
- Pilot and refine the toolkit with 5+ EU SEE members (representing diverse regions/threat levels) and 3+ EU SEE consortium partners: Test the toolkit, get feedback (online workshop), and adjust content.
- Deliver a final product that is actionable, culturally sensitive, user-friendly (creative format), and ready for immediate deployment across the network.
- Present the toolkit to EU SEE members and EU SEE consortium partners (2 online presentation sessions).

3. Scope of Work

3.1 Content

The toolkit must at least cover the following areas, with context-specific adaptations:

- Digital risk/threat assessment
- Secure communications & secure collaboration
- Data protection, privacy, consent & storage
- Device & account security
- Incident response & resilience
- Digital hygiene
- Legal compliance
- Training & Capacity building

Example of tailored tools should be encompassed in the toolkit, such as:

- Region-specific case studies
- CSO-specific case studies and threats
- Up to date, relevant resources & tools & templates. Multilingual will be a plus.
- Low-bandwidth solutions
- Circumvention tools for censored environments
- Hardware guidelines
- Software guidelines
- Response plan & protocol samples

3.2. Deliverables

Deliverables	Description
Inception report	Analysis of EU SEE's digital threats, member needs, and existing tools.
Draft toolkit	Full content in English
Pilot – Testing phase	Testing with EU SEE members and EU SEE consortium partners; revisions.
Final toolkit	Full content in English. Digital & print ready. Presentation of the toolkit (2 online sessions).

4. Consultant qualifications

The consultant will demonstrate:

4.1 Deep understanding of CSO digital risks in at least 3 continents.

- Proven experience working with human rights defenders, journalists, or advocacy networks in repressive or high-risk environments.
- Familiarity with digital security threats faced by monitoring/alert systems (e.g., secure data collection, whistleblower protections).
- Knowledge of EU SEE's context: experience with enabling environment monitoring in different contexts is a strong asset.

4.2 Technical expertise

- Digital security specialization: hands-on experience with threat modeling, secure comms, incident response, and data protection.
- Toolkit development: portfolio of accessible, non-technical guides for non-experts (e.g., activists, local NGOs).
- Adult education skills: ability to simplify complex concepts and tailor tools to diverse audiences.

4.3 Contextual adaptability

- International experience.
- Ability to quickly grasp EU SEE's workflows, threats, and member needs (e.g., through interviews, desk research).
- English required; French, Spanish is desirable for communications with Network Members.
- Cultural sensitivity: experience localizing content for diverse legal, technical, and social contexts.
- Flexibility: capacity to iterate based on pilot feedback and meet deadlines.

6. Budget and contractual terms

Maximum budget for the consultancy services: **€20,000** (inclusive of taxes).

Contract specificities:

- All EU SEE data and materials are strictly confidential.
- The toolkit will be the exclusive property of the EU SEE consortium.

7. Application process

Applicants must submit:

- Technical proposal (max 5 pages, in English): approach & sample toolkit content.
- Financial proposal (VAT must be included)
- CV + Portfolio
- References: 3 contacts from previous clients (preferably CSOs or networks).

Deadline for applications: November 2nd , 2025

Submission email: recruitment@forus-international.org