Connect, Defend, Act!

Digital Security Assessment, Curriculum Development, Training of Trainers (ToT), and Digital Security Service Mapping – Terms of Reference

1. Context and Background

Across the world, including in Palestine, civic space is increasingly constrained. Civil Society Actors (CSAs), human rights defenders, independent media, and rights-holder–led organizations face growing political, legal, institutional, and societal pressures that limit their ability to organize, express dissent, mobilize communities, and defend fundamental human rights. These restrictions are reinforced by expanding digital surveillance, cyber-attacks, online harassment, and data exploitation by both state and non-state actors.

Digital tools and platforms hold significant potential to enable safe, inclusive, and collaborative civic action. However, unequal access to technology, gaps in digital security knowledge, and rapidly evolving digital threats undermine this potential—particularly for marginalized groups such as women, youth, persons with disabilities, and grassroots or rights-holder–led organizations.

With support from the Norwegian Agency for Development Cooperation (NORAD), Hivos is implementing the Connect, Defend, Act! project. The project aims to respond to shrinking civic space in Palestine by amplifying civil society–led action to defend and expand civic space. It emphasizes local ownership, leadership, and agency, with Hivos playing a facilitating and supportive role that builds on existing knowledge and capacities within civil society.

1.1 Project Goal

Civil society actors can positively influence the openness of, and respond effectively to changes in, civic space.

1.2 Project Objectives

I. Promote coalition building among diverse civil society actors, including human rights defenders, rights holder-led civil society organizations, and independent media actors, grounded in civil society-led evidence gathering and knowledge production, and facilitated by context-specific communities of action.

II. Contribute to safe and inclusive digital civic spaces for sustained collaboration and action among civil society actors through localized holistic digital security capacity strengthening, knowledge production, and active referral to digital protection providers.
III. Increase civil society actors' flexibility to rapidly respond to changes in civic space through organizational capacity strengthening and the provision of strategic funding for sustainable action.

The project prioritizes groups marginalized within civil society, such as women, youth, and other marginalized groups. Across all activities and outcomes, Hivos promotes local ownership and leadership, emphasizing civil society actors' agency and existing knowledge.

2. Purpose and Objectives of the Assignment

2.1 Purpose of the Assignment

These Terms of Reference define the scope, objectives, deliverables, and expected outcomes for a consultancy to strengthen digital security practices among Civil Society Actors (CSAs) and Civil Society Organizations (CSOs) in Palestine. The consultancy will work with 18 Civil Society Actors (CSAs) and Civil Society Organizations (CSOs) already identified as Community of Action (CoA) members under the Connect, Defend, Act! project. These organizations will be contacted to participate in the digital security assessment and will be the primary recipients of the Training of Trainers (ToT) program.

The consultancy will deliver an integrated package of work comprising:

- A Digital Security Needs Assessment
- Digital Security Curriculum and Training Materials Development
- A Training of Trainers (ToT) Program
- Digital Security Service Mapping and Case-Based Learning

The assignment aims to:

- Assess digital security risks, capacities, gaps, and differentiated protection needs among 18 CSAs and CSOs
- Develop a context-specific, accessible, and reusable digital security curriculum and raining materials
- Build sustainable internal capacity through a Training of Trainers approach
- Increase awareness of and access to existing digital security and protection support services through structured mapping and documentation

Through these components, consultancy will strengthen digital resilience as a foundation for civic engagement, advocacy, coalition-building, and resistance to repression across digital and physical civic spaces.

2.2 Objectives

A. Digital Security Assessment

- Identify and map CSAs and CSOs participating in the assessment, with particular attention to rights-holder–led and marginalized groups.
- Design and implement a holistic digital security needs assessment using feminist and intersectional methodologies.
- Analyze and document key digital threats, vulnerabilities, risks, skills gaps, and differentiated protection needs.
- Produce actionable, context-specific recommendations to inform curriculum development.

B. Curriculum Development and Training Material

- Develop a context-specific digital security curriculum aligned with global best practices and adapted to Palestine context.
- Localize the curriculum and training materials for Palestinian context, ensuring accessibility.
- Collaborate with Community of Action (CoA) Facilitators and members to co-design content, ensuring it meets their security and advocacy needs.
- Design the curriculum and materials as reusable knowledge of products to support future training.
- Publish the finalized curriculum and training materials on a publicly accessible online platform and share active links with the commissioning entity.

C. Training of Trainers (ToT) Program

- Design and deliver a Training of Trainers (ToT) program for 18 CoA Members.
- Support CoA Members to organize and deliver at least one on-site or community-based training using the developed curriculum.
- Provide feedback and refinement of the training content based on participant experience.
- Support the dissemination of online and offline training resources beyond CoA Members.

D. Digital Security Service Mapping and Case-Based Learning

- Map existing digital security-related support services, including technical, legal, and psychosocial assistance providers relevant to CSAs in Palestine.
- Develop a confidential digital security service provider directory for internal project use.
- Document a minimum of two anonymized cases illustrating how CSAs experiencing urgent digital security incidents navigate available support mechanisms.
- Identify key gaps, risks, and limitations in accessing digital security and protection services.

2.3 Expected Outcomes

The consultancy is expected to contribute to the following outcomes:

- Enhanced understanding of digital security risks and needs among CoA Members and other CSAs, informing interventions, curriculum design, and advocacy.

- Availability of localized, accessible, and reusable digital security curriculum and training materials, tailored to contextual needs, published online and publicly accessible.
- Strengthening capacity of CoA Members to deliver digital security training to other CSAs, promoting multiplier effects in digital literacy and security.
- Increased awareness of existing digital security and protection support options through Digital Security Service Mapping and Case-Based Learning.
- Enhanced resilience of Civil Society Actors to digital threats, supporting safer and more inclusive digital civic spaces for sustained collaboration and action.

3. Scope of Work

Scope of Consultancy:

The consultancy will focus on the West Bank (including East Jerusalem) and engage the identified CoA members in the digital security assessment and Training of Trainers program.

Target Group: The consultancy will engage the 18 CoA member organizations already identified under the project.

A. Digital Security Assessment

- Conduct a comprehensive assessment of digital security practices, risks, and vulnerabilities affecting CSAs and CSOs in Palestine.
- Identify risks, vulnerabilities, and threats that could impact CSAs and CSOs
- Deliver a detailed assessment report with prioritized, context-relevant recommendations to inform curriculum, training, and advocacy.

B. Curriculum Development and Training Material

- Develop a structured, modular digital security curriculum, covering (at minimum):
    - Introduction to Digital Security and Threat Landscape.
    - Data Protection Laws and Regulations.
    - Identifying and Responding to Cyber Threats.
    - Encryption and Secure Communication Tools.
    - Social Engineering Tactics and Mitigation.
- Ensure that the curriculum includes interactive and practical exercises, such as simulations of common digital security threats.
- Include clear learning outcomes, objectives, and assessment methods to ensure the curriculum is effective and measurable.
- Develop training materials aligned with the curriculum.
- Publish finalized curriculum and training materials online (consultant/company website or recognized training platform), ensuring public access and sharing of active links with the commissioning entity.

C. Training of Trainers (ToT)

- Design multi-day ToT sessions focused on digital security topics.

- Deliver training sessions for the selected trainers, covering key concepts in digital security and adult learning methods.
- Provide CoA Members with comprehensive training packages (manuals, slides, exercises, case studies).
- Evaluate trainers' readiness and capacity to deliver training to others.
- Support CoA Members in organizing and delivering at least one on-site or community-based training course using the developed curriculum and materials.
- Collect feedback, lessons learned and refine content.
- Disseminate finalized online and offline training resources to a broader CSA audience.

D. Digital Security Service Mapping and Case-Based Learning

- Identify and document relevant local digital security and protection providers.
- Capture service scope, accessibility, eligibility, and known limitations.
- Develop a confidential directory for internal project use.
- Document at least two anonymized case summaries illustrating how CSAs navigate urgent digital security incidents.
- Apply strict confidentiality, informed consent, and do-no-harm principles.

4. Approach and Methodology

The consultant will propose a detailed methodology, including sampling criteria, participatory approaches, and data collection tools. The full study design will be presented in an inception report. The methodology must:

- Apply feminist and intersectional analysis throughout.
- Ensure meaningful participation of marginalized and rights-holder–led groups.
- Address digital and physical civic space as interconnected.
- Incorporate innovative and accessible approaches suitable for low-resource and high-risk environments.
- Focus on mapping and case-based learning.
- Limitations and mitigation measures must be clearly stated. Confidentiality, informed consent, and risk mitigation are mandatory.
- The consultant will sign a non-disclosure agreement (NDA).

5. Deliverables

The consultancy will produce the following key deliverables, primarily for the 18 CoA member organizations participating in the assessment and ToT program:

A. Digital Security Assessment

- Mapping report of participating CSAs and CSOs, including breakdown by organization type (rights-holder led, media, human rights defenders, etc.), gender, and location
- Digital security needs assessment tools.

- Assessment report with findings, analysis, and actionable recommendations for capacity strengthening, advocacy, and learning.

B. Curriculum and Training Materials Development

- Draft and final context-specific digital security curriculum, adapted to local needs and global best practices.
- Localized versions of training content where necessary.
- Pilot testing and validation report on the curriculum's effectiveness.
- Online publication of curriculum and training materials on publicly accessible platforms, with active links shared.

C. Training of Trainers (ToT) Program

- Design and deliver multi-day ToT sessions for 18 CoA Members (agenda, participant list, and feedback summary).
- Support CoA Members to conduct at least one on-site/community-based training.
- Collect feedback, lessons learned and refine curriculum content.
- Provide finalized training materials online for broader access.
- Submit ToT Training Report.

D. Digital Security Service Mapping and Case-Based Learning

- Confidential protection service directory (annexed to the Draft and Final Consultancy Reports; restricted circulation)
- Analytical note summarizing the protection landscape, access constraints, risks, and gaps
- Minimum of two anonymized case summaries illustrating CSA experiences in navigating urgent digital and/or physical protection needs

Note: The directory is for internal project use only and will not be publicly disseminated.

E. Integration & Final Consultancy Report

- Consolidated report integrating assessment findings, curriculum & Training materials, ToT program & report, protection service directory, and anonymized case documentation.
- Includes lessons learned and recommendations for ongoing capacity strengthening, training sustainability, and resource dissemination.

6. Timeline

The consultancy shall be conducted over a period of four (4) months, commencing on the agreed start date, and is expected to take place between April and July 2026

Proposed Deliverables Timeline

Deliverables	Description	Deadline
Inception Report	Outlines methodology, assessment framework, and work plan	Week 4

Needs Assessment Report	Findings from the digital security assessment, including risks, gaps, and recommendations	Week 8
Curriculum & Training Materials	Digital Security curriculum and training materials	Week 12
Digital Protection Service Directory	Digital Protection Service Directory	Week 12
Integration & Final Report Draft	Consolidates report integrating assessment findings, curriculum & Training materials, ToT program & report, protection service directory, and anonymized case documentation	Week 16
Final Consultancy Report	Comprehensive report final	Week 18

7. Consultant Requirements

Applications are welcomed by both legally registered individual consultants and organizations or consortia. based in Palestine (West Bank, Gaza, and East Jerusalem). In the case of organizations or consortia, the required qualifications and experience must be demonstrated by the proposed team, with the Team Leader/Lead Consultant meeting the minimum academic and professional experience requirements.

- Proven experience in digital security assessments, with at least 5 years in cybersecurity consulting.
- Proven expertise in digital security and cybersecurity for civil society.
- Experience conducting needs assessments and research on digital threats.
- Knowledge of feminist and intersectional methodologies in digital security.
- Experience in curriculum development and training, particularly in digital security.
- Understanding of the political and social contexts affecting CSAs, including marginalized persons, women, and indigenous communities.
- Strong facilitation skills and experience delivering Training of Trainers (ToT).
- Expertise in risk assessment methodologies and vulnerability management.
- Strong technical knowledge of network security, cloud computing, data protection, and encryption technologies.
- Experience researching civic space issues around human rights, media, digital security, enabling the environment for civil society, and strong understanding of current trends and developments in the target country are required.

8. Submission and Evaluation of Proposals

8.1 Submission Requirements

Consultants who meet the requirements should submit an expression of interest of not more than 15 pages (less annexes), which should include the following:

- A detailed proposed study methodology, including a draft work plan with a timeline outlining when each deliverable will be submitted.
- A financial proposal containing a proposed daily fee in EUR, inclusive of taxes, including applicable local taxes, with the understanding that the consultant/company is responsible for any local tax obligations.
- Updated summaries of the CV/Portfolio of the consultant and supporting team members were applicable, that spells out qualifications and experience with special emphasis on civil society programming. In detail, provide a list of staff that will be involved in the study - from the lead consultant, data analyst, etc to field researchers - with a summary of their relevant experience and proposed role in the study. A full CV for each team member should be provided as an annex.
- Three contactable references should be included in the CVs/Portfolio.
- Two previous similar or related reports written by the consultant (as annex)
- Signed and dated Annex A Form.

8.2 Submission Guidelines

- Please submit the CV/Portfolio proposal clearly outlining the proposed way of working as per the above guidelines, work plan and budget (in EUR) by Thursday, March 5th, 2026. All documents must be submitted together in one package.
- Submissions should be sent via email to menaprocurement@hivos.org with the subject line: "Digital Security Assessment, Training of Trainers (ToT), Curriculum Development, and Digital Security Service Mapping".
- The proposal will be reviewed on a rolling basis. Hivos reserves the right to close the call early should a suitable applicant be identified.
- Only shortlisted applicants will be contacted.
- Late or incomplete submissions will not be considered.

8.3 Evaluation and Selection Criteria

Applications will be evaluated using a weighted scoring approach:

Quality of Proposed Assessment Design and Methodology	40%
Quality of the Team	20%
Quality of the Consultant's Previous Work	20%
Budget, Compliance, and References	20%

Annex A: Declaration of Conflict of Interests
Tenderer's Declaration Form (to be completed, signed, and submitted)

We the undersigned accept in full and without restriction the conditions governing this call as the sole basis of this competition, whatever its own conditions of sale may be, which we hereby waive.

We have examined carefully, understood and comply with all conditions, instructions, forms, provisions and specifications contained in this call. We are aware that failure to make submissions containing all the information and documentation expressly required, within the deadline specified, may lead to the rejection of the submission at Hivos discretion.

We hold no reservation in regard to the call dossier; and are aware that any reservation may result in the rejection of the submission by Hivos.

We are not aware of any corruption practice in relation to this competition. Should such a situation arise, we shall immediately inform Hivos in writing.

We declare that we are not affected by any potential conflict of interest, and that we and any of our staff have no particular link with other parties involved in this competition. Should such a situation arise during performance of the contract, we shall immediately inform Hivos in writing.

We accept Hivos standard terms of payment, which are 10 working days from date of receipt of invoice or later after acceptance of service in question by Hivos.

*Company name and address:*_____

*Company Representative name:*_____

*Title of Representative in the Company:*_____

*Representative's signature:*_____

*Place, date:*_____

Annex B: Proposed Final Consultancy Report Structure

1. Executive Summary
    - Brief overview of the assignment, context, objectives, and methodology.
    - Key findings and recommendations from all components.
    - Summary of results against the Results Framework indicators.
    - Limit 2–3 pages for high-level stakeholders.
2. Introduction / Background
    - Context of shrinking civic space in Palestine and the role of digital security.
    - Overview of the Connect, Defend, Act! project.
    - Purpose and objectives of the consultancy.
    - Scope and deliverables.
3. Methodology
    - Approach for assessment, curriculum development, ToT, and service mapping.
    - Sampling and participating selection criteria.
    - Participatory and inclusive methods (feminist and intersectional lens).
    - Data collection, confidentiality, and risk mitigation measures.
    - Limitations and mitigation strategies.
4. Digital Security Needs Assessment
    - Mapping of participating CSAs and CSOs (demographics, type, rights-holder groups).
    - Analysis of digital security risks, vulnerabilities, and threats.
    - Identified skills gaps and differentiated protection needs.
    - Key findings and actionable recommendations.
    - Annex: Needs assessment tools (questionnaires, interview guides).
5. Curriculum Development
    - Overview of curriculum design principles, modular structure, and learning objectives.
    - Summary of pilot testing with CoA members and feedback received.
    - Final curriculum and training materials (manuals, slides, exercises, case studies).
    - Accessibility and inclusive adaptations.
    - Annex: Draft and final curriculum and training materials.
6. Training of Trainers (ToT) Program
    - Description of ToT sessions delivered (agenda, duration, participants).
    - Trainers' skill development, facilitation, and adult learning methodologies applied.
    - Implementation of at least one on-site/community training by CoA members.
    - Lessons learned, feedback, and curriculum refinements.
    - Annex: ToT Training Report, feedback summaries.
7. Digital Security Service Mapping & Case-Based Learning

- Mapping of local digital security, technical, legal, and psychosocial support providers.
- Analytical note: accessibility, gaps, limitations.
- Two anonymized case summaries illustrating CSA experiences navigating digital threats, in which covering the following:
- Case Title / Identifier
- Context / Background
- Incident Description
- Digital Security Threats & Risks Identified
- Actions Taken by the CSA
- Referral & Support Services Utilized
- Outcome & Lessons Learned
- Confidential directory (for internal circulation).
- Annex: Case summaries and service directory (restricted).

8. Integration of Findings
    - Synthesis of assessment, curriculum, ToT, and service mapping insights.
    - Analysis against project outcomes and indicators.
    - Recommendations for ongoing capacity strengthening, training sustainability, and resource dissemination.
9. Conclusion and Recommendations
    - High-level conclusions on CSA digital security resilience.
    - Recommendations for future capacity building and advocacy interventions.
    - Suggested improvements for curriculum, ToT, and service mapping initiatives.
10. Annexes
    - Needs assessment tools.
    - ToT training agenda and participant lists.
    - Service mapping directory (confidential).
    - Case summaries.
    - Any additional supporting documentation