Norwegian Afghanistan Committee

Call for Tender:

Managed Security Operations and Microsoft 365 Data Protection Services

October/November 2025

Contents

1. Introduction and background information

The Norwegian Afghanistan Committee (NAC) is a membership-based solidarity organization (non-profit) with its headquarters in Oslo and field offices in Afghanistan. NAC conducts long-term development, humanitarian, advocacy, and communications work spanning sectors such as health, disability, agriculture, education, and community development.

NAC employs approximately 1,539 people (subject to change with humanitarian contracts). Of these, 389 staff use Microsoft 365 applications to provide services in Afghanistan, under Microsoft 365 E5 licenses (cloud productivity, collaboration, security tools: Teams, SharePoint, OneDrive, Exchange Online). In Norway, nine staff also use Microsoft 365 and operate in the same online workspace as the Afghanistan users.

Over the past three years, NAC has completed a significant digital transformation, merging separate tenant environments into one, strengthening internal ICT capacity, moving finance operations online, and planning similar moves for HR, procurement, and inventory systems.

To further strengthen NAC's cyber resilience, maintain predictable costs, and ensure data protection, NAC now invites qualified vendors to propose **managed security operations (SOC 2.0)** services and a **Microsoft 365 backup / data protection** solution. The selected vendor will be critical in safeguarding NAC's operations, especially in a challenging operational environment such as Afghanistan.

2. Current Situation

- NAC currently outsources security, backup, and general IT support to an external provider, but intends to bring core IT operations in-house, outsourcing only security and backup functions.
- There are 389 M365 users in Afghanistan and 9 in Norway.
- The ICT-department comprises 15 employees in Afghanistan, as well as one IT/digitalisation lead in Oslo.
- All users have Windows PCs in the offices, except for two users who use Macs. In Afghanistan, all users use their laptops in the office, and some are allowed to take their laptops home and use Teams and Outlook on their mobile devices.
- NAC has an internal learning platform that gives training on the use of Teams, and we are currently preparing for more courses on cybersecurity, ICT security, and other relevant topics. In addition, we have invested in external competency building for our colleagues who work in the ICT-department, and our staff travel to our various offices to conduct hybrid in-person and online trainings.
- The existing security and backup systems are provided by the external provider.
- The M365 tenant, architecture, and configurations were set up by the current provider.
- During the transition, NAC expects the vendor to propose a handover plan ensuring knowledge transfer and minimising service disruption. The vendor should proactively manage transition risks and propose mitigation measures.

3. Scope of Work

The scope of this tender primarily covers security operations and Microsoft 365 data protection services. Consultation may also be provided upon request from IT employees. The tender does not cover general IT support, hardware procurement, or application development.

3.1 Managed Security Operations Center (SOC 2.0)

The vendor must provide 24/7/365 security monitoring, detection, alerting, and response services covering the entire IT infrastructure (Cloud, and hybrid components). Required capabilities include:

- Threat intelligence integration (SIEM, SOAR)
- Incident detection, response, containment, investigation, remediation, and closure with defined SLAs
- Vulnerability scanning, prioritization, and management
- Log collection, normalization, retention, and analytics aligned with compliance requirements
- Adherence to ISO 27001, GDPR, SOC 2.0, and alignment with recognized frameworks (e.g., NIST CSF, CIS Controls)
- Proactive threat hunting, forensic investigations, and root-cause analysis
- Quarterly security reports with findings and actionable recommendations
- A joint incident management framework with NAC ICT team: clear escalation path, communication flows, roles and responsibilities

3.2 Microsoft 365 Backup and Data Protection

The vendor must deliver a robust backup and recovery solution for all Microsoft 365 workloads, including:

- Daily automated backups of Exchange Online, SharePoint Online, OneDrive, Teams, and Dataverse. We do not have data in Dataverse currently available, but we may develop our applications and use Dataverse as database in future.
- Granular recovery options: single file, mailbox, SharePoint library, Teams chat, site-level restore
- Configurable retention policies (up to 7 years or more as required by compliance)
- Data residency: backup data must be stored within Norway or the EU/EEA
- Immutable storage / write-once-read-many (WORM) or equivalent ransomware-resistant architecture
- Support for legal hold, eDiscovery, litigation holds, and compliance-driven retention
- Quarterly restoration drills (test restores), with reports on success/failures and lessons learned
- Notification and remediation of backup failures, data corruption, or anomalies

3.3 Advisory / Consultation Services

On-demand consulting support to NAC ICT is also required, covering:

- Architectural reviews, security assessments, compliance audit
- It's not mandatory, but if the vendor provides Microsoft licences, they may include in the proposal the cost for E5 and E3 licences, and Adobe creative cloud, based on Afghanistan's pricing and non-profit organisation rates.
- Support for major upgrades, migrations, and change management
- Incident response planning, tabletop exercises, and training
- Advice may be included in the base contract or separately priced (vendors should clearly state which)

4. Vendor qualifications and requirements

The vendor must meet the following minimum criteria:

4.1 Experience and track record

- At least five years of experience providing security and backup services for Microsoft 365 or equivalent environments.
- Provide references or case studies of similar implementations.

4.2 Certifications and standards

- ISO 27001 certified, or an equivalent recognised standard (proof required)
- Demonstrated compliance with GDPR/EU Data Protection Laws
- Familiarity with cybersecurity standards/frameworks (e.g., NIST, CIS)

4.3 Support and response

- 24/7 multilingual support (in both Norwegian and English)
- Defined escalation paths
- Guaranteed response time of within 15 minutes for critical incidents (please specify any variant in pricing)

4.4 Business continuity and reliability

- Vendor must maintain its own business continuity and disaster recovery capabilities
- Offer SLA guarantees, with minimum uptime of 99.9%.

4.5 Data residency and legal compliance

- All backup data must reside within the EU/EEA or Norway
- Vendors must comply with GDPR, Norwegian data protection law, NAC internal policies.
- Subcontractors, if used, must also comply and be disclosed.

4.6 Financial stability, transparency, and risk disclosure

- Demonstrate financial stability (e.g., audited accounts, financial statements)
- Disclose any history of security incidents or data breaches in the past five years, including remediation and lessons learned.

5. Service Level Agreements (SLA)

Service	Metric/objective	Target/maximum
SOC Alert Response	Time to confirm and acknowledge critical security alert	≤ 15 minutes
Incident resolution (critical)	Time to full resolution (containment, remediation, closure)	≤ 4 hours
Backup Recovery Time Objective (RPO)	Max time to recover affected Microsoft 365 workloads	≤ 4hours
Backup recovery point objective (RPO)	Maximum tolerable data age in event of failure	≤ 24 hours
Uptime (availability)	Annual service uptime for security / backup solutions	≥ 99.9%

Vendors should propose penalties, credits, or remedies if SLAs are not met.

6. Intellectual property, ownership, and audit rights

- NAC shall own all custom configurations, scripts, documentation, and deliverables produced in relation to this contract.
- The vendor shall clearly list any pre-existing or third-party materials or software; NAC will be granted a perpetual, royalty-free usage license for those.

- NAC and its donors (or their auditors) retain the right to audit all financial, technical, and operational records relevant to this contract for up to **five years post-completion.**
- All information exchanged shall be treated as confidential and may only be disclosed with NAC's written consent.

7. Procurement, ethical, and legal compliance

7.1 Procurement and ethical standards

- This procurement is donor-funded. The selected vendor must comply with Norad's procurement and ethical standards.
- Vendors shall adhere to transparency, accountability, competition, equal treatment, and non-discrimination principles.
- NAC reserves the right to require the vendor to sign a **Supplier Declaration (Ethics and Compliance)** confirming no involvement in corruption, fraud, money laundering, child labour, forced labour, discrimination, or human rights abuses.

7.2 Conflict of interest

- Vendors must disclose any actual or potential conflict of interest with NAC, its staff, or any party connected to this procurement.
- Failure to disclose may lead to disqualification or contract termination.

7.3 Eligibility and exclusion criteria

NAC may exclude a vendor if:

- The vendor (or its affiliated entities) have been convicted of fraud, corruption, or similar offenses in the last five years.
- The vendor is insolvent, bankrupt, or under administration.
- The vendor has failed to perform contractual obligations in prior donor-funded contracts.

7.4 Termination and amendment

- NAC reserves the right to terminate the contract in the event of material breach, non-compliance with ethical provisions, conflicts of interest, or security violations.
- All amendments or variations must be in writing and mutually agreed.

7.5 Audit, ownership and documentation

- NAC and its donors (or auditors) may audit the vendor's records, accounts, and operations.
- NAC reserves the right to access all documentation and evidence of compliance throughout and after the contract execution.

8. Evaluation criteria and scoring

The evaluation will be based on a **weighted scoring system.** NAC reserves the right to conduct due diligence and reference checks before award.

Evaluation criterion	Weight (%)
Technical capability and compliance (security + backup)	40%
Cost and value for money	30%
Past experience and references	15%

Project management, transition, and risk mitigation approach	10%
Experienced in working with humanitarian organisations	5%

NAC may request oral presentations or clarifications and reserves the right to reject any or all proposals.

9. Proposal submission requirements

Vendors must submit the following components:

1. **Company profile**
   - Overview (history, structure, size, service lines)
   - Relevant certifications and accreditations
2. **Technical proposal**
   - Detailed strategy for SOC 2.0 and Microsoft 365 backup
   - Architecture diagrams, tools, processes, and integrations
   - Security, monitoring, forensic, and recovery workflows
3. **Implementation and transition plan**
   - A comprehensive plan for onboarding, Migration, Integration and handover
   - Strategies to minimize knowledge loss during handover, supported by fallback procedures and risk management protocols
4. **SLA and escalation matrix**
   - Full SLA definitions, roles, response times, escalation paths
5. **Pricing proposal**
   - Transparent breakdown: Setup costs, subscription fees, per-user fees, optional services
   - Confirmation that all compliance, training, documentation, audits are included
6. **References and case studies**
   - Minimum three clients with similar services delivered, including contact info
7. **Financial statements and stability**
   - Audited financial statements for the past 2-3 years (or equivalent)
8. **Security incident history disclosure**
   - Details of any breaches or major incidents over the past five years, including remediation actions
9. **Declarations**
   - Conflicts of interest disclosure
   - Ethical compliance/supplier declaration
10. **Optional addenda**
    - Any additional value propositions, optional services or similar

Format and submission
Submit one (1) signed PDF version of the technical proposal and one (1) signed PDF version of the financial proposal (in separate files). All documents must be in English. NAC may request soft copies in editable form after evaluation. Proposals must be submitted via silje.olsson@nacaf.org by **20 November 2025, 17:00 Oslo time.** Late submissions will not be accepted.

10. Timelines

Milestone	Date
Tender publication	20 October 2025
Deadline for written questions	31 October 2025
Answers to questions shared	04 November 2025
Proposal submission deadline	20 November 2025
Evaluation period	20 – 30 November 2025
Vendor notification of award	01 December 2025
Contract signing	05 December 2025
Project start	10 December 2025

11. Contact for clarification

All queries regarding this tender must be submitted in writing to:
Silje Olssøn, Head of Oslo Office
silje.olsson@nacaf.org
by 31 October 2025.

NAC will share answers to all received questions (anonymized) by 04 November 2025.