INTEGRATED AIR AND MISSILE DEFENCE
CENTRE OF EXCELLENCE

IFB FINCON 22-02

"IT Services - Technical Compliance Report"

PART III

SPECIAL PROVISIONS & TECHNICAL SPECIFICATIONS
(STATEMENT OF WORK)

March 2022

THIS PAGE IS INTENTIONALLY LEFT BLANK

PART III

NATO UNCLASSIFIED
RELEASABLE FOR INTERNET TRANSMISSION

TABLE OF CONTENTS

THIS PAGE IS INTENTIONALLY LEFT BLANK

1. **Statement of Work (SOW)**

1.1 The current Statement of Work (SOW) covers the special provisions and technical specifications that shall be covered by the Contractor for the services requested.

2. **General Specifications**

2.1 The requested services should target and focus on the compliance with the minimum Requirements of Cyber Defence of the NATO Related Unclassified Networks (as described below).

2.2 Technical compliance report is requested for the Minimum Requirements of Cyber Defence for the protection of NATO Related Networks. Technical solutions are required and analytical documentation of compliance per subject shall be provided by the Contractor (as described below).

3. **Technical Specifications - Deliverables**

3.1 Requested services to be provided:

3.1.1 Microsoft 365 Business Premium on-premises deployment;

3.1.2 Windows Auto Pilot deployment (also for future use).

3.1.3 DNS Servers setup for migration from Top Host provider to Microsoft 365 datacenters.

3.1.4 Shared Mailboxes Setup on Exchange Server Online.

3.1.5 Old Mailboxes Migration from Linux to Microsoft Exchange.

3.1.6 Local Network Survey - Devices Setup - Deployment.

3.1.7 SharePoint Online Deployment (Site & Libraries created - Users Permissions).

3.1.8 Multi Factor Authenticator setup and deployment + SSPR (self-service password reset).

3.1.9 Microsoft 365 Groups deployment (Group collaboration - File Sharing - Shared Calendars).

3.1.10 Removable Media management policy.

3.2 Deliverable: Technical compliance report with the respective suggested technical solutions for the following subjects - items:

3.2.1 Firewalls to limit the network traffic to a defined and managed set of network ports.

3.2.2 Email gateways which are capable of scanning incoming emails for malicious code, with regularly updated signatures for detecting such code.

3.2.3 Software solutions deployed at the endpoint systems to control the installation, spread and execution of malicious code, for which the signatures for detection are updated at least once per day (e.g. antivirus products).

3.2.4 Measures (dedicated software or through configuration) to limit and control the introduction of external devices to the endpoints and ensure that only authorised devices can be connected.

3.2.5 Firewalls which can apply filtering at the application layer for a more fine-grained control of incoming and outgoing network traffic.

3.2.6 Measures to limit and control the introduction of devices to the network infrastructure (e.g. by implementing certificate based network access control)

3.2.7 Measures to implement web content filtering (e.g. reverse web proxies).

3.2.8 Measures to mitigate Denial of Service attacks.

3.2.9 Host Intrusion Prevention software deployed on every endpoint to provide behaviour based detection of malicious activity to better mitigate against known, as well as emerging (including zero-day) attacks.

3.2.10 Measures to protect against unauthorised disclosure of Personally Identifiable Information (PII) (e.g. mandatory compliance with the General Data Protection Regulation (GDPR) where applicable).

3.2.11 Measures to periodically scan the network, including the endpoints, in order to detect existence of classified to identify and mitigate spillages and cross-domain information violations.

3.2.12 Data loss prevention mechanisms to be deployed on such mechanisms can be very effective in endpoints and/or network boundaries.

3.2.13 Identification and authentication mechanisms to ensure only authorised users have access to the CIS and the information contained within.

3.2.14 Measures to manage the lifecycle of user, system and application accounts, their creation, use and deletion, applying the least required privilege principle.

3.2.15 Advanced identification and authentication mechanisms that pro-

vide a higher level of assurance of ensuring only authorised users have access (i.e. implementing multi-factor authentication).

3.2.16 Measures to maintain secure configurations for all hardware and software, by applying security patches in a timely manner.

3.2.17 Measures to restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.

3.2.18 Established change management processes to track, review, approve/disapprove, and audit changes to information systems.

3.2.19 Tools to monitor and log activity within the network.

3.2.20 Tools to monitor and log activity on the endpoints, to include servers.

3.2.21 Intrusion Detection devices that are regularly updated with signatures to detect malicious activity in the networks.

3.2.22 Specialized network appliances that allow 'full packet capture' functionality, triggered by suspicious network activity, to enable detailed post-incident investigation within an acceptable time delay.

3.2.23 Specialized software deployed on endpoints, to be triggered on demand, allowing for capturing forensic images of storage and memory devices.

3.2.24 A set of contingency plans to be applied in case of incidents.

3.2.25 Measures and the ability to restore CIS to fully operational status, restoring system and information integrity, and service availability.

3.2.26 Pre-agreed and documented prioritization of which systems are most critical for urgent recovery.

3.2.27 Pre-defined lists of critical systems that should not be impacted, as well as critical data that should not be lost when executing recovery procedures.

3.2.28 Education and awareness programmes that leverage the use of digital as well as printed media to ensure end-users are made aware of the general threats and vulnerabilities applicable to the CIS they use, in order that they acknowledge their responsibility to maintain the protective security measures in place and adopt 'cyber hygiene' in their way of working.

3.2.29 Means for the personnel responsible for detecting incidents, to access all security related logs spread throughout the network.

3.2.30 Specialized software and / or appliances (e.g. a Security Incident

and Event Management tool and its sub-components for log aggregation) to automatically collect all relevant logs in a central repository to facilitate analysis.

3.2.31 A capability (person or a team) with the required training to conduct post-incident analysis activities, leveraging the information collected from the networks, to conduct root cause analysis and identify user mistakes, unpatched vulnerabilities or potential gaps in preventive mechanisms that may have led to the incident.

3.2.32 A capability (person or a team) and the required tools to evaluate security information collected through long periods, to enable correlation and trends analysis, to be complemented with threat information in order to achieve cyberspace situational awareness.

3.3 Deliverables/services to be rendered: Implementation of technical solutions with analytical documentation per subject for the following items:

3.3.1 Firewalls to limit the network traffic to a defined and managed set of network ports.

3.3.2 Email gateways which are capable of scanning incoming emails for malicious code, with regularly updated signatures for detecting such code.

3.3.3 Software solutions deployed at the endpoint systems to control the installation, spread and execution of malicious code, for which the signatures for detection are updated at least once per day (e.g. antivirus products).

3.3.4 Measures (dedicated software or through configuration) to limit and control the introduction of external devices to the endpoints and ensure that only authorised devices can be connected.

3.3.5 Measures to protect against unauthorised disclosure of Personally Identifiable Information (PII) (e.g. mandatory compliance with the General Data Protection Regulation (GDPR) where applicable).

3.3.6 Measures to periodically scan the network, including the endpoints, in order to detect existence of classified to identify and mitigate spillages and cross-domain information violations.

3.3.7 Identification and authentication mechanisms to ensure only authorised users have access to the CIS and the information contained within.

3.3.8 Measures to manage the lifecycle of user, system and application accounts, their creation, use and deletion, applying the least required privilege principle.

3.3.9 Measures to maintain secure configurations for all hardware and software, by applying security patches in a timely manner.

3.3.10 Measures to restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.

3.3.11 Tools to monitor and log activity within the network.

3.3.12 Tools to monitor and log activity on the endpoints, to include servers.

3.3.13 Intrusion Detection devices that are regularly updated with signatures to detect malicious activity in the networks.

3.3.14 A set of contingency plans to be applied in case of incidents.

3.3.15 Measures and the ability to restore CIS to fully operational status, restoring system and information integrity, and service availability.

3.3.16 Education and awareness programmes that leverage the use of digital as well as printed media to ensure end-users are made aware of the general threats and vulnerabilities applicable to the CIS they use, in order that they acknowledge their responsibility to maintain the protective security measures in place and adopt 'cyber hygiene' in their way of working.

3.3.17 Means for the personnel responsible for detecting incidents, to access all security related logs spread throughout the network.

3.4 All the required documentation (report, documents for compliance, etc.) shall be written - submitted in English and should be signed by the Contractor.

3.5 Any details required for the above requirements will be provided by the IAMD COE competent official (Support BH) in written.

4. **Guarantee**

4.1 No special guarantee is required by the Contractor.

5. **Delivery - Shipping costs**

5.1 All services requested and deliverables shall be completed, provided and delivered to the IAMD COE by 15 April 2022.

5.2 The bidder’s offer - price proposal shall include any costs for the computers installation and configuration/control, as well as the respective training services.

6. **Contractor’s Standards**

6.1 The Contractor shall be a Microsoft Partner. A written certification or the relevant link by the Microsoft web-site (to be written on the notes of the "Compliance' Statement - Bidder's Proposal") must be provided to prove this status.

6.2 The Contractor must be able to offer any services required, on situ, at the IAMD CoE’s facilities on daily basis upon request of the Centre’s competent official (Support BH). The bidder’s offer - price proposal shall include any such costs.