Cybersecurity Annex: UTM

1. Introduction

This annex outlines a focused set of technical and procedural cybersecurity requirements prioritized for the development, delivery, and lifecycle of the UTM application. These core topics are mapped to the ISO/IEC 27002:2022 standard.

Proposals will be evaluated on how comprehensively they address these security objectives. The finalized technical implementations of these objectives will be jointly refined and formally agreed upon during the project's design phase.

2. Requirements

a) Identity and Access Management

- 8.2 Privileged access rights
- 8.3 Information access restriction
- 8.5 Secure authentication

The application is expected to enforce the principle of least privilege. Users should only be granted the minimum access rights necessary to perform their specific roles via Role-Based Access Control (RBAC). Access to administrative functions, management interfaces, and sensitive data should be protected by secure Multi-Factor Authentication (MFA). *The supplier is requested to detail their proposed authentication and authorization mechanisms.*

b) System- and network security

- 8.7 Protection against malware
- 8.21 Security of network services
- 8.23 Web filtering
- 8.25 Secure development life cycle
- 8.27 Secure systems architecture and engineering principles
- 8.28 Secure coding
- 8.29 Security testing in development and acceptance
- 8.31 Separation of development, test and production environments
- 8.32 Change management

'Security by Design' should be a foundational engineering principle. The web application is expected to comply with the OWASP ASVS (v5.0) Level 2 or equivalent. Furthermore, the application aims for a 100% score on internet.nl (with any deviations formally justified) and should comply with the 'Comply or Explain' policy of the Dutch Forum Standaardisatie where applicable (including HTTPS, DMARC, RPKI, and security.txt). *The supplier is requested to explain how they perform secure development and their standard procedure for prioritizing and remediating security findings.*

c) Safe configurations

- 8.24 Use of cryptography

Encryption should be applied to all sensitive data in-transit. The supplier should utilize modern cryptographic algorithms and protocols and continue to comply with the latest cryptography guidelines published by the Dutch National Cyber Security Centre (NCSC-NL). *The supplier is requested to provide a plan demonstrating how the application guarantees continued compliance with cryptography guidelines.*

d) Management of information security events

- 5.24 Information security incident management planning and preparation
- 8.8 Management of technical vulnerabilities
- 8.15 Logging
- 8.16 Monitoring activities

The application should generate comprehensive logging of security events and critical actions (audit trails) at the OS, application, and network level. *The supplier is requested to describe their approach to proactively monitoring the application and its third-party components for technical vulnerabilities, and how security incident management is organized.*

e) Continuity

- 8.6 Capacity management
- 8.13 Information backup
- 8.14 Redundancy of information processing facilities

The system should be designed to guarantee agreed-upon availability requirements and include adequate mitigation against Denial-of-Service attacks. *The supplier is requested to provide an outline of their proposed backup and disaster recovery plans including target RPO and RTO.*

f) Information security

- 8.12 Data leakage prevention

Appropriate technical and organizational measures should be taken to minimize the risk of unauthorized disclosure or leakage of sensitive data.