

Date: 01/09/2026

TENDER SPECIFICATIONS

- TECHNICAL - part 2

Procedure No 2026_05

PREVENTIVE MAINTENANCE, SERVICING SAFETY & SECURITY SYSTEMS

Type of procedure: **Negotiated procedure for low-value contracts**

Estimated Value: **60.000,00€**

Award method: **best value for money**

Type of contract: **framework contract**

Contracting authority: **European School of Mol (ESMOL)**

TABLE OF CONTENTS

1. GENERAL TERMS AND CONDITIONS.....	3
2. COVERED FACILITIES & LOCATIONS.....	3
3. TECHNICAL DESCRIPTION	3
3.1. Fire Alarm System.....	3
3.3. Burglar Alarm / Intrusion Detection	4
3.4. CCTV / Video Surveillance	4
4. MAINTENANCE REQUIREMENTS & TEST PROTOCOL...	5
4.1. Annual Preventive Maintenance.....	5
4.2. Corrective maintenance. Repairs and Spare Parts Allocation.	6
5. SERVICE LEVEL AGREEMENT (SLA) & EMERGENCY SUPPORT.....	6
5.1. Response Times	6
5.2. Dedicated Support Hotline (24h/7 days).....	6
6. OCCUPATIONAL SAFETY OF THE STAFF	7
7. DOCUMENTATION AND DELIVERABLES.....	7
8. ACCEPTANCE, TESTING AND DELIVERY	7
9. WARRANTIES	7

1. GENERAL TERMS AND CONDITIONS.

The contractor will be responsible for design, delivery, installation, configuration, commissioning, integration and handover. And also, it shall provide all necessary labour, materials, equipment, testing fluids, and expertise required to perform the annual preventive maintenance, inspection, and 24/7 emergency support.

All components must be CE marked and comply with the relevant European/IEC/EN standards listed per system.

All network connections must be secure (authentication, encryption in transit and at rest where relevant) and comply with common cybersecurity guidelines (e.g. ETSI EN 303 645 for IoT devices where applicable).

Integration: Systems must provide open, standardized interfaces (e.g., ONVIF/API/PSIM interfaces) so that integration with VMS, access control, fire control panel, and building management systems is possible.

Privacy & legislation: all camera applications and processing must comply with GDPR and Belgian camera legislation / guidelines from the Data Protection Authority. The tenderer is responsible for providing a privacy impact analysis (DPIA) and the registration file if applicable.

2. COVERED FACILITIES & LOCATIONS

The contract encompasses all structures across the campus site, which includes, but is not limited to, the following buildings:

- Administration Building
- Secondary School Building
- Secondary Gym / Sports Hall
- Canteen / Kitchen facility
- Domus Building
- Primary School Building
- Kindergarten / Nursery School
- Childcare / After-school Facility
- Swimming Pool
- Security/Guard house

3. TECHNICAL DESCRIPTION

3.1. Fire Alarm System.

Functional requirements: Full coverage according to risk assessment: detection in technical rooms, escape routes, places with a risk of fire, server rooms, elevator rooms, etc.

- Type of detectors: smoke (optical), thermal, multisensor (where relevant).

- Zoning and logical map in fire alarm panel with the possibility of segmentation and prioritization.

Integration outputs: notifications to BMS, fire alarm panel (PZI), and remote notifications to 24/7 control room (if contractually required).

Technical requirements & standards: Equipment and components, and inspections must strictly comply with the European standards EN 54 (parts 2, 4, 11, and 21 where applicable) and Belgian national standards NBN S21-100 parts 1 & 2. with EN 54 series (product standards and system regulations).

And also Certificates and FPC (factory production control) declarations require declaration.

Test, commissioning & maintenance:

- Factory acceptance test (FAT) and site acceptance test (SAT) including scenario tests.
- Annual preventive maintenance + 24/7 breakdown service within 2 days.
- Delivery of as-built drawings, programs, configuration backups and logs.

3.3. Burglar Alarm / Intrusion Detection

Functional

Coverage according to risk analysis: perimeteric (windows/doors), volumetric (PIR/radar), glass break detectors, magnetic contacts, passive and active sensors.

Degree of security: choose and specify the required grade (EN 50131 grades 1–4) based on risk.

Notification routes: local siren, notification to control room, push/SMS to contact.

Technical & Standards

- Materials and installation in line with EN 50131 series; Grade indication (e.g. Grade 2 for commercial applications, Grade 3/4 for high-risk locations).
- The service provider must hold valid certifications under national/regional regulatory frameworks for security contractors (INCERT certificate category or equivalent European quality standard).

Testing & maintenance

- Factory & site tests; detection-loop tests and false alarm analysis.
- Periodic maintenance contracts and breakdown service (SLA).

3.4. CCTV / Video Surveillance

Functional

- Coverage plan: overview maps with camera locations, type of camera, viewing direction, minimum ID distance (e.g. identification of a person at X meters).
- Required image quality: minimum resolution (e.g. 1080p / 4MP / 4K depending on application), frame rate (min. 12–25 fps real-time), compression (H.265 or better) and day/night capabilities (IR/low-light).
- Recording duration and retention: adjustable per zone (e.g. 30 days normal, 90 days for critical zones) and automatic overwriting policy.
- Motion/analytics: motion detection, perimeter breaches, tampering detection; analytics must comply with Privacy by Design (minimal processing).

- Exchanges: NVR(s) and/or VMS with central management console; high availability (RAID and redundant recording options).
- Tru-view/forensic requirements (ability to export forensic-grade clips with checksum).

Technical & Standards

- Systems must comply with IEC/EN 62676 (video surveillance standards) and cameras must be ONVIF compliant (prefer modern profiles: Profile T/G/M depending on requirements) for interoperability.
- Image quality tests and camera performance measurement methods can follow IEC 62676-5 (or recent version).

Privacy & legal requirements

- Camera use must comply with GDPR and Belgian camera legislation; pictograms/notification, DPIA, registration/notification to police if required and minimal access to images.
- Require proof of compliance (DPIA documents and process description).

Storage & network

- Minimum IOPS/throughput specification for ingestion servers; Cryptographic protection of stored images (encryption at rest).
- WAN/remote access: Multi-factor authentication for remote management, logging of all access, and export.
- Export and chain of custody: export formats, checksum methods and chain-of-custody procedures.

4. MAINTENANCE REQUIREMENTS & TEST PROTOCOL

4.1. Annual Preventive Maintenance.

The contractor must execute a rigorous yearly service schedule.

Given the complexity of the campus, a minimum layout of one full working week with at least two qualified technicians on-site is required to guarantee meticulous testing.

The yearly protocol shall incorporate:

- Control Panel Inspections: Thorough diagnostics of all main control equipment, monitoring boards, interfaces, and power systems.
- Battery & Back-up Power Testing: Annual verification of emergency standby batteries (e.g., 12V lead-acid cells) under load conditions to evaluate primary power failure drop-outs. Preventive replacement of depleted batteries must be factored into standard upkeep workflows.
- 100% Sensor Testing: Every single reachable field component—including optical/multicriteria detectors and manual call points—must be activated manually using

appropriate specialized testing fluids, gases, or physical tools to ensure fully operational response paths.

- Component Upkeep: Physical cleaning and dust extraction of field devices using non-damaging aerosol cleaners.
- Transmission Check: Testing of transmission pathways to central stations, simulating alarm types (Intrusion, Fire, Tamper/Sabotage, Power Dropout).

4.2. Corrective maintenance. Repairs and Spare Parts Allocation.

These are repairs or corrections that are requested on demand, in the case of requests from the European School.

The bidder may charge a percentage for purchase and delivery commission, which will be determined according to their bid.

Component replacements discovered during maintenance will be addressed outside the fixed fee on a time-and-materials basis, subject to a dedicated quotation review and formal client approval prior to execution

The work will be invoiced based on the hourly rate of the attending maintenance technician, whose rate will also be set in the contract based on the bidder's financial proposal.

5. SERVICE LEVEL AGREEMENT (SLA) & EMERGENCY SUPPORT

5.1. Response Times

- Normal faults or standard technical queries shall be processed during standard regional business hours, but not exceedingly more than 72 hours.
- Critical Fault Response: In extreme cases or critical system down times, the physical intervention window on campus must not exceed 4 hours from the formal notification of the emergency call.

<u>Those bidders who commit to a reduction in this time in their financial offer will receive a better score.</u>

5.2. Dedicated Support Hotline (24h/7 days)

The contractor must provide an unmitigated 24-hour, 7-day-a-week dedicated emergency service phone line staffed by a specialized technician dispatch center.

6. OCCUPATIONAL SAFETY OF THE STAFF

To ensure adherence to European safety principles and local laws, the contractor must follow rigorous occupational safety norms, demonstrated by certifications such as VCA Safety Certification or equivalent European safety standards.

7. DOCUMENTATION AND DELIVERABLES

Following every maintenance cycle or emergency intervention, the service provider must submit comprehensive documentation to the school's Safety & Security Officer:

1. Maintenance Certificates: Formal regulatory compliance statements confirming system status as required by regional fire and safety laws.
2. Detailed Intervention Reports: A granular record highlighting all test results, identified errors, tracking modifications, and recommendations for system adjustments.
3. As-Built Update Support: If any on-site network topology configuration changes are implemented, the provider must assist in maintaining accurate site layout charts.

8. ACCEPTANCE, TESTING AND DELIVERY

- FAT (factory acceptance) and SAT (site acceptance) with test cases: alarm-flow tests, failover tests, integration tests (fire->camera pop-up, intrusion->record trigger), and privacy-compliance check.
- Documentation: as-built drawings, cable diagrams, IP address list, certificates, FAT/SAT reports, warranties and maintenance contracts.
- **Training: operator and system administration (min. 2 days for each).**

9. WARRANTIES

- Minimum warranty:
 - 2 years on hardware
 - 1 year on installation.

- Those bidders who commit to an expansion in this time in their financial offer will receive a better score.