

Date: 01/09/2026

CAHIER DES CHARGES

- Technique — partie 2

Procédure no 2026_05

MAINTENANCE préventive, SERVICING SAFETY & SYSTÈME DE SYSTÈME DE SÉCURITÉ

Type de procédure: **Procédure négociée pour les marchés de faible valeur**

Valeur estimée: **60 000,00 EUR**

Méthode d'attribution: **le meilleur rapport qualité-prix**

Type de contrat: **contrat-cadre**

Pouvoir adjudicateur: **École européenne de Mol (ESMOL)**

SOMMAIRE

1. CONDITIONS GÉNÉRALES.	3
2. LES FACILITÉS ET LOCATIONS COUVERTES.....	3
3. DESCRIPTION TECHNIQUE	3
3.1. Système d'armement.....	3
3.3. Burglar Alarm/Détection d'irrusion.....	4
3.4. CCTV/Surveillance vidéo.....	4
4. EXIGENCES EN MATIÈRE DE MAINTENANCE ET TEST PROTOCOL.....	5
4.1. Maintien annuel de la prévention.....	5
4.2. Maintenance corrective. Allocation des Réparateurs et des Spares Parts.....	6
5. ACCORD DE NIVEAU DE NIVEAU (SLA) & SOUTIEN DE L'EMERGENCE	6
5.1. Délai de réponse	6
5.2. Ligne d'assistance dédiée (24 heures sur 7 jours).....	7
6. SÉCURITÉ AU TRAVAIL DU PERSONNEL.....	7
7. DOCUMENTATION ET LIVRABLES	7
8. RÉCEPTION, TEST ET LIVRAISON.....	7
9. GARANTIES.....	8

1. CONDITIONS GÉNÉRALES.

Le contractant sera responsable de la conception, de la livraison, de l'installation, de la configuration, de la mise en service, de l'intégration et du transfert. Elle fournit également toute la main-d'œuvre, le matériel, l'équipement, les fluides d'essai et l'expertise nécessaires pour effectuer la maintenance préventive annuelle, l'inspection et l'aide d'urgence 24 heures sur 24 et 7 jours sur 7.

Tous les composants doivent être marqués par un marquage CE et respecter les normes européennes/CEI/EN pertinentes énumérées par système.

Toutes les connexions réseau doivent être sécurisées (authentification, chiffrement en transit et au repos, le cas échéant) et être conformes aux lignes directrices communes en matière de cybersécurité (par exemple, ETSI EN 303645 pour les dispositifs de l'IdO, le cas échéant).

Intégration: Les systèmes doivent fournir des interfaces ouvertes et normalisées (par exemple, interfaces ONVIF/API/PSIM) afin que l'intégration avec VMS, le contrôle d'accès, les panneaux de contrôle d'incendie et les systèmes de gestion des bâtiments soient possibles.

Respect de la vie privée et législation: toutes les applications et tous les traitements de caméras doivent être conformes au RGPD et à la législation/lignes directrices belges sur les caméras de l'autorité chargée de la protection des données. Le soumissionnaire est chargé de fournir une analyse d'impact sur la vie privée (AIPD) et le dossier d'enregistrement, le cas échéant.

2. Les FACILITÉS et LOCATIONS couvertes

Le contrat englobe l'ensemble des structures du site du campus qui comprend, sans s'y limiter, les bâtiments suivants:

- Le bâtiment de l'Administration
- Bâtiment de l'école secondaire
- Jeu secondaire Gym/Sports Hall
- Facilité de cantine/Kitchen
- Bâtiment Domus
- Bâtiment de l'école primaire
- Jardin d'enfants/École maternelle
- Garde d'enfants/facilité scolaire après
- Pool de natation
- Sécurité/Chambre du chantier

3. DESCRIPTION TECHNIQUE

3.1. Système d'armement.

Exigences fonctionnelles: Couverture complète selon l'évaluation des risques: détection dans les salles techniques, les itinéraires d'évitement, les lieux présentant un risque d'incendie, les salles de serveurs, les salles d'élévator, etc.

- Type de détecteurs: fumée (optique), thermique, multisenseur (le cas échéant).
- Zoning et carte logique dans le panel d'alarme incendie avec possibilité de segmentation et de hiérarchisation des priorités.

Résultats de l'intégration: notifications au BMS, groupe d'alarme incendie (PZI) et notifications à distance dans la salle de contrôle 24 heures sur 24 et 7 jours sur 7 (si cela est requis contractuellement).

Exigences et normes techniques: Les équipements et composants, et les inspections doivent respecter strictement les normes européennes EN 54 (parties 2, 4, 11 et 21 le cas échéant) et les normes nationales belges NBN S21-100 parties 1 & 2. à la série EN 54 (normes relatives aux produits et réglementation des systèmes).

De même, les certificats et déclarations FPC (contrôle de la production d'usines) doivent être déclarés.

Test, mise en service & maintenance:

- Test d'acceptation de l'usine (FAT) et test de réception site (SAT), y compris tests de scénario.
- Entretien préventif annuel + répartition 24/7 dans les 2 jours.
- Livraison de tirages, programmes, sauvegardes de configuration et journaux de configuration.

3.3. Burglar Alarm/Détection d'irrusion

Fonctionnel

Couverture selon l'analyse des risques: périmétrique (fenêtres/portes), voltricule (PIR/radar), détecteurs de ruptures de verre, contacts magnétiques, capteurs passifs et actifs.

Degré de sécurité: choisir et préciser l'échelon requis (EN 50131 échelons 1 à 4) en fonction du risque.

Voies de notification: siren locaux, notification de la salle de contrôle, push/SMS à contacter.

Normes techniques et normes

- Matériaux et installation selon la série EN 50131; Indication de l'échelon (par ex., échelon 2 pour les demandes commerciales, échelon 3/4 pour les emplacements à haut risque).
- Le prestataire de services doit détenir des certifications valides au titre des cadres réglementaires nationaux/régionaux pour les contractants de sécurité (catégorie de certificats INCERT ou norme de qualité européenne équivalente).

Tests et maintenance

- Tests d'usine et de site; tests de détection en boucle et analyse des fausses alertes.
- Contrats de maintenance périodique et ventilation de service (SLA).

3.4. CCTV/Surveillance vidéo

Fonctionnel

- Plan de couverture: vue d'ensemble des cartes avec les lieux de caméra, le type de caméra, le sens de la visualisation, la distance minimale d'identification (par exemple, identification d'une personne à Xmètres).
- Qualité requise de l'image: résolution minimale (p. ex. 1080p/4MP/4K selon les modalités d'application), taux-cadre (min. 12-25 fps en temps réel), compression (H.265 ou meilleure) et capacités de jour/mature (IR/low-light).
- Durée d'enregistrement et conservation: ajustable par zone (ex. 30 jours normal, 90 jours pour les zones critiques) et politique de surécriture automatique.
- Motion/analytique: détection des mouvements, dépassements de périmètres, détection de manipulations; L'analyse doit respecter la protection de la vie privée dès la conception (traitement minimal).
- Échanges: NVR et/ou VMS avec console de gestion centrale; disponibilité élevée (options d'enregistrement RAID et redondantes).
- Exigences en matière d'examen/forensic (possibilité d'exporter des clips de grade criminalistique avec contrôle).

Normes techniques et normes

- Les systèmes doivent être conformes à la norme IEC/EN 62676 (normes de surveillance vidéo) et les caméras conformes à l'ONVIF (profils modernes: Profil T/G/M en fonction des exigences) pour l'interopérabilité.
- Les tests de qualité de l'image et les méthodes de mesure des performances des caméras peuvent suivre la norme CEI 62676-5 (ou version récente).

Respect de la vie privée et exigences juridiques

- L'utilisation de caméras doit être conforme au RGPD et à la législation belge sur les caméras; pictogrammes/notifications, AIPD, enregistrement/notification à la police si nécessaire et accès minimal aux images.
- Exiger une preuve de conformité (documents de l'DPIA et description du processus).

Stockage et réseau

- Spécification minimale d'IOPS/d'entrées pour les serveurs en gestion; Protection cryptographique des images stockées (cryptage au repos).
- WAN/accès à distance: Authentification multifactorielle pour la gestion à distance, l'enregistrement de tous les accès et l'exportation.
- Exportation et chaîne de conservation: formats d'exportation, méthodes de contrôle et procédures de chaîne de conservation.

4. Exigences en matière de maintenance et TEST PROTOCOL

4.1. Maintien annuel de la prévention.

Le contractant doit exécuter un calendrier de service annuel rigoureux.

Compte tenu de la complexité du campus, une configuration minimale d'une semaine de travail complète avec au moins deux techniciens qualifiés sur place est nécessaire pour garantir des tests méticuleux.

Le protocole annuel doit inclure:

- Inspections partielles de contrôle: Diagnostics approfondis de tous les principaux équipements de contrôle, conseils de surveillance, interfaces et systèmes électriques.
- Equipement d'électricité de batterie et de back-up: Vérification annuelle des batteries de veille d'urgence (par exemple, cellules de plomb 12V) dans des conditions de charge afin d'évaluer les pannes de courant primaires. Le remplacement préventif des batteries épuisées doit être pris en compte dans les flux de travail d'entretien standard.
- 100 % Sensor Testing: Chaque élément joignable sur le champ — y compris les détecteurs optiques/multicritères et les points d'appel manuels — doit être activé manuellement à l'aide de fluides d'essais, de gaz ou d'outils physiques spécialisés appropriés afin de garantir des voies de réponse pleinement opérationnelles.
- Mise à jour des composants: Nettoyage physique et extraction de poussières à l'aide d'installations d'aérosol non diamants.
- Contrôle de transmission: Test des voies de transmission vers les stations centrales, simulant des types d'alarme (Intrusion, Fire, Tamper/Sabotage, Power Dropout).

4.2. Maintenance corrective. Allocation des Réparateurs et des Spares Parts.

Il s'agit de réparations ou de corrections qui sont demandées sur demande, en cas de demande de l'École européenne.

Le soumissionnaire peut facturer un pourcentage de commissions d'achat et de livraison, qui sera déterminé en fonction de son offre.

Les remplacements de composants découverts lors de la maintenance seront traités en dehors de la redevance fixe sur la base du temps et de l'importance, sous réserve d'un examen de cotation spécifique et de l'approbation formelle du client avant l'exécution.

Les travaux seront facturés en fonction du taux horaire du technicien de maintenance assistant, dont le taux sera également fixé dans le contrat sur proposition financière du soumissionnaire.

5. Accord DE NIVEAU DE NIVEAU (SLA) & SOUTIEN DE L'EMERGENCE

5.1. Délai de réponse

- Les dysfonctionnements normaux ou les requêtes techniques standard seront traités pendant les heures d'ouverture régionales standard, mais pas au-delà de 72 heures.
- Réponse à une catastrophe critique: Dans les cas extrêmes ou les heures critiques du système, la fenêtre d'intervention physique sur le campus ne doit pas dépasser 4 heures à compter de la notification formelle de l'appel d'urgence.

Les soumissionnaires qui s'engagent à réduire cette fois leur offre financière bénéficieront d'une meilleure note.

5.2. Ligne d'assistance dédiée (24 heures sur 7 jours)

Le contractant doit fournir une ligne de téléphone de service d'urgence d'urgence d'une durée de 24 heures non atténuée, d'une durée de 7 jours à semaine, composée de membres d'un centre d'appel technicien spécialisé.

6. SÉCURITÉ AU TRAVAIL DU PERSONNEL

Pour garantir le respect des principes européens de sécurité et de la législation locale, le contractant doit respecter des normes rigoureuses de sécurité au travail, attestées par des certifications telles que la certification de sécurité VCA ou des normes européennes de sécurité équivalentes.

7. DOCUMENTATION ET LIVRABLES

Après chaque cycle de maintenance ou intervention d'urgence, le prestataire doit soumettre une documentation complète au responsable Prévention et sécurité de l'école:

1. Certificats de maintenance: Déclarations formelles de conformité réglementaire confirmant le statut du système tel que requis par les législations régionales en matière d'incendie et de sécurité.
2. Rapports d'intervention détaillés: Enregistrement granulaire mettant en évidence tous les résultats des tests, les erreurs identifiées, le suivi des modifications et les recommandations relatives aux ajustements du système.
3. Appui à la mise à jour en cours: Si des modifications de la configuration du réseau sur site sont mises en œuvre, le fournisseur doit aider à maintenir des graphiques précis de mise en forme des sites.

8. RÉCEPTION, TEST ET LIVRAISON

- Graisses (acceptation des usines) et SAT (acceptation sur place) avec cas de test: tests d'alerte-flux, tests de secours, tests d'intégration (fire->camera pop-up, intrusion->déclencheur), et contrôle de la conformité au respect de la vie privée.
- Documentation: prélèvements asconstruits, diagrammes à câbles, liste IP adresse, certificats, rapports FAT/SAT, garanties et contrats de maintenance.
- **Formation: opérateur et gestion système (moins 2 jours pour chacun).**

9. GARANTIES

- Garantie minimale:
 - 2 ans sur le matériel informatique
 - 1 an après l'installation.

- | |
|---|
| <ul style="list-style-type: none">• <u>Les soumissionnaires qui s'engagent à étendre cette offre financière bénéficieront d'une meilleure note.</u> |
|---|