MY TRUST PARTNER
CISO | SOC | Resilience

PROGRAMME DE FORMATION

Sécurité numérique, bonnes pratiques et protection des données pour les établissements sanitaires, sociaux et médico-sociaux

1. Identification de la formation

Élément	Description
Intitulé	Cybersécurité et bonnes pratiques numériques en établissement sanitaire, social et médico-social
Référence interne	CYB-ESMS-2026
Durée	1 jour (7 heures) — format conforme aux durées du marché
Public	Agents administratifs, personnels soignants, éducatifs, cadres intermédiaires, services supports, équipes SI
Pré-requis	Aucun prérequis technique — formation accessible à tous les professionnels, techniciens ou non
Modalités	Présentiel en intra dans les établissements du Grand Est (conformément à l'Art. 6 du CCTP)
Formateur	Professionnel de la cybersécurité en exercice (vCISO / auditeur), certifié ISO 27001, SecNumAcad
Accessibilité	Supports adaptables, salle PMR, alternance oral/visuel, possibilité de traduction FALC

2. Objectifs pédagogiques opérationnels

À l'issue de la formation, les participants seront capables de :

1. **Identifier les principales menaces cyber** qui ciblent les établissements sanitaires / sociaux / médico-sociaux.
2. **Adopter les bonnes pratiques de sécurité numérique** au quotidien (messagerie, mots de passe, patientèle, documents sensibles).
3. **Protéger les données sensibles**, notamment médicales et sociales (aligné RGPD & recommandations ANSSI).
4. **Reconnaître un email frauduleux** (phishing) et réagir efficacement.
5. **Réagir face à une cyberattaque** : premiers réflexes, escalade interne, procédure.
6. **Utiliser les outils numériques de l'établissement en toute sécurité** (poste de travail, applications métier, dossiers patients, téléphonie).

3. Compétences visées

- **C1. Comprendre les risques cyber** propres au secteur sanitaire et médico-social.
- **C2. Appliquer les bonnes pratiques de cybersécurité au quotidien.**
- **C3. Protéger les données personnelles et sensibles conformément au RGPD.**
- **C4. Détecter les tentatives de fraude et d'ingénierie sociale.**
- **C5. Connaître les bons réflexes en cas d'incident numérique ou d'attaque.**

4. Programme détaillé de la journée

Séquence 1 — Comprendre les menaces (1h30)

Contenu :

- Panorama des cyberattaques en France dans le secteur médical et social (attaques récentes contre EHPAD, CH, IME, CCAS, services sociaux)
- Démonstration : comment une attaque peut commencer
- Impact concret pour les établissements : service bloqué, perte de données, indisponibilité dossier patient
- Les données sensibles mais pas que : dossiers patients, données sociales, données RH, données financières

Méthodes :

- Vidéos pédagogiques
- Cas réels issus d'incidents ANSSI et cybermalveillance.gouv.fr
- Échanges interactifs

Évaluation :

- Quiz

Séquence 2 — Messagerie, phishing et attaques courantes (2h)

Contenu :

- Détection des emails frauduleux : signaux d'alerte
- Exercices : reconnaissance d'emails piégés
- Tentatives de fraude financières (« fraude au président » dans les associations/collectivités)
- Manipulation de liens malveillants et pièces jointes

- Sécurisation de la messagerie professionnelle

Méthodes :

- Ateliers et exercices pratiques
- Analyse d'exemples réels
- Mise en situation avec exercices de tri (vrai/faux)

Évaluation :

- Score individuel « niveau anti-phishing »

Séquence 3 — Bonnes pratiques au quotidien (1h30)

Contenu :

- Mots de passe et gestion des accès
- Confidentialité au poste de travail (accueil, bureaux partagés, service de soins)
- Sécurisation des documents sensibles (soins, éducatif, administratif)
- Hygiène informatique : mises à jour, verrouillage de session, sauvegardes locales
- Dossier patient / dossier usager : ce que dit la loi et ce qu'il faut absolument éviter

Méthodes :

- Démonstrations par le formateur
- Cas concrets issus d'établissements du Grand Est

Évaluation :

- QCM

Séquence 4 — Sécurité des données et RGPD appliqué (1h)

Contenu :

- Données personnelles & données sensibles : ce que dit le RGPD
- Règles incontournables dans les ESMS
- Confidentialité en service : contenus écrits, transmissions, mobilité
- Comment éviter une violation de données ?

Méthodes :

- Mini-atelier : "classer une donnée"
- Support synthétique remis aux participants

Évaluation :

- Évaluation orale collective

Séquence 5 — Les bons réflexes en cas d'incident (1h)

Contenu :

- Que faire si :
  - l'ordinateur est bloqué
  - un message suspect apparaît
  - une pièce jointe a été ouverte
  - un dossier a disparu
- Les mauvaises pratiques à bannir (ne jamais redémarrer ! ne jamais supprimer !)
- Comment remonter l'incident, à qui et quand ?
- Procédures internes et communication à chaud

Méthodes :

- Jeu de rôle "incident en service"
- Analyse d'un scénario ransomware

Évaluation :

- Retour collectif + grille d'auto-évaluation finale

5. Modalités d'évaluation

Conforme aux exigences du RC/CCTP :

Type	Objectif	Modalité
Diagnostic	Mesurer le niveau de départ	Quiz
Formative	Vérifier la compréhension	Exercices, tri d'emails, mises en situation
Sommative	Valider les acquis	QCM final
Satisfaction	Mesurer la qualité perçue	Questionnaire à chaud / à froid

6. Livrables remis aux participants

- Guide « Bonnes pratiques cybersécurité – secteur médico-social »
- Fiche réflexe « Incident / suspicion de cyberattaque : que faire ? »
- Modèles d'affiches de sensibilisation (salle de pause, accueil, bureaux)
- Supports de formation (PDF)
- Mini-checklist d'autocontrôle pour les équipes

7. Accessibilité & adaptations

- Supports en lecture simplifiée (FALC) sur demande
- Vidéos sous-titrées
- Documents avec police contrastée 16+
- Prise en compte handicaps visuels, auditifs, cognitifs

8. Suivi et traçabilité

- Feuilles de présence via notre outil
- Attestation individuelle de fin de formation
- Évaluations à chaud et à froid
- Rapport final transmis à l'établissement :
    - niveau atteint
    - recommandations opérationnelles
    - axes d'amélioration