



ASSOCIATION CGPC

Politique de sensibilisation à la sécurité informatique

Bonnes pratiques et règles applicables à l'ensemble des collaborateurs — Édition
2026



Pourquoi cette politique ?

1 association sur 2

a subi une tentative d'attaque au cours des 12 derniers mois.

9 incidents sur 10

ont pour origine une erreur humaine, non une faille technique.

Données adhérents

cotisations, coordonnées et pièces justificatives sont des données sensibles.



Périmètre et engagements



Qui est concerné ?

Salariés, intervenants, administrateurs, stagiaires et prestataires disposant d'un accès aux outils de l'association.



Quels équipements ?

Postes fixes et portables, téléphones, tablettes, supports amovibles et matériels personnels utilisés en télétravail.



Quels services ?

Messagerie, espaces de stockage partagés, CRM, sites internet et réseaux sociaux.



Quelles données ?

Données personnelles des adhérents, données financières, documents internes et identifiants de connexion.

Règle n°1 : des mots de passe robustes



À FAIRE

- 12 caractères minimum, mélangeant majuscules, chiffres et symboles
- Une phrase de passe facile à retenir (ex. : « 3Chats!DansLeJardin »)
- Un mot de passe différent pour chaque service
- L'authentification à deux facteurs activée sur la messagerie
- Le gestionnaire de mots de passe fourni par l'association



À PROSCRIRE

- Noter ses identifiants sur un post-it ou un fichier Excel
- Réutiliser son mot de passe personnel sur les outils CGPC
- Partager un compte entre plusieurs collaborateurs
- Utiliser un prénom, une date de naissance ou « CGPC2026 »
- Enregistrer ses accès sur un poste public ou partagé

Règle n°2 : reconnaître un e-mail frauduleux



Le phishing reste le premier vecteur d'attaque. Cinq signaux doivent déclencher votre vigilance :

1

Expéditeur inconnu ou
adresse légèrement
modifiée

2

Urgence, menace ou
promesse inhabituelle

3

Fautes d'orthographe et
mise en forme
approximative

4

Pièce jointe ou lien
inattendu

5

Demande de virement ou
d'identifiants

En cas de doute : ne cliquez pas, ne répondez pas. Transférez le message à renaudduval@cgpc.fr puis supprimez-le.

Règle n°3 : sécuriser son poste et sa mobilité



Verrouiller systématiquement

Windows + L dès que vous quittez votre bureau, même pour quelques minutes.



Mettre à jour sans délai

Acceptez les mises à jour système et antivirus proposées : elles corrigent des failles connues.



Bureau et écran propres

Aucun document confidentiel laissé sur le bureau, à l'imprimante ou visible en open space.



Télétravail et Wi-Fi public

Évitez les réseaux ouverts pour accéder aux données adhérents.



Un geste simple, répété chaque jour, protège mieux qu'un outil complexe.

Règle n°4 : protéger les données des adhérents

01

Collecter

Uniquement les données nécessaires à la gestion de l'adhésion.

02

Stocker

Sur les espaces partagés de l'association, jamais sur un disque local ou une clé USB personnelle.

03

Partager

Par lien sécurisé et à durée limitée, jamais en pièce jointe non protégée.

04

Conserver

3 ans après la fin de l'adhésion, puis suppression définitive.

Toute fuite ou perte de données personnelles doit être signalée au référent RGPD dans les 24 heures : l'association dispose de 72 heures pour notifier la CNIL.

Que faire en cas d'incident ?

1

Isoler

Déconnectez le poste du réseau et du Wi-Fi. N'éteignez pas la machine.

2

Signaler

Prévenez immédiatement le référent informatique : renaudduval@cgpc.fr

3

Documenter

Notez l'heure, les actions effectuées et conservez le message ou la capture d'écran.

4

Ne pas payer

Aucune rançon n'est versée. Aucun contact direct avec l'attaquant.

Signaler une erreur n'est jamais sanctionné : le silence, lui, aggrave toujours l'incident.

Le dispositif de sensibilisation CGPC

Trimestriel

Une session de 45 minutes pour tous les collaborateurs

2 / an

Campagnes de faux phishing avec retour pédagogique

100 %

Des nouveaux arrivants formés dès la première semaine

1 charte

Signée par chaque utilisateur à la remise de ses accès

Pilotage : le référent informatique présente chaque semestre au bureau un bilan des incidents, du taux de participation aux formations et des actions correctives engagées.

VOTRE ENGAGEMENT

La sécurité de l'association commence par vous

Je protège mes accès et active la double authentification.

Je vérifie avant de cliquer, je signale en cas de doute.

Je traite les données des adhérents comme les miennes.

Contact : renaudduval@cgpc.fr • Référent RGPD : renaudduval@cgpc.fr