# Charte Informatique des Associations Cultuelles (église)

## Préambule

L’usage des outils informatiques et des données numériques au sein de notre association nécessite des règles claires afin de garantir un fonctionnement sécurisé et conforme aux bonnes pratiques de cybersécurité. Cette charte vise à encadrer l’utilisation des équipements et des services numériques mis à disposition des membres, bénévoles et administrateurs de l’association. Chaque utilisateur doit adopter une attitude responsable pour préserver l’intégrité et la confidentialité des informations.

## 1. Champ d’Application

Cette charte s’applique à toute personne utilisant les outils informatiques et numériques de l’association, qu’il s’agisse d’ordinateurs, de messageries électroniques, de bases de données, de logiciels, du site internet ou encore des supports de stockage en ligne (cloud, serveurs distants, clés USB). Elle concerne aussi bien les salariés, bénévoles, prestataires et partenaires ayant accès à ces outils.

## 2. Principes Généraux

- L’utilisation des outils informatiques doit être conforme aux valeurs et aux missions de l’association.
- Chaque utilisateur est responsable des équipements et des accès qui lui sont confiés.
- Toute tentative d’accès non autorisé à des informations sensibles ou tout usage détourné des ressources de l’association est strictement interdit.
- Le partage d’informations doit être effectué de manière sécurisée et dans le respect de la confidentialité.

Exemple : Un bénévole ne doit pas transmettre la liste des adhérents par e-mail sans l’autorisation du bureau. De même, il est interdit de stocker ces informations sur un ordinateur personnel non sécurisé.

## 3. Gestion des Accès et des Identifiants

- Chaque utilisateur doit posséder un identifiant unique et un mot de passe personnel.
- Les mots de passe doivent comporter au minimum 12 caractères avec un mélange de lettres, chiffres et caractères spéciaux.
- Il est strictement interdit de partager son mot de passe avec un tiers.
- Les mots de passe doivent être modifiés régulièrement (tous les 6 mois minimum).
- En cas d’oubli ou de compromission d’un mot de passe, il doit être réinitialisé immédiatement par un responsable informatique.

Exemple : Ne jamais inscrire son mot de passe sur un post-it collé à l’écran ou le noter dans un fichier non sécurisé.

## 4. Utilisation d’Internet et de la Messagerie

- L’accès à Internet via les équipements de l’association doit être réservé à des usages liés aux activités de l’association.
- Les sites web visités doivent être en accord avec l’éthique et les objectifs de l’association.
- Ne jamais cliquer sur des liens douteux dans des e-mails non sollicités (hameçonnage/phishing).
- Il est interdit d’utiliser la messagerie de l’association à des fins personnelles ou pour des activités commerciales extérieures.

Exemple : Un membre qui reçoit un e-mail suspect lui demandant de confirmer un mot de passe ou un paiement ne doit pas y répondre et doit en informer un responsable.

## 5. Protection des Données Personnelles

- Les données des membres, bénévoles et partenaires de l’association sont confidentielles.
- Seules les personnes autorisées peuvent accéder aux informations sensibles (listes d’adhérents, données financières, etc.).
- Les fichiers contenant des données personnelles doivent être protégés par un mot de passe ou stockés sur des plateformes sécurisées.
- La durée de conservation des données doit être limitée au strict nécessaire.

Exemple : Si l’association n’a plus besoin d’une liste d’anciens adhérents, ces données doivent être supprimées de manière sécurisée.

## 6. Sécurité des Équipements

- Les ordinateurs, tablettes et autres supports numériques doivent être protégés par un antivirus multicouche et mis à jour régulièrement.
- Il est interdit d’installer des logiciels non autorisés sur les équipements de l’association.
- Ne pas brancher de périphériques de stockage (clés USB, disques durs externes) sans vérification préalable.

Exemple : Un bénévole ne doit pas utiliser son ordinateur personnel pour gérer les comptes de l’association sans sécurisation adéquate.

## 7. Sauvegarde des Données

- Une sauvegarde régulière des données sensibles doit être effectuée (au moins une fois par mois).
- Les sauvegardes doivent être stockées sur un support sécurisé (cloud chiffré, disque dur externe protégé).
- Il est recommandé de conserver plusieurs copies des sauvegardes en cas de sinistre.

## 8. Réactions en Cas d’Incident

- Tout utilisateur suspectant une anomalie (virus, vol d’informations, comportement suspect) doit en informer immédiatement le responsable de l’association.
- En cas de suspicion de piratage, l’équipement concerné doit être déconnecté du réseau et une analyse de sécurité doit être effectuée.
- Ne jamais tenter de dissimuler un incident de sécurité.

Exemple : Si un bénévole ouvre accidentellement une pièce jointe infectée, il doit immédiatement informer le responsable avant que le virus ne se propage.

## 9. Sanctions en Cas de Non-Respect

Tout non-respect des règles édictées par cette charte peut entraîner des sanctions décidées par le bureau de l’association :
- Avertissement écrit de l’association en cas de faute grave (ex. : fuite intentionnelle de données).
- Restriction temporaire ou définitive d’accès aux outils numériques.
- Exclusion de l’association en cas de faute grave (ex. : fuite intentionnelle de données).

## 10. Adoption et Engagement

Chaque membre de l’association s’engage à respecter cette charte et à appliquer les bonnes pratiques décrites.

Date : \_\_ / \_\_ / \_\_\_\_
Signature du membre : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_