**1. Identification de l’Incident**

- Toute activité suspecte (accès non autorisé, fichier inconnu, e-mail suspect) doit être signalée immédiatement.

- Noter l’heure et les circonstances de la découverte de l’incident.

 **2. Confinement**

- Déconnecter les équipements affectés du réseau pour éviter la propagation.

- Changer immédiatement les mots de passe des comptes compromis.

**3. Notification et Signalement**

- Informer immédiatement le responsable informatique ou le référent cybersécurité de l’association.

- Si des données personnelles sont concernées, notifier la CNIL sous 72h.

**4. Analyse et Correction**

- Identifier la source de l’attaque (phishing, virus, intrusion).

- Restaurer les données à partir d’une sauvegarde propre si nécessaire.

**5. Prévention et Amélioration**

- Mettre à jour les mots de passe et vérifier les autorisations d’accès.

- Sensibiliser les membres pour éviter de nouvelles attaques.

- Conserver un rapport d’incident pour améliorer la cybersécurité.

[Nom du Responsable]

[Contact]

[Date d’Application]