

# Fiche des rôles en cas d'incident cyber

Pour la direction, l'informatique et les équipes métier : attribuer les responsabilités, communiquer de façon sûre et consigner les décisions. Complétez les contacts et pouvoirs de décision avant utilisation. En cas de soupçon urgent, appelez immédiatement le contact informatique convenu, sans attendre un dossier complet.

Organisation : \_\_\_\_\_ Responsable : \_\_\_\_\_  
Date de revue : \_\_\_\_\_ Validation : \_\_\_\_\_

| Rôle et tâche                                                                                 | Nom et suppléant | Contact et secours |
|-----------------------------------------------------------------------------------------------|------------------|--------------------|
| Pilotage de l'incident<br>Coordonner priorités, actions et points de situation                | _____<br>_____   | _____<br>_____     |
| Informatique ou prestataire<br>Évaluer le périmètre, piloter l'endiguement et la reprise      | _____<br>_____   | _____<br>_____     |
| Direction et responsable métier<br>Évaluer l'impact opérationnel et autoriser les décisions   | _____<br>_____   | _____<br>_____     |
| Communication<br>Diffuser les informations internes et externes validées                      | _____<br>_____   | _____<br>_____     |
| Protection des données et juridique<br>Évaluer notifications obligatoires et recours externes | _____<br>_____   | _____<br>_____     |

## Communication et pouvoir de décision

Canal de secours autorisé si la messagerie est compromise : \_\_\_\_\_

Qui peut isoler ou arrêter les systèmes : \_\_\_\_\_

Qui valide la reprise et les messages externes : \_\_\_\_\_

Prochain point de situation et responsable : \_\_\_\_\_

Dans une petite équipe, les rôles peuvent être cumulés, mais chaque responsabilité et suppléance doit rester explicite. Convenez des contacts hors horaires normaux. Vérifiez les canaux susceptibles d'être compromis avant de les utiliser.

# Premier signalement interne

Pour la personne qui signale et le pilote de l'incident. Consignez les observations, identifiez les hypothèses et les inconnues. Ce signalement interne ne remplace aucune notification externe obligatoire.

| Champ                                                                   | Informations |
|-------------------------------------------------------------------------|--------------|
| Référence et auteur du signalement<br>Contact sûr pour rappel           | <hr/> <hr/>  |
| Date et heure de découverte<br>Préciser le fuseau horaire               | <hr/> <hr/>  |
| Observation et source<br>Ce qui est réellement établi                   | <hr/> <hr/>  |
| Services touchés et impact métier<br>Ce qui ne fonctionne plus          | <hr/> <hr/>  |
| Actions déjà effectuées<br>Qui a fait quoi et quand                     | <hr/> <hr/>  |
| Contacts informés et transmission<br>Qui prend en charge le signalement | <hr/> <hr/>  |
| Questions ouvertes et prochain point<br>Responsable et heure            | <hr/> <hr/>  |

## Transmettre les informations en sécurité

Ne consignez ni mots de passe, ni codes MFA, ni données personnelles inutiles. Référez les preuves par identifiants internes et emplacements autorisés. Faites préserver les originaux et journaux par du personnel qualifié ; convenez des durées de conservation et droits d'accès. N'ouvrez pas de fichier suspect pour l'examiner et ne le transférez pas par une voie non autorisée.

# Journal d'incident et transmission

Pour la personne chargée du journal. Chaque entrée comporte date, heure et fuseau. Distinguez observations, décisions et résultats. Dupliquez les pages si nécessaire et consignez toute correction dans une nouvelle entrée.

Référence du dossier : \_\_\_\_\_ Tenue du journal : \_\_\_\_\_

| Heure et source         | Observation ou décision | Action et responsable   | Résultat ou référence de preuve |
|-------------------------|-------------------------|-------------------------|---------------------------------|
| _____<br>_____<br>_____ | _____<br>_____<br>_____ | _____<br>_____<br>_____ | _____<br>_____<br>_____         |
| _____<br>_____<br>_____ | _____<br>_____<br>_____ | _____<br>_____<br>_____ | _____<br>_____<br>_____         |
| _____<br>_____<br>_____ | _____<br>_____<br>_____ | _____<br>_____<br>_____ | _____<br>_____<br>_____         |

## Transmission et reprise

Périmètre actuel et risques résiduels : \_\_\_\_\_  
Actions ouvertes, responsables et échéances : \_\_\_\_\_  
Transmission de / à / heure : \_\_\_\_\_  
Reprise validée par / heure / conditions : \_\_\_\_\_  
Tests fonctionnels, surveillance et prochaine revue : \_\_\_\_\_

## Assurer le suivi

Amélioration à mettre en œuvre : \_\_\_\_\_  
Responsable / échéance / efficacité vérifiée le : \_\_\_\_\_

## Utilisation et guides complémentaires

Modèles originaux de Paragamix GmbH. Utilisation interne, adaptation et partage avec les clients gratuits ; un lien vers la source est apprécié. À faire vérifier par les responsables avant utilisation. Aide organisationnelle, pas manuel technique d'intervention. Protégez les dossiers remplis.

[NIST SP 800-61 rév. 3 \(anglais\)](#) | [Version actuelle et outils](#)