Plan de Communication de Crise FAKESEC

version 1.0

Table des matières

Introduction et Gouvernance

Objectifs du PCC

Le principal objectif du plan de communication de crise est d'organiser de la manière la plus efficace possible une communication rapide, précise, et coordonnée pendant et après un incident de cybersécurité.

L'objectif secondaire est de protéger l'image et la réputation de l'entreprise et maintenir la confiance des parties prenantes, ainsi que de respecter les obligations légales (ex : CNIL).

Portée du PCC

Le présent Plan de Communication de Crise s'applique dès lors qu'un incident de cybersécurité entraîne l'activation de la cellule de crise.

Il englobe la gestion de la parole interne et externe pour tout événement affectant les infrastructures propres à FAKESEC (Google Workspace, Réseau local) ou celles gérées par ses prestataires critiques (Scaleway).

Il s'étend de la première détection de l'anomalie en passant par la clôture de la crise (Désactivation) jusqu'à la phase de retour d'expérience et d'amélioration.

Termes définitions et abréviations

Termes et définitions :

- **PCC :** *Un plan de communication de crise (**PCC)** est un dispositif formalisé qui décrit comment l'entreprise doit communiquer avant, pendant et après un incident cyber majeur.*
- **Répudiation :** *La répudiation désigne la possibilité pour une personne de contester une action qu'elle a réellement effectuée, en l'absence de preuves techniques fiables permettant de l'attribuer.*
- **Non-répudiation :** *La non-répudiation désigne l'impossibilité pour une personne de contester une action qu'elle a réellement effectuée, grâce à des preuves techniques et irréfutables permettant d'en attester avec certitude l'origine et l'intégrité.*
- ***CNIL :** La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*
- **Journal de crise cyber** *: Document qui sert à noter en temps réel tout ce qui se passe pendant une cyberattaque ou un incident de sécurité ainsi que tout ce qui est fait pour y faire face.*
- **Analyse Forensic :** *Ensemble des méthodes scientifiques et techniques permettant de collecter, préserver, analyser et présenter des données numériques (ordinateurs, téléphones, serveurs, réseaux) afin de détecter un incident, reconstituer des faits et fournir des preuves exploitables juridiquement.*

Termes et leurs abréviations :

- **PCC :** *Plan de communication de crise.*
- ***CNIL :** Commission nationale de l'informatique et des libertés.*
- ***RGPD :** Règlement général sur la protection des données.*
- **PRA :** Plan de reprise d'activité.
- **PCA :** Plan de continuité d'activité.
- **PRI :** Plan de reprise informatique.
- **PCI :** Plan de continuité informatique.

Grands Principes de communication de crise

Il est important d'appliquer les principes suivants en tout temps et en toute circonstance pour maintenir la crédibilité d'FAKESEC et limiter les impacts réputationnels, ces grands principes doivent être rappelés régulièrement pour que chacun puisse pleinement les intégrer.

Parler d'une seule voix (Unicité) : Désigner un porte-parole unique. Cela évite les contradictions entre les services qui détruisent la confiance et la crédibilité d'FAKESEC. Tout collaborateur sollicité doit répondre uniquement par : *"Une cellule de crise est en cours, je vous invite à contacter notre porte-parole." et ne doit répondre à aucune autre question.*

Privilégier la transparence (Honnêteté) : Ne jamais mentir ou dissimuler un fait avéré. En revanche, il est impératif de ne communiquer que des **faits vérifiés**. Si une information est inconnue, la posture doit être : *"Nous menons des investigations pour confirmer ce point précis, nous reviendrons vers vous dès que nous aurons une certitude technique."*

Occuper le terrain médiatique (Réactivité) : En communication de crise, le silence laisse place aux rumeurs. Si FAKESEC ne parle pas, les réseaux sociaux, la presse et les rumeurs le feront à sa place. Il faut communiquer tôt, même pour dire que l'on cherche encore, et que rien n'a évolué.

Faire preuve d'empathie envers nos Clients (Empathie) : Une crise cyber n'est pas qu'un problème technique, c'est avant tout un problème pour les gens qui utilisent vos services. Chaque message et appel téléphonique doit être réalisé avec une approche empathique et humaine. Par exemple, un message doit commencer par la reconnaissance de la gêne occasionnée : *"Nous sommes conscients de l'impact de cette interruption sur vos activités...".*

Posture de Leadership Opérationnel (Maîtrise) : En communication de crise, il est important de toujours renvoyer une image de **maîtrise** de la situation. Chaque communication décrivant un impact doit s'achever par les solutions mises en œuvre pour y remédier. Par exemple : "L'incident est localisé, nos experts sont en phase d'intervention pour un retour à la normale dans les meilleurs délais ".

Ne jamais spéculer sur l'attribution (Prudence) : Ne jamais désigner un coupable (ex : "ce sont des hackers russes" ou "c'est la faute de notre fournisseur") sans preuve judiciaire. Cela expose FAKESEC à des poursuites en diffamation ou à des représailles techniques plus agressives de la part des attaquants.

Protéger les informations sensibles (Confidentialité) : Communiquer sur l'incident ne signifie pas donner le mode d'emploi de l'attaque. Ne divulguez jamais de détails techniques précis sur les vulnérabilités exploitées tant qu'elles ne sont pas totalement corrigées, au risque d'attirer d'autres attaquants.

L'Équipe de Crise et les Rôles

Effectif de l’équipe

Rôle	Responsabilités Clés
Chef de Crise (Direction/Gérant)	Décisionnaire final. Valide les communications externes. Responsable du journal de crise cyber
Responsable de la Sécurité et des opérations techniques	Fournit l'analyse technique de l'incident et l'état de la résolution, et supervise les actions de remédiation.
Responsable Communication	Rédige et diffuse les messages. Gère les médias et les réseaux sociaux.

Matrice RACI Rôles Cellule de Crise

Matrice R.A.C.I Cellule de Crise			
Tâche \ Rôle	(RSSI)	(Responsable de comunication)	(Chef de crise)
Détection & Alertes	R	I	I
Activation de la cellule de crise	C	R	A
Désactivation de la cellule de crise	C	R	A
Obligations Légal (CNIL, Plainte..)	C	C	R
Gestion des Relations Médias & Réseaux Sociaux	I	R	I
Gestion Communication clients & Obligations Clients	I	R	I
Communication Interne salariés	C	R	I
Communication Externes Stratégique	I	I	R
Remonté Avancement PCA/PRA	R	I	I
Réunion Post Crise Retour sur éxpériences	C	C	R

lien Matrice original : Matrice RACI

Annuaire d’urgence:

lien Annuaire : Annuaire de contact cellule de crise

Personnes	Rôle	Téléphone	Contact Olvid
john doe	Chef de crise		
jeff lebowski	RSSI		
walter sobchak	Chef de Communication		

Moyens de déclaration d’un potentiel incident de cybersécurité

Généralités

Principe de Déclaration Sans Jugement : Tout collaborateur constatant une anomalie, même mineure, doit la signaler sans tenter d'en analyser la cause ou la gravité. **Le diagnostic de compromission est une prérogative exclusive du RSSI.**

Stratégie de déclaration

L'alerte doit obligatoirement transiter par un canal tiers (Téléphone/SMS) ou verbalement en présentiel pour éviter toute interception. Voir Fiche Locaux Déclaration Incident cyber

Processus d’Activation

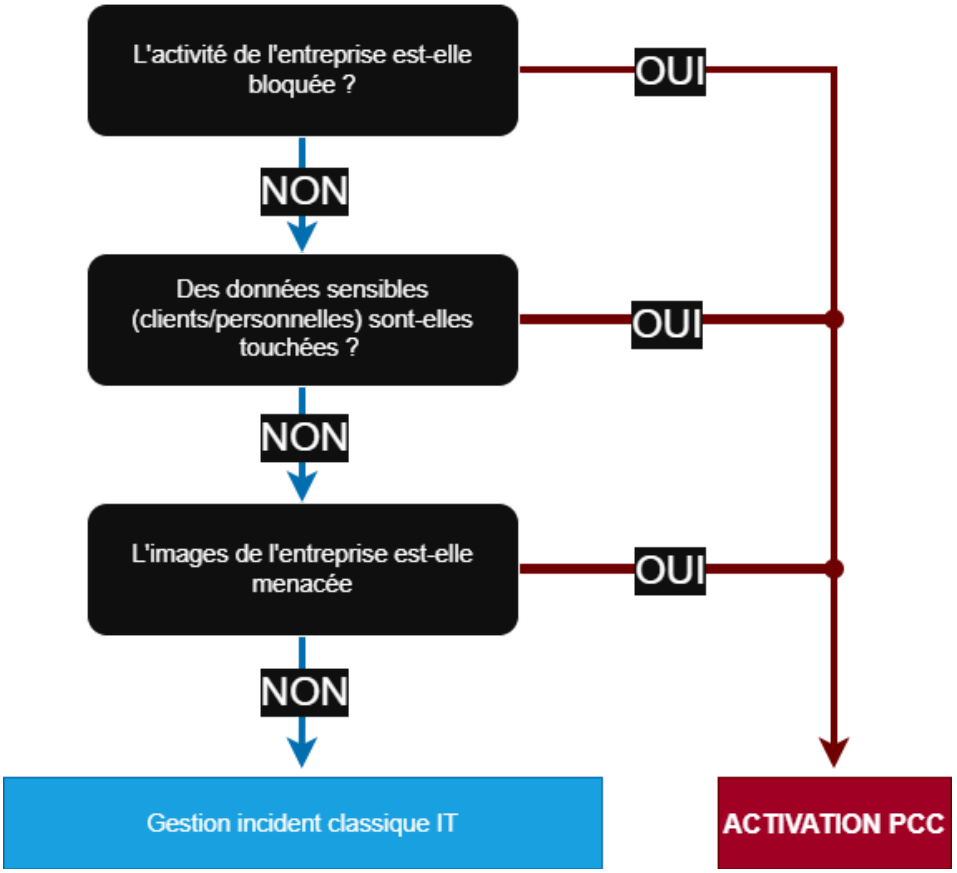
Procédures d’activation

Qualification de la situation (Réunion flash)

Le **RSSI**, le **Directeur Général**, le **Responsable de communication** se réunissent, évaluent la situation et prennent une décision selon l’arbre de décision ci-dessous.

Arbre de décision d’activation du PCC

Un incident technique n'est pas forcément une crise.



Procédure de déclenchement

Check-list déclenchement :

- ☐ L’alerte a-t- elle été vérifiée, et confirmée ?
- ☐ Chef de crise est-il informé ?
- ☐ L'équipe de crise est-elle réunie ?
- ☐ Le journal de crise est-il ouvert ?

Stratégie de Communication Interne

Utilisation d'OLVID installé sur les téléphones portables de chacun des employés devient l'unique source de vérité.

Communication Cellule de crise

Seuls les membres de la cellule de crise peuvent accéder au canal de la cellule de crise

Stratégie de communication

Fréquences des points de situation cellule de crise canal CELLULE DE CRISE

- **Rythme** : Un compte rendu flash au chef de crise toutes les 2 heures (même si aucune évolution majeure).
- **Consigne :** Même si la situation n'a pas évolué le RSSI doit effectuer un petit compte rendu de l'état d'avancement du PCA/PRA et de l'étendue des dégâts ainsi que le Responsable de communication également un compte rendu flash toute les 2 heures détaillant ses actions, que le chef de crise utilisera pour remplir avec soin le journal de crise pour relater chaque événement.

Canal de communication

Canal Olvid CELLULE DE CRISE **:** Décisions stratégiques entre les membres de la cellule de crise.

Communication salariés

Stratégie de communication

Seuls les membres de l'entreprise peuvent accéder en lecture seule au canal FAKESEC-INFO

Fréquence des points de situation employés canal -INFO

- **Rythme :** Un flash info toutes les 4 heures (même si aucune évolution majeure).
- **Consigne :** Rappeler à chaque message l'interdiction de communiquer sur l'incident à l'extérieur (famille, amis, réseaux sociaux).

Canal de communication

Canal Olvid FAKESEC-INFO **:** Groupe en lecture seule pour tous les salariés. Diffusion des consignes de sécurité (ex: *"Ne branchez aucune clé USB"*, *"Laissez vos postes allumés…"*).

Stratégie de Communication Externe

Communication aux clients et partenaires

Segmentation des clients

L'objectif est de préserver la réputation d'FAKESEC en démontrant une maîtrise totale de l'incident :

- **Clients stratégiques / Grands Comptes :** Appel direct et personnel sous **4h** après la qualification de la crise.
- **Clients Utilisateurs (Solutions IA/API) :** Envoi d'un communiqué technique par e-mail et publication d'un bandeau d'information sur la plateforme sous **8h**.
- **Anciens Clients / Partenaires :** Communication uniquement si l'analyse technique (Forensic) confirme une exfiltration de données les concernant.

Respect des Obligations Contractuelles Clients

FAKESEC s'engage à respecter les clauses de sécurité signées avec ses partenaires :

selon les termes des différents contrats pour les différents projets les directives mentionnées dans ces contrats doivent être impérativement honorées, prise de contact avec la ou les personnes responsables de la sécurité chez le client pour l'informer de l'incident et le rassurer quant à l'étendue des dégats et l'impact.

- **Veille Contractuelle :** Le responsable de Crise doit immédiatement consulter le registre des contrats pour identifier les délais de notification imposés.
- **Point de contact Sécurité :** L'information technique doit être transmise prioritairement au **RSSI du client** ou à son référent sécurité technique, afin d'éviter que l'alerte ne se perde dans un service commercial ou administratif.
- **Nature de l'information :** La notification doit être factuelle. Elle doit préciser :
    1. La nature de l'incident.
    2. Les mesures prises pour isoler la menace.
    3. L'impact potentiel sur les services fournis par FAKESEC.
    4. Les recommandations pour le client (ex: changement de clés API).

Communication Externes Stratégiques

Prestataires et infogérance

Prise de contact initiale pour informer le ou les prestataires de la situation et des actions qu'il sera amené à réaliser pour initier un dialogue fluide et transparent et permettre pour mener à bien les phases du PCA/PRA qui peuvent nécessiter leur intervention dans le cadre d'une prestation d'infogérance.

Dispositif d'aide étatique

Remplissage du formulaire de diagnostic 17Cyber et obtention d'une assistance technique en ligne.

Prestataire d'investigation Forensic (CSIRT)

À l'issue de la prise de contact avec Cybermalveillance.gouv.fr qui permet d'effectuer un diagnostic en ligne le 17Cyber vous mettra en relation avec des prestataires de proximité labellisés « ExpertCyber » pour aider dans la partie investigations (Forensic).

Gestion des Relations Médias et Réseaux Sociaux

Règle d'or : On ne crée pas une crise médiatique là où il n'y en a pas encore.

Palier de visibilité médiatique

Niveau	Impact Image & Media
Niveau 1	Clientèle restreinte. Plaintes au support. Pas de bruit sur les réseaux.
Niveau 2	Risque Réputationnel. Une personne en parle sur un réseau social ou un média tech pose une question.
Niveau 3	Crise publique. Article de presse, bad buzz massif, ou nom d'FAKESEC sur le Dark Web.

Stratégie Médiatique

Stratégie Médiatique : Niveau 1 (Gestion Silencieuse)

Résoudre l'incident sans alerter le marché ou les concurrents.

- **Action Presse : Silence strict.** Aucune sollicitation des médias.
- **Action Réseaux Sociaux : Veille passive.** Surveillance accrue des mentions "FAKESEC" pour vérifier que l'incident ne "fuit" pas. voir section veille et monitoring
- **Communication Clients :** Envoi d'une note d'information officielle aux clients et utilisateurs concernés

Stratégie Médiatique : Niveau 2 (Réaction Ciblée)

Éteindre l'incendie avant qu'il ne devienne viral et reprendre le contrôle.

- **Action Presse :** On ne diffuse pas de communiqué de presse, on se prépare à une Réponse aux demandes de renseignements à l'aide de la fiche Q&A au cas où un journaliste appellerait.
- **Action Réseaux Sociaux :** Si un client se plaint sur les réseaux sociaux, on répond publiquement et de manière courte. exemple *"Bonjour, nous traitons cet incident avec la plus grande rigueur. Pour vous aider au mieux, poursuivons cet échange en message privé."*
- **Consigne interne :** Alerte de la direction sur le risque de basculement en Niveau 3.

Stratégie Médiatique : Niveau 3 (Frontale et Transparente)

Objectif : Protéger la marque FAKESEC par une communication massive, honnête et experte.

- **Action Presse : Posture Proactive.** Diffusion d'un communiqué de presse officiel à nos contacts médias. Le chef de communication se tient prêt à répondre à des appels des médias et de la presse à l'aide du document de Q&A et se préparer à des interviews.
- **Action Réseaux Sociaux : Post Paratonnerre.** Publication d'un post officiel sur les réseaux sociaux officiels (LinkedIn, Twitter), d'FAKESEC expliquant la situation (sans détails techniques sensibles). Ce post sert de seuls lieux d'échange pour centraliser les questions et éviter l'éparpillement.
- **Communication Clients :** Notification générale à tout l'écosystème. Transparence sur les mesures de sécurité prises.
- **Consigne interne :** Interdiction absolue pour tout salarié de s'exprimer sur la situation.

Veille Médiatique

La veille est doit être effectuée dès le début de la crise et maintenue jusqu'à la clôture de la crise. L'objectif est de détecter les "signaux faibles" (une plainte isolée, un tweet, un message sur un forum) pour anticiper un basculement vers les Niveaux 2 ou 3.
Le Responsable Communication doit s'assurer que les outils suivants sont paramétrés avec une fréquence de notification "En temps réel" (Fiche paramétrage Alerts veille) :

- Web & Presse **:** Google Alerts**.**
- Réseaux sociaux **:** Talkwalker Alerts.

Procédure d'Alerte en cas de "Détection Positive"

Dès qu'une mention critique est détectée :

- Capture d'écran **:** Archiver la preuve pour le journal de crise.
- Alerte Flash **:** Notification immédiate de la cellule de crise sur Olvid canal “CELLULE DE CRISE”.
- Réévaluation : Analyse immédiate pour décider du passage au Palier de visibilité 2 ou 3.

Obligations Légales et Réglementaires

Dépôt de plainte gendarmerie

Le dépôt de plainte est indispensable pour les assurances et pour prouver la bonne foi de FAKESEC.

Il faut se rendre en Gendarmerie ou Commissariat sous 72h, avec les éléments techniques, les preuves d'intrusion et inventaire préliminaire des dommages que le RSSI aura constitués au préalable.

Déclaration à la CNIL

Conformément au RGPD, toute violation de données personnelles doit être signalée idéalement sous 72h.

Le chef de cellule de crise soumet la notification sur `notifications.cnil.fr`. Si toutes les informations demandées ne sont pas connues, effectuer une notification initiale, puis des notifications complémentaires plus tard.

Données personnelles (RGPD)

Conformément aux articles 33 et 34 du RGPD :

- **Violation de données :** Si l'incident entraîne une fuite de données personnelles, FAKESEC (en tant que sous-traitant ou responsable de traitement) doit notifier ses clients **par écrit** afin qu'ils puissent eux-mêmes remplir leurs obligations légales.
- **Transparence sur l'impact :** Toute affirmation concernant l'absence de vol de données doit être appuyée par des preuves techniques (logs de serveurs). À défaut de preuve, utiliser la formule : *"À ce stade des investigations, aucune preuve d'exfiltration n'a été détectée"*.

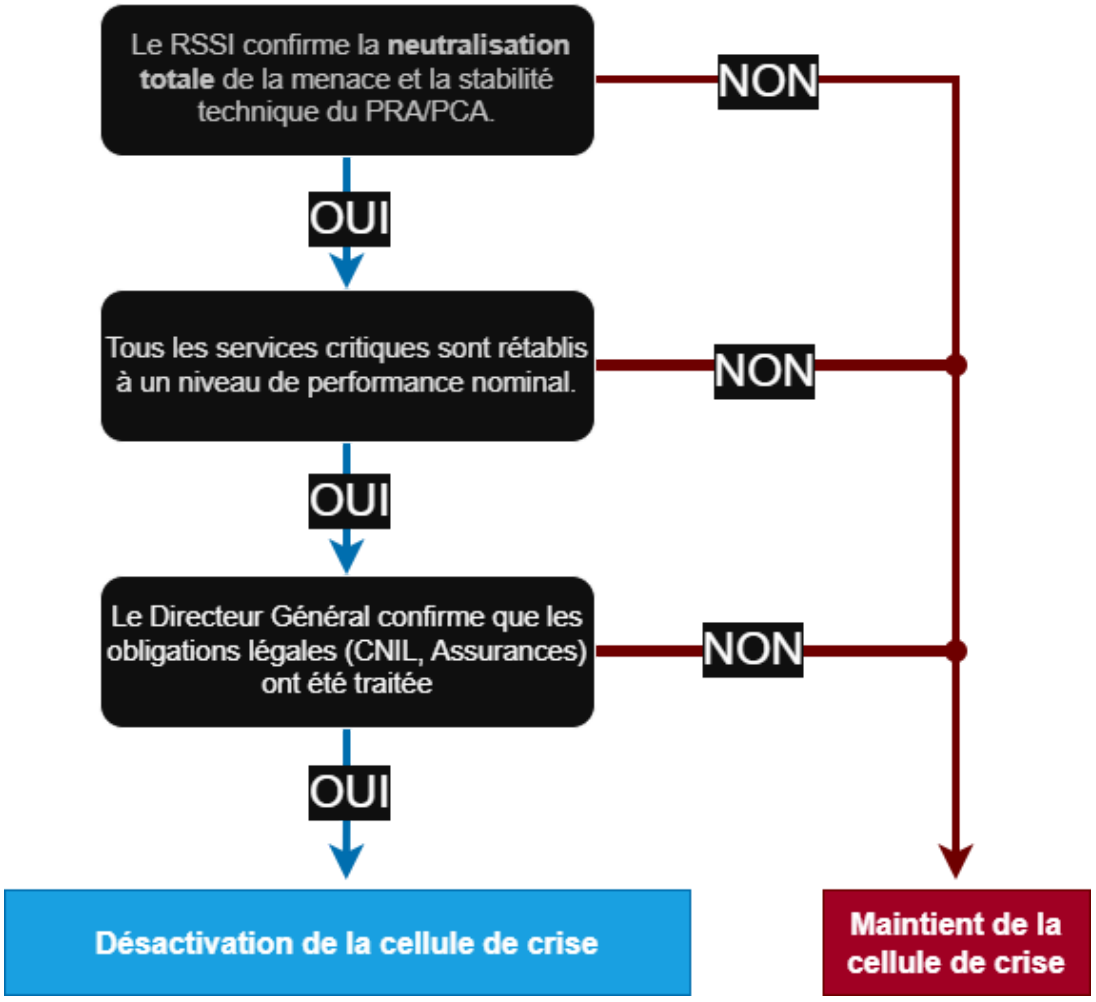
Clôture et Post-Crise

Procédures de désactivation

La désactivation est prononcée uniquement si et seulement si :

1. Le RSSI confirme la neutralisation totale de la menace et la stabilité technique du PRA/PCA.
2. Tous les services critiques sont rétablis à un niveau de performance nominal.
3. Le Directeur Général confirme que les obligations légales (CNIL, Assurances) ont été traitées.

Arbre de décision de désactivation du PCC



Procédure de désactivation

Check-list désactivation :

- ☐ Le Responsable Communication diffuse l'alerte de "Retour à la normale" à l'ensemble du personnel, clients, prestataires.
- ☐ Le Journal de Crise est clos et archivé de manière sécurisée
- ☐ Une date de réunion de Retour d'Expérience est fixée **sous 10 jours** pour identifier les améliorations nécessaires.

Annexes Opérationnelles

Journal de Crise
Fiches déclaration incident
...