

**Confidentiel**

**Fiche de traitement des Incidents de Sécurité (FISEC N° [xxx])**

**[Titre]**

🞎 **SI Chorus** 🞎 **SI interne**

|  |  |
| --- | --- |
| **Niveau de gravité** | Validation |
| Impact mineur | Adjoint AQSSI |
| Impact moyen | Adjoint AQSSI |
| Impact critique | Adjoint AQSSI puis Direction de l’A.I.F.E. |
| Impact majeur | Adjoint AQSSI puis Direction de l’A.I.F.E. |

**Définition du niveau de gravité :** le niveau de gravité est évalué par le propriétaire de la donnée et/ou de l’application impactée avec l’assistance du Responsable de la Sécurité des Systèmes d’Information (RSSI).

**Principe d’escalade :** il est de la responsabilité du propriétaire de la donnée et/ou de l’application impactée d’informer son supérieur hiérarchique.

|  |
| --- |
| **Rappel :** Est défini comme incident relatif à la sécurité des systèmes d’information, tout événement qui pourrait porter atteinte à la **disponibilité, intégrité, confidentialité et auditabilité** des données et des systèmes d’information dont l’AIFE a la charge.  La survenue d’un incident de sécurité affectant l’un des composants du SI ou des données à caractère personnel **doit être déclarée immédiatement** par toute personne le constatant **auprès de sa hiérarchie** (responsable de département ou délégué) **et de l’équipe SSI de l’AIFE** (voir le cartouche Définitions en annexe). |

|  |
| --- |
| Date de création de la FISEC (à remplir par l’observateur ou le pilote SSI) : xx/xx/20xx |

|  |  |
| --- | --- |
| Phase ➊ **Constat** (à remplir par l’observateur ou par le propriétaire de la donnée et/ou de l’application) | |
| **Description de l’incident** | Date de découverte de l’incident : *xx/xx/20xx*  Date d’occurrence de l’incident : *xx/xx/20xx*  *Préciser de façon la plus claire et synthétique possible l’incident : ce qui est arrivé et comment :* |
| **Ressources impactées** | *Préciser de façon la plus claire possible les ressources impactées – données, applications, réseaux, serveurs, documentation, processus,… :*  Impact sur des données à caractère personnel (RGPD) :  🞎 Oui : destruction, perte, altération, divulgation  🞎 Non |
| **Noms des personnes**  **impliquées** | Observateur : ………………………………….  Nom de l’entreprise pour un prestataire : ………………………………..  Pilote SSI : ……………………………..  Propriétaire de la donnée et/ou de l’application (cf. tableau :  <https://intranet.aife.economie.gouv.fr/mon-quotidien/securite/politiques-procedures/> )  ……………………………………………….. |

|  |  |
| --- | --- |
| Phase ➋ **Analyse** (à renseigner par le propriétaire de la donnée et/ou de l’application) | |
| **Description**  **De l’impact** | *Présenter de façon claire les impacts - actuels et à venir - de l’incident en termes de :*  🞎 Disponibilité 🞎 Intégrité 🞎 Confidentialité 🞎 Auditabilité  Données à caractère personnel impactées (RGPD)  Application utilisant les données (ex Chorus Pro, PLACE, etc …) : …………………….   |  |  | | --- | --- | | **Type de donnée** | **Décrire les données** | | Etat civil, identité, données d'identification, images… |  | | Vie personnelle (habitudes de vie, situation familiale, etc.) |  | | Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.) |  | | Données de connexion (adresse IP, logs, etc.) |  | | Données de localisation (déplacements, données GPS, GSM, etc.) |  | | Autre |  |   Volume de données impactées :  Nombre d’enregistrements : ……….  En Mo : …….. Mo |
| **Causes** | *Renseigner cette section est obligatoire. Préciser de façon claire les causes de l’incident et si un événement proche a déjà eu lieu. Si les causes n’ont pu être établies, en préciser les raisons.* |
| **Niveau de gravité** | 🞎 Mineur\* 🞎 Moyen\* 🞎 Critique\*\* 🞎 Majeur\*\*  *\*Informer obligatoirement le délégué concerné \*\*Informer obligatoirement la direction*  *(cf. critères de gravité décrits en fin de document)*  🞎 Validation de l’évaluation par l’adjoint à AQ-SSI en cas de désaccord propriétaire/SSI |

|  |  |  |
| --- | --- | --- |
| Phase ➌ **Plan de retour à la normale** (à renseigner par le propriétaire de la donnée et/ou de l’application) | | |
| Actions | Préciser les solutions techniques et/ou organisationnelles et le planning de mise en œuvre :  **Plan d’actions de retour à la normale** :   |  |  |  |  | | --- | --- | --- | --- | | **Action** | **RGPD O/N\*** | **Responsable** | **Échéance** | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   \**Actions liées à une violation de donnée à caractère personnel*  *Nota : le responsable de l’action peut être différent du propriétaire*  **Notification** **au DPD** : à faire par l’adjoint à l’AQSSI dans les 48 heures   |  |  | | --- | --- | | **Destinataire** | **Mail de notification au DPD en date du** | | DPD du ministère :  [le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr](mailto:le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr) |  |   **Risques résiduels** :  Indiquer si cet incident est récurrent  Indiquer dans quelle mesure cet incident peut se reproduire  Indiquer si la cause est non connue, non maîtrisée, …    **Remarques éventuelles :** | |
| **Traçabilité** | *(reporter les éventuels n° de DIV,…)* | |
| **Documents**  **liés** | *(faire référence aux éventuels plans d’actions plus détaillés,…)* | |
| Phase ➍ **Fermeture de la fiche (retour à la normale)** | | |
| **Preuve du retour à la normale validée par le délégué** | | ……………………………………. |
| **Validation de l’adjoint AQSSI** | | 🞎 Date : ../../…. |
| **Validation pour les incidents d’impact critique et d’impact majeur** | | 🞎 Direction A.I.F.E. / AQSSI  Date : ../../…. |

|  |  |
| --- | --- |
| Phase ➎ **Plan de prévention** (à renseigner par le propriétaire de la donnée et/ou de l’application) | |
| Actions | Préciser les solutions techniques et/ou organisationnelles et le planning de mise en œuvre :  **Plan d’actions préventives** :   |  |  |  |  | | --- | --- | --- | --- | | **Action** | **RGPD O/N\*** | **Responsable** | **Échéance** | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   \**Actions liées à une violation de donnée à caractère personnel*  *Nota : le responsable de l’action peut être différent du propriétaire de la donnée et/ou de l’application*  **Risques résiduels** :  Indiquer si cet incident est récurrent  Indiquer dans quelle mesure cet incident peut se reproduire  Indiquer si la cause est non connue, non maîtrisée, …    **Remarques éventuelles :** |
| **Traçabilité** | *(reporter les éventuels n° de DIV,…)* |
| **Documents**  **liés** | *(faire référence aux éventuels plans d’actions plus détaillés,…)* |

|  |
| --- |
| **Critères de gravité** |
| **Mineur :** l’incident aurait des conséquences ponctuelles ou acceptables à l'échelle de l’A.I.F.E. ;  **Moyen :** l’incident aurait des conséquences limitées mais gênantes pour l’A.I.F.E. ;  **Critique :** l’incident aurait des conséquences supportables mais très lourdes pour l’A.I.F.E. ;  **Majeur :** l’incident mettrait en cause la mission de l’A.I.F.E. pour une durée prolongée. |

|  |
| --- |
| **Définitions** |
| **Observateur**: personne qui constate un incident de sécurité. Elle doit informer l’équipe SSI.  **Propriétaire de la donnée et/ou de l’application** : personne qui a la responsabilité de la donnée et/ou de l’application. Elle est garante de l’application des mesures de sécurité.  **Pilote SSI** : RSSI, membre de l’équipe SSI, (respectivement Moustapha Niang, Phong Tran, Sandrine Laffaurie, Ali Harrabi).    Il est responsable du suivi du traitement de l’incident de sécurité.  Il pilote la FISEC, de son ouverture à sa fermeture.  Il accompagne le propriétaire de la donnée et/ou de l’application dans l’analyse de l’incident.  Il accompagne le propriétaire de la donnée et/ou de l’application dans l’élaboration des plans d’actions.  Il s’assure que les plans d’actions sont définis, ont un responsable et une échéance.  Il vérifie que les plans d’actions sont exécutés et en vérifie les résultats.  Il s’assure que la FISEC est fermée selon le processus (phase 4).  Il contrôle l’exécution du plan d’actions préventif.  **DPD** : délégué à la protection des données à caractère personnel du Ministère des finances (RGPD). Toute violation de données à caractère personnel doit être notifiée au DPD. |

|  |
| --- |
| **Processus de traitement de la FISEC** |
| L’observateur d’un incident de sécurité en informe immédiatement le RSSI Chorus ou l’équipe SSI (Département Architecture et Sécurité) : [l-aife-ssi@finances.gouv.fr](mailto:l-aife-ssi@finances.gouv.fr)  Le pilote SSI est responsable du suivi du traitement de l’incident de sécurité, et donc de la FISEC, jusqu’à sa fermeture. Il s’assure que les plans d’actions sont adaptés et mis en œuvre.  Le pilote SSI saisit le propriétaire de la donnée et/ou de l’application.  Le propriétaire de la donnée et/ou de l’application, accompagné du pilote SSI :   * Analyse l’impact de l’incident, en précisant si des données à caractère personnel sont impactées, en recherche les causes, évalue sa gravité. * Elabore le plan d’actions de retour à la normale, * Identifie les risques résiduels, * Informe son délégué (incidents d’impact mineur ou moyen) ou la direction (incidents d’impact critique ou majeur) * Fait exécuter le plan d’actions de retour à la normale. * En cas d’atteinte à des données à caractère personnel : l’adjoint à l’AQSSI notifie le DPD du ministère immédiatement.   L’adjoint AQSSI valide le retour à la normale sur preuve fournie par le Délégué concerné par la donnée et ou l’application.  Pour les incidents à l’impact critique ou majeur, la direction/AQSSI valide également le retour à la normale.  Le propriétaire de la donnée et/ou de l’application, accompagné du pilote SSI :   * Elabore le plan d’actions préventif, * Identifie les risques résiduels, * Fait exécuter le plan d’actions préventif.   Le pilote SSI contrôle l’exécution du plan d’actions préventif. |

La liste des systèmes d’information et leurs propriétaires est à consulter sur Aifevescence :

<https://intranet.aife.economie.gouv.fr/mon-quotidien/securite/politiques-procedures/>