SIGNALER UNE VULNÉRABILITÉ INFORMATIQUE

Safran s'appuie sur des valeurs et une éthique partagées par l'ensemble de ses parties prenantes. Il veille à ce que ses activités soient conduites conformément à des standards élevés d'honnêteté, d'intégrité et d'exigence professionnelle. Ces valeurs et cette éthique doivent permettre de répondre pleinement à la confiance que placent dans le Groupe, ses clients, son personnel, ses actionnaires, ses fournisseurs et l'ensemble de ses partenaires.

Les valeurs et principes de référence sont formalisés dans la Charte Ethique de Safran, disponible ici.

Dans chacun des domaines couverts dans la charte éthique, Safran a développé un dispositif de conformité mettant en œuvre des procédures internes, des référentiels et des guides régulièrement mis à jour dans une approche de progrès continu.

Pour les personnels de Safran, le Groupe a développé et entretient un document visant à aider à la bonne compréhension et connaissance des grands principes et pratiques en jeu : le Guide de la Conformité Safran, disponible sur l'intranet de Safran.

En cas d'interrogation sur une situation ou un comportement qui pourrait s'avérer contraire aux principes et engagements du Groupe, ou de doute sur la conduite à tenir, Safran met à disposition plusieurs canaux de signalement[1] :

- Signalement de comportement non éthique ou de fraude ;
- Signalement lié à un évènement pouvant avoir un impact sur la sécurité aérienne ;
- Signalement de vulnérabilité informatique.

1) Dans le respect des dispositions de la Directive UE 2019/1937 du 25 septembre 2019 relative à la protection des personnes qui signalent des violations du droit de l'Union et dans le respect des dispositions législatives nationales en matière de protection d'actifs. stratégiques et de sécurité nationale.

SAFRAN

1. PRINCIPES GÉNÉRAUX DE TRAITEMENT DES ALERTES ET SIGNALEMENTS

Sauf règles spécifiques décrites dans la procédure relative à la qualité en matière de sécurité aérienne ou en matière de vulnérabilité produit, les règles suivantes sont appliquées par Safran dans le processus de traitement des signalements :

a. Principes directeurs :

Une démarche de bonne foi

- L'auteur du signalement doit agir de bonne foi.
- La bonne foi s'entend d'un signalement sans malveillance ou sans attente d'une contrepartie personnelle.
- A défaut, l'auteur du signalement ne pourra pas bénéficier de la protection que lui confère son statut de lanceur d'alerte.

Les mesures de protection de l'auteur du signalement

- Sous réserve qu'elles aient agi de bonne foi, aucune mesure disciplinaire ou de représailles ne sera exercée à l'encontre des personnes émettant un signalement, même si les faits rapportés se révèlent infondés après traitement ou enquête.
- Toute mesure de représailles, directe ou indirecte, à l'encontre d'un employé du groupe Safran ayant émis un signalement ne saurait être tolérée et pourra donner lieu à des sanctions disciplinaires à l'encontre de l'auteur de ses représailles, allant jusqu'à la rupture du contrat de travail, conformément au droit local applicable.

L'identité de l'auteur du signalement

- Il est recommandé que les employés, collaborateurs occasionnels ou extérieurs qui souhaitent signaler une situation s'identifient, leur identité étant traitée de manière confidentielle. Toutefois, respectant en cela certaines législations locales, le signalement peut être anonyme.
- Le Groupe s'engage à prendre toutes les mesures nécessaires afin de protéger l'identité des personnes lorsque leur signalement concerne une fraude, une situation non éthique ou un délit. Leur identité ne peut être communiquée à la ou les personnes éventuellement mises en cause dans l'alerte, sauf accord exprès de l'intéressé.
- Les éléments collectés lors du traitement du signalement seront traités en toute confidentialité, sous réserve des obligations légales ou des procédures judiciaires, le cas échéant.

Collecte et conservation des données à caractère personnel

- Le traitement de données personnelles mis en œuvre est effectué sur la base de l'intérêt légitime de Safran de contrôler le respect de la charte éthique du Groupe, de vérifier la qualité de ses produits et services et de détecter les failles et vulnérabilité de ses systèmes et services

informatiques, le tout en vue de prendre les mesures adéquates de prévention et de remédiation, le cas échéant.

- Les données à caractère personnel recueillies à l'occasion d'un signalement ne seront utilisées qu'aux fins d'identifier et de traiter les éléments du signalement, mener les investigations internes et répondre au signalement.
- Dans ce cadre, Safran collecte conformément à la réglementation applicable[2] :

  - l'identité et les coordonnées de l'auteur du signalement (nom, prénom, email d'émission)

  - toute autre donnée à caractère personnel pouvant être indiquée dans le signalement (y compris de personnes tierces au groupe Safran en lien avec la vulnérabilité signalée)
- Ces données personnelles sont conversées au minimum jusqu'à la fin du traitement du signalement et au maximum jusqu'à la fin des prescriptions légales en cas de contentieux.
- Elles ne sont accessibles que par les personnes ayant besoin d'en connaitre dans le cadre de leur mission d'instruction du signalement et du traitement de la situation objet du signalement.
- Safran a mis en place des mesures physiques, logiques et organisationnelles à l'état de l'art pour protéger les données personnelles de toute perte d'intégrité, de disponibilité ou de confidentialité.
- Si un signalement concerne une entité Safran implantée en dehors de l'Union européenne, certaines données personnelles peuvent y être transférées en vue d'instruire le signalement et mener les actions de remédiation, le cas échéant. Ce transfert sera encadré par les règles internes d'entreprise – Responsable de traitement (Binding Corporate Rules – Controller) disponibles sur le site interne de Safran.

Les droits des personnes concernées

- Les personnes identifiées dans le recueil et le traitement des signalements ont des droits d'accès, de rectification, d'effacement, de limitation et de portabilité ainsi qu'un droit d'opposition. Ces droits peuvent être exercés en contactant directement et en priorité le Délégué à la protection des données personnelles Safran : safran.dpo@safrangroup.com
- L'exercice des droits dont vous disposez n'entrainera aucune forme de discrimination de la part de Safran.
- Les personnes concernées peuvent adresser leur demande à l'autorité française de contrôle des données personnelles (www.cnil.fr) ou à leur autorité nationale de contrôle des données personnelles.

b. Processus

Pour chaque alerte ou signalement, le processus de traitement interne respecte les étapes suivantes :

- apprécier la recevabilité de l'alerte / signalement,
- accuser réception du signalement,
- assurer la confidentialité du lanceur d'alerte / de l'auteur du signalement et ménager la

2) Notamment au Règlement UE 2016/679 et à la Directive UE 2016/680 en matière de protection des données personnelles.

présomption d'innocence de la personne objet du signalement ; à ce titre ne pas transmettre en aval des informations ou documents pouvant permettre de reconnaître l'identité de l'auteur, sauf accord préalable de celui-ci,

- informer les directions concernées,
- faire compléter la documentation de l'alerte par le lanceur d'alerte / l'auteur du signalement en tant que de besoin,
- mettre en place les diligences à conduire (enquête par la direction concernée, et si besoin par des enquêteurs spécialisés) et définir les mesures conservatoires éventuelles, en fonction du résultat des investigations, décider des suites à donner (clôture, mesures préventives, correctives, disciplinaires, juridiques, ...),
- définir les critères de clôture du dossier, et faire connaître la clôture du dossier quand elle intervient,
- informer l'auteur de l'alerte / du signalement (lorsque cela est possible) et le cas échéant la personne objet du signalement de l'avancement des investigations puis des mesures prises,
- archiver (en anonymisant) les éléments du dossier,

Tenir informé (ou saisir si besoin) le Comité Conformité Éthique et Anti-Fraude. En outre, la Direction de la Qualité et/ou la Direction du digital et des systèmes d'information seront également informées lorsque la nature du signalement relève de leurs compétences.

2. VULNÉRABILITÉS INFORMATIQUES

a. Quelle est la Politique de Divulgation de Vulnérabilité (PDV) de Safran ?

Les industries de l'aéronautique, de la défense et de l'espace en général sont en permanence guidées par le plus grand impératif de sûreté et de sécurité. C'est également le cas pour Safran, dont les produits et services sont marqués au sceau de cette même exigence.

Pour maintenir ce principe, Safran encourage ceux qui en auraient connaissance à lui rapporter les vulnérabilités affectant, réellement ou potentiellement, ses produits, ses services ou ses propres réseaux informatiques.

b. Que faire en cas de découverte d'une vulnérabilité ?

Si vous pensez avoir découvert une vulnérabilité sur un produit, un service ou sur les réseaux informatiques de Safran, si vous êtes témoin d'un incident de sécurité, vous pouvez nous le signaler par message électronique à l'adresse suivante : alert.vulnerability.saf@safrangroup.com.

Pour ce faire, nous vous recommandons au préalable de prendre connaissance avec attention du cadre de notre Politique de Divulgation de Vulnérabilités afin de vous permettre de bien évaluer si la divulgation que vous vous apprêtez à faire satisfait aux conditions de ce cadre.

c. Dans quel cadre s'exerce la divulgation de vulnérabilité ?

En choisissant de signaler à Safran une vulnérabilité, vos objectifs sont :

- Garantir la confidentialité de la vulnérabilité, au moins en attente de notre réponse, en particulier vis-à-vis de ceux qui seraient susceptibles de l'exploiter ;
- Ne pas mettre en œuvre la vulnérabilité sur un produit, un service ou le système d'information de Safran, au-delà ce qui permet de s'assurer de son existence ;
- Ne pas porter atteinte à l'image de Safran ;
- Ne copier que les informations de Safran dont vous avez strictement besoin à l'appui de votre divulgation et leur faire bénéficier des mêmes standards de protection et de conservation que ceux appliqués à vos propres données personnelles ;
- Ne pas porter atteinte à l'intégrité des produits, services, données ou systèmes d'information de Safran ;
- Ne pas perturber la disponibilité des services de Safran ;
- Ne pas capter ou rendre publiques des données de Safran;
- Ne pas tenter de pénétrer un réseau de Safran ;
- Ne pas tenter de monnayer la vulnérabilité avec Safran, qui n'accorde aucune rémunération ;

Si vous avez des doutes sur la conformité de la divulgation que vous envisagez de faire avec le cadre de la PDV ici décrit, vous pouvez demander conseil à l'adresse : alert.Cyber-Security.saf@safrangroup.com.

d. Vulnérabilités hors sujet

Certaines vulnérabilités ne sont pas considérées entrant dans le champ de la Politique de Divulgation Volontaire de Safran, comme :

- Les attaques en disponibilité (DDoS) sur les réseaux du Groupe ou les attaques par épuisement de ressources (resource exhaustion) ;
- Les vulnérabilités impossibles à reproduire.

e. Quelles sont les informations dont Safran a besoin pour traiter utilement votre divulgation ?

Afin de rendre le traitement de la divulgation rapide et efficace, elle doit inclure les éléments suivants :

- Une description de la vulnérabilité, y compris son potentiel impact ;
- Des éléments sur les circonstances de la découverte et les actions prises à la suite de cette découverte ;
- Des éléments sur les produits, services ou systèmes que la vulnérabilité affecte et éventuellement leur version ou configuration ;
- Tous éléments techniques permettant de comprendre la vulnérabilité : copie d'écran, fichier d'audit... ;

- Vos coordonnées, si vous le souhaitez, que nous garderons confidentielles ;
- Toute autre information jugée utile.

f. Que pensez-vous de la PDV de Safran ?

Si vous souhaitez exprimer votre avis sur la PDV de Safran, proposer des pistes pour son amélioration, merci de nous contacter à l'adresse alert.vulnerability.saf@safrangroup.com