REPORTING A COMPUTER VULNERABILITY

Safran depends on values and ethics shared by all of its stakeholders. Our business is conducted in compliance with the highest standards of honesty, integrity and professionalism. These values and ethics ensure that our customers, employees, shareholders, suppliers, and partners can depend on our commitments.

Our basic values and principles are formalized in the Safran Ethics Charter, available here.

In each of the areas covered by the Ethics Charter, Safran has established a compliance system based on internal procedures, standards, and guides that are regularly updated as part of a continuous improvement philosophy.

For Safran employees, the Group has developed and maintains a document to help them learn and understand the main principles and practices involved: the Safran Compliance Guide, available on the Safran intranet.

If you have any questions about a situation or behavior that could be contrary to the Safran's policies, you are encouraged to report the following situations to the appropriate parties with the responsibilities for the below situations[1]:

- reporting unethical behavior or fraud
- reporting events that may have an impact on flight safety
- reporting computer vulnerabilities

1) In compliance with the provisions of EU Directive 2019/1937 of 25 September 2019 on the protection of persons who report breaches of EU law and in compliance with national legislation on the protection of strategic assets and national security.

SAFRAN

1. GENERAL PRINCIPLES FOR HANDLING ALERTS AND REPORTS

Except for specific rules on aviation safety or product vulnerabilities described in the chapters on quality and airworthiness, the following rules are applied by Safran when processing reports.

a. Governing principles:

A good faith approach

- The reporter must act in good faith.
- Good faith is defined as reporting without malice or expectation of personal gain.
- If that is not the case, the reporter may not benefit from protective measures.

Protective measures for the reporter

- Provided they have acted in good faith, no disciplinary action or retaliation measures will be taken against persons reporting, even if the facts reported prove to be unfounded after processing or investigation.
- Any direct or indirect retaliation against a Safran employee who has made a report will not be tolerated and may result in disciplinary action against the retaliator, up to and including termination of the employment, in accordance with applicable local law.

The identity of the reporter

- It is recommended that employees, temporary workers and external staff who wish to report a situation identify themselves, as their identity will be treated as confidential. However, in compliance with certain local laws, the report may be anonymous.
- Safran is committed to taking all necessary steps to protect the identity of individuals when reporting fraud, unethical situations or crimes. Their identity cannot be communicated to any person or persons subject to the report, except with the express agreement of the individual concerned.
- The information collected during processing will be treated confidentially, subject to legal obligations or proceedings, if any.

Collection and storage of personal data

- Personal data is processed based on Safran's legitimate interest in monitoring compliance with the Group's ethics charter, verifying the quality of its products and services and detecting flaws and vulnerabilities in its IT systems and services, in order to take appropriate preventive and remedial measures, if necessary.
- Personal data collected in connection with a report will only be used for the purposes of identifying and processing the information in the report, conducting internal investigations and responding to the report.

- In this context, and in accordance with applicable regulations,[2] Safran collects:

  - the identity and contact details of the reporter (last name, first name, email address)

  - any other personal data that may be indicated in the report (including from persons outside the Safran Group in connection with the reported vulnerability)

- This personal data is stored at least until after the report is processed and at most until the end of any legal requirements in case of litigation.

- It is only accessible to those who need to know it in the course of investigating the report and processing the situation reported.

- Safran has implemented state-of-the-art physical, logical and organizational measures to protect personal data from loss of integrity, availability or confidentiality.

- If a report concerns a Safran entity located outside the European Union, certain personal data may be transferred to that entity in order to investigate the report and carry out remedial actions, if necessary. This transfer will be subject to the "Binding Corporate Rules - Controller", available on the Safran internal website.

Rights of data subjects

- The persons identified during the collection and processing of reports have the right to access, rectify and erase personal data and to restrict or object to its processing, as well as the right to data portability. These rights can be exercised by contacting the Safran Data Protection Officer directly: safran.dpo@safrangroup.com

- Exercising your rights will not result in any discrimination by Safran

- Data subjects may send their request to the French personal data control authority (www.cnil.fr) or to their national personal data control authority.

b. Process

For each alert or report, the internal handling process proceeds as follows:

- assess the eligibility of the alert / report

- acknowledge receipt of the report

- ensure the confidentiality of the whistleblower / reporter and protect the presumption of innocence of the person subject to the report; in this respect, do not release information or documents that could allow the identity of the reporter to be recognized, except with their prior agreement

- inform the relevant departments

- have the whistleblower / reporter complete documentation for the report as needed

- set up the procedures to be conducted (investigation by the department concerned, and if need be by specialized investigators), determine potential precautionary measures, and depending on the result of the investigations, decide on the proper follow-up (closing out the case, preventive, corrective, disciplinary, legal measures, etc.)

2) In particular EU Regulation 2016/679 and EU Directive 2016/680 on personal data protection.

- define the criteria for closing out the case, and inform the relevant parties when it is closed
- inform the whistleblower / reporter (when possible) and, if applicable, the person subject to the report of the progress of the investigations and the measures taken
- archive case information anonymously

The Compliance, Ethics and Anti-Fraud Committee is kept up-to-date or refer the matter to them. In addition, the Quality Department and/or the Digital and Information Systems Department will be informed when the nature of the report falls within their competence.

2. COMPUTER VULNERABILITIES

a. What is Safran's Vulnerability Disclosure Policy (VDP)?

The aeronautics, defense and space industries are constantly guided by the highest imperative of safety and security. This is also the case for Safran, whose products and services are subject to this same requirement.

In order to maintain this principle, Safran encourages anyone who may be aware of such vulnerabilities to report them to the company, whether they actually or potentially affect its products, services or its own IT networks.

b. What to do if a vulnerability is discovered

If you believe you have discovered a vulnerability in a Safran product, service or computer network, or if you have witnessed a security incident, you can report it to us by e-mail at the following address: alert.vulnerability.saf@safrangroup.com.

To do so, we recommend that you first carefully review our Vulnerability Disclosure Policy so as to properly assess whether the disclosure you are about to make meets the terms of that policy.

c. What are the rules for disclosing a vulnerability?

When choosing to report a vulnerability to Safran, the following rules are required:

- Protect the confidentiality of the vulnerability, at least pending our response, especially from those who might exploit it
- Do not implement the vulnerability on a product, a service or the Safran information system, beyond what is needed to ensure its existence
- Do not damage Safran's image
- Copy only the information from Safran that you strictly need to support your disclosure and apply the same standards of protection and retention as your own personal data
- Do not undermine the integrity of Safran products, services, data or information systems

- Do not disrupt the availability of Safran services
- Do not collect or make public any Safran data
- Do not attempt to penetrate a Saffron network
- Do not attempt to monetize the vulnerability with Safran, which does not provide any compensation

If you have any doubts about whether the disclosure you are considering is consistent with the VDP described here, you may seek guidance at alert.Cyber-Security.saf@safrangroup.com.

d. Vulnerabilities not covered by the policy

Some vulnerabilities are not considered to be within the scope of Safran's Voluntary Disclosure Policy, such as:

- DDoS attacks on the Group's networks or resource exhaustion attacks
- Unreplicable vulnerabilities

e. What information does Safran need to process your disclosure?

To enable quick and efficient processing, disclosures should include:

- A description of the vulnerability, including its potential impact
- Information on the circumstances of the discovery and the actions taken following this discovery
- Information on the products, services or systems that the vulnerability affects and their version or configuration, if applicable
- Any technical information that may clarify the vulnerability: screenshots, audit files, etc.
- Your contact information, if you wish, which we will keep confidential
- Any other information that you deem useful.

f. What do you think of Safran's VDP?

If you wish to express your opinion on Safran's VDP, or suggest ways to improve it, please contact us at alert.vulnerability.saf@safrangroup.com