Aerosystems "OpenLine" Policy - 2025

Introduction
Aerosystems S.r.l. is committed to full compliance with laws and regulations and to high standards of ethical business conduct as reflected in our Code of Conduct and related policies. Ethics & Compliance is the responsibility of every person in the company and is reflected not only in our relationships with each other but also with our customers, suppliers, shareholders and other stakeholders.

Aerosystems is also committed to developing a "Speak-Up" culture (Safety Just Culture) where all former or current employees, interns, temporary workers, candidates for employment, shareholders and third parties (including but not limited to contractors, subcontractors, direct or indirect suppliers and local communities around our and our suppliers' sites) (together the "Reporters") feel comfortable reporting what they perceive as suspected wrongdoing or violations of laws, regulations, our Code of Conduct or other Airbus policies. Reporters speaking up should feel confident that they will be heard and recognised and that it is the right thing to do to allow potential problems to be solved. Speak-Up also means that Aerosystems does not tolerate retaliation against Reporters for making alerts in good faith or against any Protected Third-Party, as defined below.

Several channels exist for Reporters to Speak-Up, verbally or in writing, including immediate supervisors, Human Resources, Quality Assurance representatives or Senior Management. In-person or videoconference meetings will also be arranged, where required by law.
Reporters may also submit an alert to the competent national authority directly. Competent authorities may vary from a jurisdiction to another.

As part of the Speak-Up mechanisms Aerosystems has established the "OpenLine": a channel through which alerts may be submitted securely and anonymously, where permitted by law. The use of the OpenLine is entirely optional and voluntary.

The objective of this policy is to present the key principles guiding use of the "OpenLine", how the "OpenLine" system works, and the steps followed by Aerosystems Ethics, Compliance, Safety and Information Security (Cybersecurity) personnel once it receives an alert.

Protection from Retaliation
Aerosystems will not tolerate retaliation (including threats or attempts of retaliation) by any Aerosystems employee against:

- a Reporter who, in good faith, submits an alert
- a "Protected Third-Party": Individuals or non-profit legal entities who assist a Reporter in submitting an Ethics & Compliance Allegation, as well as colleagues or corporate entities who may face retaliation measures, threats or attempts, in a professional context by virtue of their relationship, either professional or personal, with the Reporter. Protected Third Parties are protected by Aerosystems non-retaliation principles.

Retaliation is not only the opposite of leading by example, but also a form of ethical misconduct in itself. Retaliation can take many forms, including harassment, unfair performance evaluations, withholding or unequal allocation of work assignments, denial of recruitment or promotion opportunities, dismissal or any other form of sanctions, in particular related to compensation (such as bonuses or period pay raises).

Any person who is a victim of, or witnesses, an actual or potential act of retaliation should immediately alert Aerosystems, via the "OpenLine" or any other channel. If confirmed, the Aerosystems employee who engaged in retaliation, or who attempted or made threats of retaliation, will be subject to disciplinary action up to and including dismissal. Importantly, any such acts, attempts or threats of retaliation may also give rise to criminal and/or civil sanctions in certain jurisdictions.

Presumption of Innocence
Any person who is implicated in an "OpenLine" report is presumed to be innocent unless and until any allegation of wrongdoing is substantiated.

Anonymity and Confidentiality
Users of the "OpenLine" have the choice either to disclose their identity to Airbus, or to remain anonymous, where legally permissible.

If the user shares his/her identity, Aerosystems will treat the information confidentially, including any information that may directly or indirectly reveal the identity of the Reporter. Aerosystems will treat as confidential the identity of third parties referenced in the alert (report), as well as all other information provided by the Reporter as part of the alert. While the information will be treated as confidential, Aerosystems may disclose the information referenced in the alert, including names of individuals involved, to government authorities as necessary.

If the Reporter decides to anonymously use the "OpenLine" system, the only communication channel with Aerosystems will be through the "OpenLine" system.

Acting in Good Faith
Users of the "OpenLine" must act in good faith and must not make deliberately false allegations. Good faith is when the user has a plausible reason to believe an allegation is true, even if the allegation later proves unfounded or any statement or disclosure is later shown to be inaccurate.
It is only when a Reporter deliberately makes false or misleading statements that he/she may be subject to investigation action for submitting an alert.

"OpenLine" process

Channels to submit a Report
Reporters can submit a report (an alert, an occurrence) to the "OpenLine" via the website www.aerosystems.it.

Scope
Reporters may use the "OpenLine" to submit an alert on the following topics:

Business Compliance Allegations:

1) **Bribery** - giving, offering, promising or receiving anything of value to obtain or retain business or other improper advantage. Active bribery refers to a bribe paid by or on behalf of Airbus. Passive bribery refers to receipt of a bribe by someone at Aerosystems. Bribery includes the making of facilitation payments, i.e., small, unofficial payments to low-level public officials to speed up or obtain routine administrative processes.

2) **Falsification of documents or intentional violation of policies or procedures** - obtaining money or objects from others through deceit; falsifying documents such as invoices or contracts; improper or wrongful dispensing of assets of the company to the disadvantage of Aerosystems; intentional evasion of Aerosystems policies and procedures

3) **Accounting or tax fraud** - Misstatements or omissions in accounting records, financial statements or tax filings.

4) **Competition -** agreements, practices or behaviours having the object or effect to limit competition, including access to competitors' commercially sensitive and/or confidential information.

5) **Conflict of interest** - situations in which an employee's personal interests interfere, or appear to interfere, with his/her ability to perform his/her job without bias.

6) **Breach of confidentiality or of data protection regulations** - unauthorised disclosure of confidential or classified information owned by the company or entrusted to Aerosystems by third parties, or any breach of data protection rules and regulations.

7) **Export control and international sanctions and diversion ("Export Control Allegations")** - violation of policy, national or international law or regulations relating to (i) export controls, including materials, services, technical data and technologies designed for military or dual use purposes by an entity or (ii) international sanctions or diversion (for example, in the event of commercial activity with prohibited parties).

8) **Human rights -** issues related to a violation of policy, regulation, legislation or international standards related to human rights, including any form of forced or child labour, including human trafficking, as well as labour practices and other working conditions not covered by the People Matters category.

9) **Breach of procurement processes -** issues related to suppliers or subcontractors which are not covered in any other category defined in this Method, such as breaches of Airbus' supplier selection processes, the Airbus Supplier Code of Conduct or applicable laws/regulations related to Procurement.

10) **Aviation Safety / Quality -** allegations that the Safety or Quality of Aerosystems products or services has been compromised, with risk of harm to people working on an Aerosystems product (component) (including Aerosystems workforce, maintenance or ground operations personnel) or which may jeopardize the integrity of the Aerosystems products or services.

11) **Information Security -** breach of security policies, including physical or IT security;
- Information security events,
- Information security risks with a potential impact on aviation safety,
- Suspicious emails or phishing attempts,
- Unauthorized access attempts,
- Lost or stolen devices,
- Data breaches or suspected leaks,
- Weaknesses in software or hardware systems,
- Use of systems for unauthorized purposes or in ways that violate company policies unusual system behavior or performance issues,
- Systems running unexpectedly slow, crashing, or behaving abnormally,
- Potential signs of malware or compromise,
- Social engineering attempts and hacking (phone calls, visits, or messages attempting to trick staff into revealing confidential) information.
- Unapproved software or hardware (installation or use of unauthorized applications, devices, or tools that bypass security controls),
- IS Manual, Policy or Procedure violations (non-compliance with Aerosystems information security manual, policies or procedures),
- Physical security breaches (unauthorized individuals accessing secure areas, or tampering with security systems or devices),
- Suspicious network activity (unexpected connections, large data transfers, or access from unusual geographic locations),
- Changes in user roles or access levels not reflected in systems (when employees change roles or leave the organization and their access is not promptly updated or removed),
- Incidents reported by customers, partners, or third parties (security concerns raised by external stakeholders should be escalated internally),
- and any other Information Security related event.

12) **Environment -** breach of environmental law or Aerosystems company policy and procedures.

13) **Health & Safety -** breach of health and safety law or Aerosystems company policy and rules.

14) **Retaliation -** any form of retaliation (including threats or attempts of retaliation) against a Reporter or a Protected Third-Party related to a previous Ethics & Compliance Allegation.

People Matters Allegations:

1) **Moral harassment and bullying** - unwanted or unwelcome behaviour towards another person, resulting in deteriorating working conditions that is likely to impact a person's physical and mental health and can create a hostile, degrading, humiliating or offensive environment for the person.

2) **Sexual harassment -** sexual harassment is an unwanted act or behaviour of a sexual nature or with a sexual connotation such as unwelcome sexual advances, inappropriate touching or verbal comments.

3) **Discrimination -** any distinction, exclusion or preference that has the effect of nullifying equality of treatment or opportunity based on illegitimate grounds such as, but not limited to, color, nationality, sexual orientation, gender, age, disability, or pregnancy.

4) **Breach of HR policies or processes** - issues relating to violations of Aerosystems HR policies and processes not covered by any other category.

The following information cannot be registered on the Aerosystems "OpenLine" channel:

- Classified information, or controlled unclassified information (including information that is subject to export control restrictions);
- Information covered by legal or medical professional privilege;
- Information covered by the secrecy of a criminal investigation;
- Information covered by the secrecy of judicial deliberations;

If the reprot (alert) involves one of the above topics, please submit a report but do not include the above-mentioned information. When the report is submitted, request a meeting with the investigator to provide the additional information in a manner that respects legal constraints.

Operation of the "OpenLine"

Communication and Reporter Feedback

Once a Reporter submits an alert through "OpenLine", it will be automatically transferred to the CISO Chief Information Security Officer and the CMM Compliance Monitoring Manager of Aerosystems.

An acknowledgement of receipt will be provided to the Reporter following receipt of the alert. Aerosystems reserves the right to discard alerts that do not meet conditions defined by applicable laws, and in such situations, it will inform the Reporter and specify why the alert does not meet legal requirements.

The Compliance Monitoring Manager will communicate with the Reporter as necessary to receive additional information. Within three months after the acknowledgment of receipt, the Compliance Monitoring Manager will provide the Reporter with feedback of the investigation. In the event that the investigation lasts more than three months, feedback must be provided periodically until the closure of the case.

At the end of the investigation, the Reporter will receive feedback about the outcome and the closure of the investigation.

Investigation
All investigations related to "OpenLine" alerts will be carried out in accordance with Aerosystems Safety Management System, Information Security Management System, Quality and Environmental System, methods for Investigation of Compliance.

Recording and Rights of Access
Information provided in connection with a reported alert that is deemed to be unfounded or immaterial will be destroyed immediately. In addition, personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

Information provided in connection with an alert will be retained for a period that is deemed necessary, proportionate and in accordance with applicable laws. After this time period, the information will be destroyed in a manner consistent with national laws. This does not apply to cases in which disciplinary and/or judicial proceedings have been brought against the implicated person or the person who submitted the alert or any third parties.
In some jurisdictions, the implicated person may have the right to access data concerning him or her and to request that such data be corrected or deleted, as applicable. On the basis of such rights of access, an implicated person generally may not obtain information regarding third parties, such as the identity of the person who made the alert, the identity of other individuals who are referenced in the alert, or any information that may reveal, directly or indirectly, these identities.
Further, Aerosystems will make all possible efforts to protect from disclosure all information provided by the Reporter as part of the alert.

More information on the processing of data and the rights of "OpenLine" users can be found in Privacy Policy, which is available on the Aerosystems website.

Contact Details
It is possible to get in contact with the "OpenLine" by:

Connecting to the Aerosystems "OpenLine" channel on company website: www.aerosystems.it.
This medium is available in English.

or

Calling one of the following numbers to make a report through a recorded voice messaging system available 24/7.
Please note the voice messaging system is available in the languages listed below:

Worldwide: 0039.0331.1090536.
Language: Italian / English
Voice Messaging System: based in Italy

September 29, 2025

AEROSYSTEMS

Aerosystems S.r.l.
Prescision Aerospace Components

Via San Gottardo 4, 21021 Angera (VA) Italy
Telephone: 0039.0331.1090536
Email: info@aerosystems.it
Website: www.aerosystems.it