



FIRST EDITION / CORPORATE GOVERNANCE

WHISTLEBLOWING POLICY

Aerospace Federation

PROTECTED REPORTING

INDEPENDENT INVESTIGATION

NO RETALIATION

Publication identity and use

Control field	Controlled value
Title / code	Whistleblowing Policy / AF-PL-016
Edition / revision / language	First Edition / Revision 00 / English master text
Edition date	30 September 2026
Document owner	Legal and Integrity Coordinator
Operating interface	P03 and P17; all AF process and service interfaces
Institutional scope	Aviation, space, the whole defense industry, heavy and advanced industry, defense- and space-purpose mobility; all AF corporate and service activities.
Approval and effectivity	Actual authority, adoption, commencement, role holders and operating readiness shall be recorded through AF-FR-001 and AF-ML-001. The edition date is not approval evidence.
Relationship to existing files	Separate expanded policy. Existing AF source documents, prior policies and the final AF 9100:2026 files remain unchanged.
Distribution	Policy text may be published after authorized release. Completed case, declaration and personal-data records are protected according to their content.

Speak up safely. Protect people. Preserve the truth.

This policy applies across governance, membership, committees, technical and assurance services, learning, events, awards, research, funding, partners, chapters and enabling functions. Requirements follow the actual relationship and lawful mandate; they do not create general authority over unrelated third parties.

Reading and implementation route

Read the numbered sections for requirements and responsibilities, then use the annexes for scope matrices, timelines, decision controls, communication models and records. The final annex identifies inherited AF requirements and the implementation controls added in this edition. Complete actual contacts, roles, approvals and jurisdiction-specific conditions before operational use.

“Shall” states a requirement following valid adoption; “should” states a recommendation; “may” states permission. Examples are synthetic. A template is evidence-capture space, not a completed approval or a factual public notice. Mandatory law and higher AF instruments retain their effect.

Contents

Clause and annex identifiers control references. Page numbers show where each section begins.

Section	Page
1 Purpose and institutional commitment	4
2 Persons and activities covered	4
3 Reportable concerns and routing	4
4 Protection threshold and honest mistakes	4
5 Reporting channels and safe contact	5
6 Anonymous reporting and confidentiality	5
7 Accountability and independence	5
8 Receipt, acknowledgment and initial triage	6
9 Non-retaliation and protective arrangements	6
10 Assessment and investigation planning	6
11 Evidence preservation and controlled information	6
12 Fairness to respondents and witnesses	7
13 Communication, feedback and elapsed time	7
14 Findings, decisions and corrective action	7
15 Reviews, appeals and external reporting	8
16 Partners, chapters and supply chains	8
17 Records, privacy and retention	8
18 Capability, monitoring and improvement	9
19 Adoption, interpretation and continuing protection	9
Annex A Whole-federation concern and routing matrix	10
Annex B Reporting-channel deployment and safe intake	11
Annex C Triage and investigation record	12
Annex D Protection and anti-retaliation plan	13
Annex E Timetable, notifications and worked chronology	14
Annex F Communication and partner terms	15
Annex G Readiness tests and measures of effectiveness	16
Annex H Source alignment, adoption and controlled release	17

1 Purpose and institutional commitment

1.1 A safe route for concerns

Aerospace Federation shall provide a credible route to raise suspected wrongdoing connected with its governance, people, services, authorized operators and relevant partners. The purpose is early protection, fair investigation and correction, not the suppression of criticism or the protection of institutional reputation at the expense of truth. Reports concerning aviation, space, all defense-industrial domains, heavy and advanced industry or defense- and space-purpose mobility shall receive competent, scope-specific handling. A person need not prove the complete allegation before asking AF to examine a reasonable concern.

1.2 Relationship to the AF system

This policy expands protected reporting under AF-PL-012, AF-PR-019 and AF-PL-013. AF-PL-017 administers complaints and decision appeals; AF-PL-018 controls personal information; AF-PL-019 controls interests. AF-CON-001 retains constitutional powers and safeguards. A protected report may trigger linked technical, employment, membership, privacy or governance proceedings, but shall not be converted into a less-protective route to avoid confidentiality, independence or anti-retaliation duties.

2 Persons and activities covered

2.1 Inclusive access

Employees, former employees, applicants, directors, officers, volunteers, interns, members, students, contractors, suppliers, experts, examiners, jurors, research partners, participants and affected members of the public may raise relevant concerns. Facilitators, witnesses and people associated with a reporter shall be protected against related retaliation within AF's authority. The policy covers in-person, remote, online and hybrid work and relevant conduct before or after an engagement. Membership, current employment, payment, nationality and seniority are not prerequisites for receiving a concern.

2.2 Limits of institutional authority

AF investigates matters within its own valid powers and agreements. It may request cooperation, protect its services, refer matters and enforce appropriate contract or scheme terms; it does not acquire police powers or regulate every activity of a member enterprise. An allegation about an unrelated organization shall be assessed for any material AF connection and, where appropriate, directed to a competent external route without unnecessary transfer of identity. Outside employment protection or remedies depend on applicable law, not merely this policy.

3 Reportable concerns and routing

3.1 Examples of reportable wrongdoing

Reportable concerns include unsafe practices or concealed hazards; falsified tests, qualifications, votes, records or credentials; bribery, fraud, theft or misuse of restricted funds; compromised assessments or awards; serious conflicts; retaliation, harassment, safeguarding failures or exploitation; unlawful technology transfer; serious privacy or cybersecurity failures; research misconduct; deliberate misleading claims; obstruction of oversight; and concealment of any such matter. Attempted wrongdoing and credible future harm may be reported. A technology or program label shall not narrow protection where the underlying concern falls within AF's remit.

3.2 Distinguishing related routes

A service complaint concerns dissatisfaction; an appeal challenges a specific decision; a personal grievance concerns an individual employment or participation issue; a protected disclosure concerns suspected wrongdoing. These descriptions guide handling, not eligibility traps. Mixed submissions shall retain the original receipt time, a common linkage and appropriate distinct owners. An immediate safety or security incident also activates AF-PR-015. An appeal deadline is not a deadline for raising later evidence of wrongdoing. Annex A provides the routing matrix.

4 Protection threshold and honest mistakes

4.1 Reasonable reporting and good faith

AF shall protect a person who reports information they honestly believe indicates wrongdoing, including a report made on reasonable grounds that later proves mistaken. Motive, personal disagreement or a parallel grievance does not by itself defeat protection; any more protective applicable legal threshold prevails. The reporter shall distinguish observation, hearsay, inference and uncertainty where possible. AF shall not require the reporter to establish a legal offense or correctly identify a policy code before receiving and triaging the information.

4.2 False information and self-involvement

An unsubstantiated, withdrawn or mistaken report is not a malicious report. Knowing fabrication or deliberate destruction of material evidence may be examined only through a separate fair process supported by evidence, not inferred from an unfavorable outcome. Reporting one's own involvement does not automatically immunize unrelated misconduct; truthful cooperation, coercion and mitigation shall be assessed within the applicable procedure. No threat of defamation action, disciplinary sanction or contractual penalty shall be used to discourage a lawful protected disclosure.

5 Reporting channels and safe contact

5.1 Actual monitored routes

Before operational use, AF shall publish verified written and oral reporting routes, a safe means to request a private meeting, responsible role holders and deputies, accessibility arrangements and monitoring hours. An unimplicated supervisor, the Legal and Integrity Coordinator or the Ethics and Impartiality Committee may receive a report. A reporter may bypass the management chain. No specific mailbox, telephone, hotline, portal or round-the-clock service is represented as active by this document; the deployment record in Annex B shall be completed and tested before such a claim is made.

5.2 Safe alternatives and misdirected reports

Ask how and when contact is safe, whether a work account is monitored by an implicated person, and whether a neutral subject line or representative should be used. An unintended recipient shall protect the information, avoid unnecessary forwarding, pass it promptly through a secure unimplicated route and preserve the original receipt time. Provide oral, assisted and non-digital alternatives where necessary. The receipt team shall not demand an exclusive form. Imminent danger shall be directed immediately to appropriate emergency or competent authorities rather than waiting for AF business hours.

6 Anonymous reporting and confidentiality

6.1 Anonymous access

Relevant anonymous reports shall be assessed on their available evidence. Where a secure anonymous two-way facility is actually deployed, explain its use, limitations and loss-of-access risk. Do not falsely promise that an ordinary email or web form conceals metadata. No person shall attempt to identify an anonymous reporter merely because the report is inconvenient. A necessary investigation of deliberate material abuse or an actual legal duty requires documented independent authorization and lawful proportionality, not unrestricted identity hunting.

6.2 Need-to-know identity protection

Store the reporter's identity and safe contact information separately from the working case file. Use a case identifier in ordinary tracking and disclose identifying details only to authorized people who need them for lawful protection or fair handling. Explain confidentiality limits without promising absolute secrecy. Before a compelled or necessary disclosure, assess legal basis, alternatives, minimum content and harm; inform the reporter in advance where lawful and safe. Do not circulate raw allegations or identifying details to the full Council, a sponsor, an employer or a technical committee by default.

7 Accountability and independence

7.1 Named functional responsibilities

The Legal and Integrity Coordinator shall administer the protected-report process; the Ethics and Impartiality Committee shall oversee integrity and independent escalation; designated investigators shall establish facts; competent decision authorities shall determine remedies within their actual mandates. The Information and Security Manager supports protected systems without discretionary access to case substance. People and program managers implement lawful protective measures. The Quality Manager tracks de-identified corrective learning. Roles and deputies shall be assigned, conflict-cleared and resourced before sensitive case work is undertaken.

7.2 Cases involving leadership or handlers

An implicated President, director, officer, supervisor, case handler or committee member shall not select the investigator, control relevant evidence, approve their own protection arrangements or direct the outcome. The independent oversight route shall secure an appropriately independent external professional where necessary. A complaint about the oversight function itself shall use an unimplicated independent appointment route maintained under AF-CON-001 Article 23. Absence of internal capacity shall trigger external support or a restriction of the affected work, not a return of control to the subject of the allegation.

8 Receipt, acknowledgment and initial triage

8.1 Case registration

Record the actual receipt time and time zone, channel, issue summary, safe contact preference, relevant programs, immediate risks and known conflicts. Assign a restricted case ID and preserve the original submission. Acknowledge within five calendar days where safe communication is possible; an automated receipt does not establish substantive review. Any shorter controlling legal duty applies. Acknowledge an anonymous report only through a functioning safe channel; record why direct contact is not possible rather than inventing a response.

8.2 Protective triage

Triage credible urgent harm, retaliation, evidence loss, compromised independence, safeguarding, controlled data and mandatory notifications immediately on recognition. As a new AF administrative control, record the initial triage within one calendar day of receipt, with any safety-driven action occurring sooner. Identify competent authorities and all separate clocks. Do not delay triage until a submission is complete, an invoice is paid or a scheduled meeting occurs. Annex C records facts, preliminary risk, evidence protection and the assigned next action.

9 Non-retaliation and protective arrangements

9.1 Prohibited detrimental treatment

Prohibit dismissal, demotion, threats, unfavorable reassignment, exclusion from committees or events, withheld payment, blacklisting, loss of unrelated services, harassment, intimidation, doxxing and other adverse treatment because a person reported, assisted, testified or sought advice on a protected concern. Prohibit indirect retaliation through affiliates, contractors or informal influence. Do not use membership standing, competence review or confidentiality language as a disguised penalty. A report of retaliation is a separate urgent concern even where the original allegation remains unresolved.

9.2 Individual protection plan

Agree a proportionate plan addressing safe contact, supervision, access, physical or digital risk, assignment continuity and available support, without forcing the reporter into a disadvantageous transfer. Preserve legitimate independent employment and technical decisions supported by unrelated evidence; an unimplicated reviewer shall check potentially adverse actions for retaliatory linkage. As AF implementation checks, review protection at case opening, material changes and normally 7, 30 and 90 days after closure where safe and relevant. These dates do not end continuing protection or a legal remedy.

10 Assessment and investigation planning

10.1 Mandate and scope

The independent appointing authority shall issue written terms identifying allegations, relevant requirements, jurisdiction and authority, people and systems affected, investigator competence, access, safety, confidentiality, resources, milestones and reporting recipient. Define the applicable evidential standard before merits determination; no universal criminal, employment or constitutional standard is invented here. Preserve facts favorable and unfavorable to each explanation. A preliminary assessment may close a clearly out-of-scope or duplicate issue with reasons, but material new information and protection needs shall still be addressed.

10.2 Proportionate methods

Use document review, interviews, observed practice, transaction tracing and competent technical analysis appropriate to the issue. Seek corroboration without making corroboration a condition of intake. Record gaps, conflicting accounts and reliability limitations. Interview witnesses individually where appropriate, agree accurate notes, and prevent coaching or unnecessary disclosure. Commission specialized metrology, cybersecurity, safeguarding, financial or legal expertise where the investigator lacks it. A failed test or research result is not automatically misconduct; examine the actual rule, conduct and evidence.

11 Evidence preservation and controlled information

11.1 Lawful preservation

Preserve relevant original records, versions, timestamps, access histories and correction trails through a scoped hold. Document who collected each item, its source, actual date, method and integrity check where useful. A file hash supports identity, not the truth of its content. Do not direct a reporter to hack systems, enter restricted locations, covertly record unlawfully or export controlled files to prove a concern. They may describe what they

know and seek a lawful protected evidence route. Unlawfully obtained material requires competent handling, not automatic distribution.

11.2 Sensitive and technical material

Classified, export-controlled, personal, privileged and commercially sensitive information shall be handled only by appropriately authorized persons and systems. A nondisclosure agreement or AF membership is not access permission. Use necessary secure local inspection, redaction or other lawful arrangements while recording evidential limits. Refuse unapproved public AI processing and preserve model-assisted analysis as analysis, not independent witness evidence. An ordinary protected-report channel shall warn against uploading restricted technical files until a suitable route is confirmed.

12 Fairness to respondents and witnesses

12.1 Meaningful opportunity to respond

Give a respondent sufficient particulars of material allegations and a fair opportunity to answer before an adverse final finding, subject to proportionate lawful limits protecting people and evidence. Record any justified delay in notification and review it. Do not treat an allegation as a proven fact in a directory or public statement. Respect representation and support rights under the actual relationship. Separate the reporter's identity from the substance where an anonymized summary or controlled access can provide fairness.

12.2 Protected procedures remain intact

Membership discipline retains at least 21 calendar days to respond under AF-CON-001 Article 7. Director-removal proceedings retain the separate Article 13 notice, independent investigation and decision rules; this policy creates no additional removal power. Elected committee offices retain Article 16 protections. Employment and contractual measures follow the actual lawful procedure. Urgent provisional protection may precede a final finding only through valid authority and prompt independent review. A desire to meet a 60-day case target shall not shorten a protected response period.

13 Communication, feedback and elapsed time

13.1 Substantive feedback

Provide an initial substantive response within 30 calendar days and normally determine the matter within 60 days from original receipt, consistently with AF-PR-019 and the constitutional complaint framework. Explain the route, what can be examined, relevant progress, next steps and any material limits without disclosing confidential third-party details. Where a legal protected-disclosure regime imposes an additional feedback or consultation requirement, record and meet it independently. Do not report that an investigation is complete merely because a receipt was sent.

13.2 Necessary extensions

A justified extension shall identify the reason, revised date, outstanding work, protection measures and accountable approver; communicate progress at least every 30 days. Administrative incompleteness, referral or a change of handler shall not silently reset receipt. A necessary external authority pause shall identify what is paused and what remains active. Urgent protection, evidence preservation, statutory filing limits and scheme notifications continue on their own clocks. Where safe feedback is impossible, preserve the attempted contact and the objective handling record.

14 Findings, decisions and corrective action

14.1 Reasoned outcomes

The investigator shall distinguish substantiated, partially substantiated, not substantiated on available evidence, inconclusive and out-of-scope matters. Explain the requirement, evidence, contrary material, uncertainty and rationale. Not substantiated does not mean a report was false. The investigator's factual conclusion shall remain separate from disciplinary, technical, financial or constitutional action by the authority empowered to take it. Preserve material dissent and do not edit the report to satisfy a sponsor or respondent.

14.2 Remedies and effectiveness

Remedies may include containment, corrected reports or credentials, re-evaluation, recovery of funds where lawful, restored participation, training, changed controls, contract action or referral to a competent authority. Apply AF-PR-018 to systemic defects and trace affected earlier work. A revised policy or apology alone does not establish effectiveness. Assign owners, deadlines and independent verification proportionate to consequence. Notify affected users when necessary to correct a material public or technical claim without exposing unrelated confidential information.

15 Reviews, appeals and external reporting

15.1 Challenging handling or an adverse decision

A reporter may challenge unsafe handling, loss of confidentiality, retaliation or a reasoned closure through AF-PL-017; the right to information about another person's discipline remains bounded. A person affected by a formal decision receives the applicable independent appeal route. Ordinary appeals use a three-person independent panel, normally filed within 30 days of notification and determined within 60 days of receipt. Original investigators, reviewers and decision makers shall not determine the same appeal. New material wrongdoing may still be reported after those administrative periods.

15.2 No internal exhaustion requirement

Nothing requires a person to exhaust AF channels, obtain AF permission or give advance notice before making a lawful report to an authority or exercising a protected remedy. AF shall not require withdrawal of such a report, waiver of a legally protected reward, or a settlement term obstructing lawful disclosure. Internal processing does not stop or extend an external filing deadline. Public disclosure protections and controlled-information restrictions depend on the actual law; provide accurate independent advice rather than promising unrestricted public release or universal immunity.

16 Partners, chapters and supply chains

16.1 Contractual implementation

Relevant partner, chapter and supplier terms shall provide safe reporting, prompt escalation, evidence preservation, non-retaliation and cooperation within the actual contractual scope. Authorized operators shall also comply with AF-SR-001 and applicable technical clocks. Do not make a concern depend on the local manager first approving it. A partner's investigation may contribute evidence, but AF shall independently examine its own affected authority, public claims and oversight duties. Commercial dependence on a provider shall not defeat necessary protective action.

16.2 Reporter transfers and multiple organizations

Before sharing a case with another entity, establish lawful purpose, minimum data, receiving competence, conflicts, confidentiality, protection and safe communication. Do not send the reporter's identity to an implicated employer by default. One coordinated investigation may support several remedies when lawful, but each entity retains its own authority and obligations. At partner closure, preserve custody, outstanding protection plans, technical decisions and access to remedies; a contract end is not permission to destroy a protected case.

17 Records, privacy and retention

17.1 Separated case architecture

Maintain a minimal case register, a separately protected identity/contact file, the evidence and investigation dossier, the reasoned decisions and the remediation record. Access shall be role-based and logged, including necessary administrator access. Use AF-FR-017 and the annex modules without copying sensitive narratives into general dashboards. AF-PL-018 applies to notices, lawful basis, rights requests, international access and processor arrangements. A respondent's access request does not automatically entitle them to a reporter's identity; consider the actual rights and lawful redaction separately.

17.2 Necessary retention and disposal

Necessary R09 case and decision evidence follows the AF default of seven years after closure or the last related decision, subject to applicable law, documented necessity and holds. Corporate resolutions remain permanent. This is not a blanket seven-year instruction for every allegation, irrelevant attachment or incidental personal detail. Delete or isolate clearly irrelevant data promptly through authorized handling; select the least necessary reliable record for the justified period. Review holds at least every six months and after material change, preserving a lawful disposal record.

18 Capability, monitoring and improvement

18.1 Training and channel assurance

Train recipients, supervisors, investigators and decision makers on confidentiality, retaliation, fair interviewing, case separation, technical escalation and the limits of authority. Conduct scenario-based learning at induction and after material change. As new AF implementation controls, test ordinary and bypass routes before launch and at least quarterly, including a failed delivery and handler-conflict scenario. A test shall be labeled Exercise and shall not be counted as a genuine report. Correct inaccessible or insecure channels before relying on them.

18.2 Oversight and effectiveness

Report de-identified quarterly information on received issues, timely triage, acknowledgments, unresolved risks, confidentiality incidents, retaliation concerns, findings and verified remedies. Distinguish allegation, substantiation and closure; low report counts do not prove a safe culture. The Ethics and Impartiality Committee shall receive necessary unaltered findings within its mandate. Audit the process annually under AF-HB-009 and review this policy at least annually and after a serious failure. Do not incentivize managers to reduce report numbers or maximize substantiation rates.

19 Adoption, interpretation and continuing protection

19.1 Effective operation

Record the actual approval, effective date, responsible people, channel directory, jurisdiction review, resources and readiness tests under AF-FR-001 and AF-ML-001. First Edition and the publication date identify this text; they do not establish a functioning hotline or completed organizational adoption. Existing cases shall receive a documented transition preserving accrued rights, evidence and earlier protective obligations. A change cannot retrospectively make an honest report unprotected.

19.2 Non-waiver and resolution of conflicts

A form, local arrangement, confidentiality agreement or website cannot reduce a controlling constitutional, technical or legal protection. Resolve genuine conflicts through competent independent review and the proper change process. A severed invalid provision shall not be replaced by an invented power. Continuing confidentiality, non-retaliation, correction and record duties survive assignment or membership exit to the extent lawfully applicable. Annex H provides the source and release record.

Annex A — Whole-federation concern and routing matrix

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Use the nature of the concern and any urgent protective need, not the reporter's preferred label alone. Preserve separate issues and original timestamps.

Concern coverage

Activity / concern	Primary route and necessary linked action
Governance, elections and appointments	Protected report for fraud, pressure or obstruction; constitutional/election remedy retains its own authority and dates.
Membership and representation	Complaint/appeal for an individual admission or status error; protected route for corruption, retaliation or systemic exclusion.
Standards and committee work	Protected report for manipulated evidence, hidden interests or suppressed objections; technical change uses its separate approval process.
Recognition, accreditation and conformity	Protect affected scope; notify the scheme operator; investigate integrity separately from the independent technical status decision.
Education and personnel examinations	Secure exam evidence; protect learners; separate marking appeal from cheating, coercion or compromised independence.
Events, visits and demonstrations	Immediate safety/safeguarding response; protected conduct investigation; separate refunds or service complaints.
Awards, competitions and grants	Preserve original eligibility and scores; investigate influence or fabricated submissions; use the applicable merit-review route.
Research and public-benefit work	Examine fabrication, plagiarism, concealed adverse results, misuse of data or funds; preserve the scientific record.
Finance, procurement and investments	Protect payments and records; independent financial review; no assumed financial-service authority.
Data, security and controlled technology	Activate incident response and legal notification analysis immediately; safe evidence route, not unrestricted upload.
Arbitration and expert services	Institutional misconduct may be reported; no corporate appeal of an arbitral merits award; preserve external rights.
Chapters, contractors and supplier tiers	Use AF connection and contract scope; safe bypass of an implicated local party; independent AF oversight of affected services.
Retaliation against any participant	Separate urgent protected case and protection plan; the original allegation need not first be proven.
Unrelated external dispute	Explain AF limits; identify a competent route where possible; do not transfer identities unnecessarily.

Annex B — Reporting-channel deployment and safe intake

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

WB-B01 | Verified channel directory

Field	Instruction and entry space
Protected written route	Actual address/portal, named custodian and deputy, monitoring hours, safe response mechanism and last test. Record: _____
Oral and private meeting route	Actual telephone or appointment method; language support; record/consent arrangement; safe alternatives. Record: _____
Independent bypass	Actual Ethics and Impartiality Committee or external recipient; conflict-screened routing outside implicated leadership. Record: _____
Urgent instructions	Relevant emergency/competent authority route, hours limitations and notice that AF is not an emergency service. Record: _____
Anonymous option	Actual technology, two-way capability, metadata limits and instructions; do not advertise unimplemented anonymity. Record: _____
Secure evidence route	Permitted information classes, authentication, upload restrictions and controlled-technology escalation. Record: _____
Launch verification	Test receipt, backup handler, access separation, accessibility, failed delivery and confidential response; date/approver. Record: _____

WB-B02 | Reporter intake

Field	Instruction and entry space
Case and receipt	ID, actual receipt time/zone and channel; whether linked cases exist. Record: _____
Safe contact	Optional name/contact, safe time/medium, representative, anonymity or confidentiality needs. Record: _____
Concern	What happened, when, where, parties/AF link, direct facts versus uncertainty. Record: _____
Protection and evidence	Immediate danger, retaliation concerns, available lawful evidence; do not seek restricted uploads by default. Record: _____

The form is optional for the reporter. Staff shall accept meaningful reports in other forms and complete the necessary internal record without changing the reporter's account.

Annex C — Triage and investigation record

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

WB-C01 | Triage, mandate and evidence plan

Field	Instruction and entry space
Immediate risk	Safety, safeguarding, retaliation, evidence destruction, privacy, technical status and required urgent action. Record: _____
Authority and routing	AF link, independent recipient, applicable jurisdictions, linked proceedings and external reporting obligations. Record: _____
Conflict clearance	Who is implicated; appointing independence; investigator/expert competence; excluded people and access restrictions. Record: _____
Allegations and criteria	Number each allegation; identify requirement, possible evidence and applicable evidential standard before determination. Record: _____
Investigation methods	Documents, interview plan, technical review, lawful access, preservation, expected milestones and limitations. Record: _____
Response safeguards	Respondent notice, meaningful evidence summary, representation, protected response period and any lawful notification delay. Record: _____
Evidence log	Item ID/source/date/custodian, acquisition method, original location, integrity check and access history. Record: _____
Outcome and referrals	Facts, counter-evidence, uncertainties, finding by allegation, authorized remedy/referral and actual decision time. Record: _____

Necessary additional pages shall retain the case ID and version. A technical adviser's conclusion is not itself a disciplinary decision; a disputed original fact shall not be overwritten.

Annex D — Protection and anti-retaliation plan

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Risk indicators and controls

Indicator	Proportionate response
Supervisor or budget owner is implicated	Independent contact and evidence custody; exclude the person from selecting handlers or protection decisions.
Changed duties, pay or invitations after reporting	Preserve chronology; independently review objective grounds and comparators; stop substantiated retaliatory treatment.
Threatened disclosure or doxxing	Restrict identifying information; preserve threat evidence; safety/security escalation and lawful external assistance.
Reporter employed by a partner	Assess safe contractual intervention without sending identity to the employer by default; explain AF's authority limits.
Anonymous reporter and no reply channel	Investigate available facts; protect potentially affected groups; document communication limits.
Serious technical danger	Protect the actual activity and status under controlling scheme rules; do not wait for the personnel investigation.

WB-D01 | Individual protection review

Field	Instruction and entry space
Needs and preferences	Risk, protected persons, safe contact, support requested and confidentiality constraints. Record: _____
Controls and authority	Action, responsible unimplicated person, scope, start, resources and review/expiry where relevant. Record: _____
Follow-up	At opening and material change; normally 7/30/90 days after closure where relevant. Record safety, retaliation and unmet needs. Record: _____
Closure of measures	Evidence that risks are controlled; reporter feedback where safe; ongoing duties and next route. Protection does not expire automatically. Record: _____

Annex E — Timetable, notifications and worked chronology

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Time control

Action	AF baseline / source boundary
Credible urgent protection	Immediately on recognition; legal and AF technical notifications retain their separate earlier clocks.
Initial documented triage	Within one calendar day from receipt: new administrative control; protective action may be earlier.
Acknowledgment	Within five calendar days from receipt where a safe response route exists; AF-PR-019.
Initial substantive response	Within 30 calendar days from receipt; constitutional complaint interface.
Ordinary determination	Normally within 60 calendar days from receipt; reasoned extensions and progress at least each 30 days.
Member discipline response	At least 21 calendar days; AF-CON-001 Article 7, not shortened by ordinary case targets.
Director-removal notice	At least 30 calendar days plus other Article 13 safeguards; no new removal authority.
Ordinary appeal	Normally 30 days to submit after notified decision; 60 days to determine after receipt; AF-PL-017.
External filing limits	Separate jurisdiction-specific clocks. AF handling does not toll, extend or replace them.

Synthetic chronology: receipt 30 September 2026; documented triage by 1 October, acknowledgment by 5 October, substantive response by 30 October, ordinary determination by 29 November. These are calendar-day calculations for the example, not historic AF events. Record precise time/zone where material. A serious concern identified on receipt still requires immediate action.

Do not use “awaiting complete file”, case transfer or a later report date to restart the initial clock. An exceptional investigation extension does not extend a credential, defer an urgent notice or reduce a respondent’s protected time.

Annex F — Communication and partner terms

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Model acknowledgment: “We received your concern on [actual date/time] and registered it as [case ID]. Your safe-contact preferences are [confirmed arrangement]. [Unimplicated role] will handle the next stage. We will protect your information on a need-to-know basis subject to lawful limits. Please do not send controlled technical or unnecessary personal material until we confirm a suitable route. Contact [verified route] promptly about danger, evidence loss or retaliation. Internal handling does not prevent lawful external reporting or extend external deadlines.”

Model progress/extension: “We have completed [actual steps]. [Specified work] remains because [recorded reason]. The revised expected date is [date]; next update is [date]. Existing protection measures are [safe summary]. No conclusion should be inferred from the extension.”

Model closure: “The issues examined were [scope]. Our outcome is [finding by issue], based on [lawful summary]. [Action/owner/date] has been assigned; [verified or outstanding] effectiveness is recorded separately. This response does not disclose protected third-party discipline. You may raise a handling concern or an applicable appeal through [verified route]. Reporting and external rights remain available.”

Model partner clause: “The Provider shall maintain a safe route for concerns connected with its AF work; prohibit retaliation; promptly preserve and escalate material safety, integrity, privacy and authorization concerns; cooperate through lawful, minimum-information channels; and permit independent scrutiny within the agreement. No implicated person shall control their own investigation. This clause does not compel disclosure of information forbidden by law or require internal exhaustion before lawful external reporting. Separate scheme notifications and technical-status decisions retain their controlling timetable.”

Complete model fields with verified particulars before sending or signing. A confidentiality statement shall not promise immunity, absolute anonymity or a guaranteed outcome.

Annex G — Readiness tests and measures of effectiveness

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Exercise / review

Exercise / review	Expected evidence
A senior leader is the subject	A tested independent bypass; access and appointment decisions exclude that leader.
Anonymous technical concern	Evidence-based triage without identity pressure; safe two-way contact only if deployed.
Misrouted email with personal attachments	Restricted forwarding and original timestamp; minimized working copy and preserved necessary original.
Concern later not substantiated	No automatic malicious-report finding; safe outcome communication and continued retaliation check.
Controlled design file offered	Hold upload; authorized local/secure evidence method or recorded limitation.
Simultaneous appeal and misconduct	Linked cases, separate mandates, original times and technical protection.
Channel outage or handler departure	Safe alternative, custody transfer, actual chronology and tested restored access.

Measure: acknowledgment on time = on-time safe acknowledgments / reports for which acknowledgment was possible and due; also disclose reports without a safe contact route. Measure overdue cases, unresolved protection risks, confidentiality failures and verified systemic remedies separately. A zero denominator is Not applicable, not 100%. Synthetic example: 18 of 20 eligible acknowledgments = 90%; two other reports had no safe reply route and remain separately disclosed.

Training and testing shall not manipulate case volumes. Oversight receives necessary detail under protected access; public reporting uses carefully de-identified aggregate information.

Annex H — Source alignment, adoption and controlled release

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

This annex distinguishes established AF requirements from the additional implementation controls authored for this policy. It does not amend a source document, authenticate a historic approval or establish that a reporting channel, appointed officer or digital service is already operating.

Inherited AF requirements and interfaces

Source	Preserved requirement / implementation interface
AF-CON-001 Articles 7, 13, 22–24, 26, 28	Protected reporting, independent handling, constitutional discipline/remedies, records and annual assurance.
AF-PL-012; AF-PR-019; AF-FR-017	Accessible intake, five-day acknowledgment, ordinary 30/60-day appeals and protected case record.
AF-PL-013; AF-SR-001; AF 9100:2026	Conduct, technical independence, immediate protection and unchanged scheme-specific notifications/status.
AF-SC-001; AF-GD-003; AF-PR-014/015	Necessary retention, protected identity, lawful access, holds and incident response.

Additional controls in this edition

Control	Nature and approval boundary
One-day documented triage	New AF administrative control; immediate protective action is not delayed.
Quarterly channel tests; 7/30/90 protection follow-up	New operating checks, not statutory durations or an expiry of protection.
Expanded anonymous/safe-contact and partner modules	New implementation detail; actual facilities and agreements must be verified.
Reasonable-ground and mixed-motive safeguard	Express protective policy elaboration; more protective mandatory law remains controlling.

Controlled AF references: AF-CON-001; AF-QM-001; AF-ML-001; AF-PL-012; AF-PL-013; AF-PL-017; AF-PL-018; AF-PL-019; AF-PR-001; AF-PR-004; AF-PR-014; AF-PR-015; AF-PR-018; AF-PR-019; AF-SC-001; AF-GD-003; AF-HB-009; AF-FR-001; AF-FR-003; AF-FR-016; AF-FR-017; AF-SR-001; AF 9100:2026. Use the applicable current effective version. Where an older corporate instruction conflicts with the Constitution, record the conflict and complete the required controlled change; this file does not silently rewrite the earlier file. AF 9100:2026 remains unchanged.

Adoption and implementation record

Field	Instruction and entry space
Exact text	Record AF-PL-016, Whistleblowing Policy, First Edition, Revision 00, 30 September 2026 and the approved file identity. Record: _____
Authority and approval	Identify actual approving organ/delegation, decision, reviewers, date and authenticated signatories. Record: _____
Commencement and transition	Enter the real effective date; affected contracts, rights, documents and pending cases; notices and transition actions. Record: _____
Owners and channels	Identify competent role holders/deputies, independent escalation, actual monitored contacts and operating hours. Record: _____
Readiness evidence	Record training, secure access, channel/record tests, case rehearsal and remaining restrictions. No fictitious test result. Record: _____
Master List and review	Add the proposed entry only through AF-FR-001 and AF-ML-001; assign next review and implementation checks. Record: _____

Proposed Master List entry: AF-PL-016 | Whistleblowing Policy | Policy | First Edition | Revision 00 | 30 September 2026 | Approval/effectivity: enter actual record. R01 publication lineage; completed records follow their substantive record classes. Existing Master List and source files remain unchanged by delivery of this policy.