



AF-OM-9500-001

Cybersecurity Operations and Recovery Manual

Space / Aviation / Defense

FIRST EDITION

AF 9500 SUPPORTING DOCUMENT



Document identity and use

FIRST EDITION MANUSCRIPT - Prepared for Aerospace Federation review

Field	Controlled identity
Document	AF-OM-9500-001 - Cybersecurity Operations and Recovery Manual
Parent standard	AF 9500 - Aerospace Digital Systems, Software & Cybersecurity
Edition / language	FIRST EDITION / English master text
Family	Manuals
Primary source anchors	18-24, 29-40; Annexes G-J, L-N
Suggested local owner	Cybersecurity operations owner
Authority	Publisher approval and effective date are not assigned. Local use requires authorized adoption and completed parameters.

Use with the main standard

This document implements the identified AF 9500 clauses and annexes. Read the complete applicable requirements in the main standard. The source anchors are navigation references; a template does not replace technical judgement, evidence, permission or eligible approval.

AF-ML-9500-001 lists the complete supporting set. AF-CM-9500-001 maps the main clauses and annexes to working documents. AF-TP-9500-001 establishes the common local parameter baseline; add the relevant discipline profiles.

Record control

Identify the object, configuration, record owner and dates. Reference attachments by stable identifier and version. Keep superseded evidence and decisions traceable. Use the approved local retention, access and authentication arrangements. No technical limit, numerical limit, interval or acceptance value is assigned by a blank template.

Implementation model: Translate the stated responsibilities and controls into the actual organization. Informative examples remain explanatory; use approved programme-specific values for operational decisions.

1 Know the actual service and authority

Maintain AF-RG-9500-001 for assets, configurations, owners and dependencies. Confirm which functions affect safety, mission, product evidence, data and continuity. Operators shall know who can contain, change, restore and authorize use. Apply the approved technical profiles and local parameters to the actual environment.

1.1 Identity, trust and data

Use AF-PR-9500-014/015/016 for access, keys and data handling. Inventory references rather than secret values. Reconcile actual privileges and protect emergency or offline access. Maintain authoritative data meaning, freshness, purpose and restrictions through operation and recovery.

1.2 Configured environments

Use AF-PR-9500-017/018/022 to verify communication, platforms, cloud or industrial duties and secure configuration. Examine management paths and shared dependencies. Protect article-linked results and physical process state in production or test environments.

2 Manage changes and observations

Use AF-PR-9500-023 for updates. Verify authenticity, compatibility, operating conditions and recovery separately. Track every target through actual transition states. A package download or installation message does not establish confirmed operation.

2.1 Monitoring

Use AF-FR-9500-024 to define detection objectives, time quality, sources, coverage and response. Validate rules with representative data and measure relevant false alarms and misses. Keep blind spots and source loss visible. Automated actions shall remain within consequence-aware limits.

2.2 Vulnerabilities

Use AF-PR-9500-025 and AF-RG-9500-009. Assess actual component versions, exposure, paths and operational consequences. Set treatment and deadlines with eligible authority and documented interim controls. Verify deployed population closure rather than closing the case when a patch is published.

3 Respond without losing essential control

Use AF-FR-9500-026 to preserve incident chronology, facts, uncertainty and affected scope. Coordinate containment with physical and mission owners. Do not assume that removing power or network access is always the safest action.

3.1 Evidence and communication

Preserve provenance, integrity, custody and time uncertainty. Assess live collection for its effects on the target. Communicate known facts, restrictions and next-update conditions to appropriate recipients through authorized routes. Avoid treating hypotheses as confirmed causes.

3.2 Recovery and reconciliation

Use AF-PR-9500-027 and AF-SC-9500-005. Restore trusted identities, keys, artifacts, configuration and data. Reconcile pending commands, transactions, privileges, product results and issued decisions. Compare actual recovery time and state with approved objectives. Return to service and incident closure require separate accountable conclusions.

4 Maintain people, support and retirement

Remote sessions shall have bounded purpose, targets, actions and duration. Verify resulting configuration and terminate access. Shift handovers preserve active incidents, exceptions and blocked decisions. Practical competence and realistic intervention time support human controls.

4.1 Legacy and end of support

Use AF-FR-9500-028 and AF-RG-9500-013 for supported continued-use arguments. Demonstrate compensating controls and maintain withdrawal triggers. Supplier promises and prior operation do not establish present recoverability.

4.2 Retirement and assurance

Use AF-PR-9500-029 to remove unintended authority and verify data disposition. Reconcile inventory, subscriptions, shared credentials and residual duties. Use AF-PR-9500-030 for independent review, corrective effectiveness, metrics and record continuity.

Required evidence: Actual operational state, validated monitoring, configuration-specific treatment, consequence-aware response and demonstrated semantic recovery.