



AF-PL-9500-004

Resilient Operations, Updates and Incident Recovery

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-PL-9500-004 - Resilient Operations, Updates and Incident Recovery
Parent standard	AF 9500 - Aerospace Digital Systems, Software & Cybersecurity
Edition / language	FIRST EDITION / English master text
Family	Policies
Primary source anchors	29-35, 37
Suggested local owner	Accountable executive / policy 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 Keep superseded evidence and decisions traceable.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.

Interactive record: Complete the fields in a PDF reader that supports AcroForms. Save a working copy and verify that entries remain visible after reopening. Link controlled continuation sheets when space is insufficient; every row requires its own evidence and disposition. Typed names identify people but are not self-authenticating signatures.

1 Policy and accountable commitment

The organization shall maintain known operational configurations, safe update paths, validated monitoring and demonstrable recovery. Cybersecurity actions shall account for physical, safety and mission effects.

1.1 Controlled operation and change

Authorize deployment only for verified targets and prerequisites. Distinguish package transfer, installation, activation and confirmation. Keep mixed, failed and unreachable populations visible. Treat urgent fixes through an accountable technical route with justified interim restrictions.

1.2 Detection and response

Validate detection coverage and response feasibility. Preserve blind spots, false alarms and missed scenarios in performance claims. Assess vulnerabilities for actual configuration and consequence. Containment shall protect essential functions and retain evidence without assuming that every shutdown is safe.

1.3 Recovery and continued use

Exercise complete restoration, including identities, keys, data relationships, pending actions and actual function. Record achieved recovery time and state. Legacy exceptions shall have demonstrated controls, owners and withdrawal triggers. A running service shall not be treated as complete recovery or incident closure.

Required evidence: Actual configuration, update and monitoring records, consequence-aware response, verified recovery and bounded continued-use decisions.

Decision control: Availability, delivery acknowledgment or an untested backup shall not establish trustworthy operation.

2 Local adoption and accountable implementation

Organization, scope, policy owner and controlled local policy ID

Accountable executive; technical and decision authorities; eligible delegates

Implementation records, review triggers and unresolved dependencies

Authorized adoption, authentication reference and effective conditions