

FedRAMP Incident Communications Procedures

- **Release:** 25.11A
- **Published:** 2025-11-08
- **Designator:** ICP
- **Description:** Initial release of simplified 20x version of this existing FedRAMP policy.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x:**
 - This release is effective **2025-11-01** for 20x.
 - This policy applies to all FedRAMP 20x authorizations.
- **FedRAMP Rev5:**
 - This version does not apply to Rev5; the full Rev5 requirements related to this policy are documented in FedRAMP's Incident Communications Procedures.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119](#).
- FedRAMP-specific terms defined in [FRD-ALL \(FedRAMP Definitions\)](#) are italicized throughout this document for reference.

Background & Authority

Purpose

This set of requirements and recommendations converts the existing FedRAMP Incident Communications Procedures (https://www.fedramp.gov/resources/documents/CSP_Incident_Communications_Procedures.pdf) to the simpler FedRAMP 20x standard style and clarifies the expectations for FedRAMP 20x.

The only notable change from the default Rev5 Incident Communications Procedures for 20x is the addition of a recommendation that incident information be made available in both human-readable and machine-readable formats.

Requirements

FRR-ICP

These requirements apply **ALWAYS** to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-ICP-01

Applies to: Low, Moderate, High

Providers MUST responsibly report *incidents* to FedRAMP within 1 hour of identification by sending an email to fedramp_security@fedramp.gov or fedramp_security@gsa.gov.

FRR-ICP-02

Applies to: Low, Moderate, High

Providers MUST responsibly report *incidents* to all agency customers within 1 hour of identification using the *incident* communications points of contact provided by each agency customer.

FRR-ICP-03

Applies to: Low, Moderate, High

Providers MUST responsibly report *incidents* to CISA within 1 hour of identification if the incident is confirmed or suspected to be the result of an attack vector listed at <https://www.cisa.gov/federal-incident-notification-guidelines#attack-vectors-taxonomy>, following the CISA Federal Incident Notification Guidelines at <https://www.cisa.gov/federal-incident-notification-guidelines>, by using the CISA Incident Reporting System at <https://myservices.cisa.gov/jrf>.

FRR-ICP-04

Applies to: Low, Moderate, High

Providers MUST update *all necessary parties*, including at least FedRAMP, CISA (if applicable), and all agency customers, at least once per calendar day until the *incident* is resolved and recovery is complete.

FRR-ICP-05

Applies to: Low, Moderate, High

Providers MUST make *incident* report information available in their secure FedRAMP repository (such as USDA Connect) or *trust center*.

FRR-ICP-06

Applies to: Low, Moderate, High

Providers MUST NOT irresponsibly disclose specific sensitive information about *incidents* that would *likely* increase the impact of the *incident*, but MUST disclose sufficient information for informed risk-based decision-making to *all necessary parties*.

FRR-ICP-07

Applies to: Low, Moderate, High

Providers MUST provide a final report once the *incident* is resolved and recovery is complete that describes at least:

1. What occurred
2. Root cause
3. Response
4. Lessons learned
5. Changes needed

FRR-ICP-08

Applies to: Low, Moderate, High

Providers SHOULD use automated mechanisms for reporting incidents and providing updates to all necessary parties (including CISA).

FRR-ICP-09

Applies to: Low, Moderate, High

Providers SHOULD make *incident* report information available in consistent human-readable and *machine-readable* formats.
