SAMPLE - FICTIONAL - NOT A REAL INCIDENT

IronWiFi FedRAMP 20x sample: Initial Incident Report (IEC-CSO-IIR)

> SAMPLE - FICTIONAL - NOT A REAL INCIDENT. Illustrative format example only, published in the IronWiFi Trust Center for FedRAMP 20x review. Does not describe any real IronWiFi, customer, tenant, employee or federal agency event. IronWiFi is pursuing FedRAMP 20x Class A and is not FedRAMP Certified.

Human-readable twin of `fedramp-20x-sample-incident-report-initial.json`. Both files follow the FedRAMP Incident Report JSON Schema `fedramp-incident-report-schema-2026-06-24.json` (version 0.2.1, https://www.fedramp.gov/schemas/fedramp-incident-report-schema-2026-06-24.json). Rules: https://www.fedramp.gov/2026/reference/20x/b/incident-evaluation-and-communication/

Report issued (fictional): 2026-03-12T16:00:00Z

Report header

Schema field	Value
`reportType`	Initial
`providerTrackingId`	SAMPLE-IR-2026-0001-FICTIONAL
`certificationPackageOverviewUri`	https://www.ironwifi.com/fedramp/ironwifi-fedramp-public.json
`federalIncidentCoordinator`	SAMPLE ONLY: Jane Q. Coordinator <federal-ir-coordinator@example.com>; +1-555-0100

1. Incident description (`incidentDescription`)

SAMPLE - FICTIONAL - NOT A REAL INCIDENT. A staging support-console misconfiguration allowed an unauthorized engineering role to run read-only queries against RADIUS authentication-event metadata (usernames, device identifiers, NAS identifiers, timestamps; no passwords, EAP secrets, shared secrets or private keys) for one fictional federal pilot tenant (agency.example.gov). Access was limited to a US-region analytics replica. Treated as a FedRAMP Reportable Incident under IEC-CSO-EFR because confidentiality of federal customer data was potentially affected. Status at time of report: contained; scope still being confirmed.

2. Timeline (`timeline`)

Schema field	Value
`startedAt`	2026-03-12T14:05:00Z
`detectedAt`	2026-03-12T14:38:00Z

SAMPLE - FICTIONAL

Schema field	Value
`detectionSource`	SAMPLE: Privileged-access monitoring alert on the staging support console (fictional alert rule SAMPLE-PRIV-QUERY-SPIKE)
`evaluationCompletedAt`	2026-03-12T15:10:00Z

`occurredAt`	`milestoneDescription`
2026-03-12T14:05:00Z	SAMPLE: Misconfiguration introduced during a fictional staging role-template change.
2026-03-12T14:38:00Z	SAMPLE: Detection via privileged-access monitoring; on-call engineer paged.
2026-03-12T14:55:00Z	SAMPLE: Role revoked; misconfigured template rolled back; affected queries stopped.
2026-03-12T15:10:00Z	SAMPLE: FedRAMP reportability evaluation completed (possible confidentiality impact; integrity and availability not indicated).
2026-03-12T16:00:00Z	SAMPLE: Initial Incident Report (IEC-CSO-IIR) issued.

3. Potential Agency Impact N-rating (PAIN), IEC-CSO-EFI (`potentialImpact`)

Schema field	Value
`historicalRating`	3
`currentRating`	3
`evaluationNotes`	SAMPLE IEC-CSO-EFI: Estimated PAIN-3 (likely disruptive customer effect on 1 fictional agency) because authentication-event metadata for that agency's tenant may have been exposed. Estimated promptly, so the IEC-CSO-DPR default of PAIN-5 does not apply. PAIN-3 sets a 6-hour window for this Initial report; it was issued 50 minutes after the evaluation completed.

4. Functional impact (`functionalImpact`)

SAMPLE: Potential confidentiality impact to authentication-event metadata for one fictional federal pilot tenant. No integrity impact to RADIUS/802.1X authentication decisions. No availability impact. Impacted data types (fictional): usernames, device identifiers, NAS identifiers, timestamps. Not impacted: passwords, EAP method secrets, RADIUS shared secrets, private keys, payment data. Whether any data left the staging environment is still under review.

SAMPLE - FICTIONAL

5. Recovery plan (`recoveryPlan`)

SAMPLE (estimated): (1) Containment complete at 2026-03-12T14:55Z (role revoked, template rolled back). (2) Review query logs for any destination outside the staging environment, estimated complete by 2026-03-13T18:00Z. (3) Add an automated check that blocks role templates without an environment guard, estimated by 2026-03-14. (4) Verify recovery and issue the Final Incident Report within 3 business days of resolution. Ongoing Incident Reports at least every business day until then.

6. Likely affected customer agencies (`affectedAgencies`)

- SAMPLE ONLY: Fictional Pilot Agency (agency.example.gov), NOT a real agency

Notification parties (sample)

Under the IEC-CSO rules a real report goes to FedRAMP (fedramp_security@fedramp.gov), to affected agencies through their own incident reporting procedures, and to all necessary parties as an update in the provider's Trust Center. This sample was not sent to FedRAMP's security inbox or to any agency; it is published only as a format example.

End of SAMPLE - FICTIONAL - NOT A REAL INCIDENT.

SAMPLE - FICTIONAL