EDUC ALLIANCE

FEDERATED IDENTITY INCIDENT RESPONSE PROCEDURE

SIRTFI v2 Compliance & Operational Framework

Target Entity / Service Provider:	https://disco.educalliance.eu/sp
Document Reference:	EDUC-SEC-SIRTFI-PRO-v1.0
Compliance Standards:	REFEDS SIRTFI v2 | Spanish National Security Framework (ENS - Medium Level)
Hosting & Admin Lead:	Universitat Jaume I (UJI) - Castelló de la Plana, Spain
Effective Date / Status:	08 October 2026 | Version 3.0 (Final version)

1. Executive Summary & Quality Assurance Context

In accordance with the ongoing Quality Assurance review of federation metadata within research and education identity federations (such as DFN and eduGAIN), this document formally defines the incident response procedures and security controls for the EDUC Alliance Service Provider ("https://disco.educalliance.eu/sp").

The Service Provider currently carries the REFEDS Data Protection Code of Conduct (CoCo v2) Entity Category. To maintain this category in federation metadata registers, member organisations are required to implement and self-attest conformance with the REFEDS Security Incident Response Trust Framework for Federated Identity (SIRTFI v2). This document serves as the official operational manual and self-attestation baseline for EDUC Alliance.

> **[SIRTFI v2 MANDATE]** *Per REFEDS CoCo v2 specifications, support for SIRTFI v2 is strongly recommended to ensure cross-organisational security incident coordination, accurate log traceability, and prompt threat containment across federated identity trust networks.*

2. Purpose, Scope & Legal Alignment

2.1 Scope

This procedure applies to all operational security processes, identity data flows, and infrastructure components supporting the central EDUC Alliance authentication and discovery services, specifically covering the Service Provider entity URL https://disco.educalliance.eu/sp and all associated identity integration points across member institutions.

2.2 Legal & Regulatory Basis

All security controls and data processing activities executed under this procedure strictly align with the legal frameworks governing EDUC Alliance:

- **Public Task & Employment Context (GDPR):** Personal data processing for authentication and access control relies on GDPR Article 6(1)(e) for students and third parties, and Article 88 (read alongside relevant national employment laws) for university staff.
- **Technical Support & User Assistance:** Technical logs and contact data processed during support requests are handled under explicit user consent (GDPR Article 6(1)(a)).
- **Spanish National Security Framework (ENS):** The platform infrastructure is hosted and managed by Universitat Jaume I (UJI) under the ENS Medium Level security standard pursuant to Royal Decree 311/2022 of 3 May.
- **Cookie & Session Management:** Session cookies stored on user devices strictly adhere to Article 22(2) of Spanish Law 34/2002 (LSSICE).

3. Organisational Governance & Escalation Contacts

EDUC Alliance comprises eight partner universities under a joint controller governance framework. Technical infrastructure management is centralized at Universitat Jaume I (UJI).

3.1 Controller Structure

Role	Institution	Contact / DPO Email
Administrator Controller	Universitat Jaume I (UJI) - Spain	dpd@uji.es
Processor Controller	University of Potsdam - Germany	datenschutz@uni-potsdam.de
Processor Controller	University of Cagliari - Italy	dpo@unica.it
Processor Controller	Masaryk University - Czech Republic	poverenec@muni.cz
Processor Controller	University Paris Nanterre - France	dpo@parisnanterre.fr
Processor Controller	University of Pécs - Hungary	adatvedelem@pte.hu
Processor Controller	University of Rennes - France	dpo@univ-rennes.fr
Processor Controller	University of South-Eastern Norway	postmottak@usn.no

3.2 Published Operational Security Contact [SIRTFI Section 3.6]

In compliance with SIRTFI v2 section 3.6, EDUC Alliance maintains a dedicated, non-publicly archived security contact to handle security incident reports from federation members:

- **Security Contact Function:** EDUC Alliance Security Response Team (UJI CSIRT)
- **Operational Security Email:** csirt@educalliance.eu

- **Publication Channel:** Published in SAML Entity Metadata via DFN MDV using REFEDS Security Contact Schema Extension.

4. Operational Security Assertions [OS]

To fulfill SIRTFI v2 Normative Assertions for Operational Security, EDUC Alliance self-attests to the following operational security controls:

- **[OS1] Patch Management:** Operating system and application software security patches are monitored continuously and applied in a timely manner according to risk severity. High-severity patches affecting federated authentication endpoints are applied within 48 hours of release.
- **[OS2] Vulnerability Management:** A continuous vulnerability management process is maintained across all servers hosting the Service Provider. Regular vulnerability scanning, dependency auditing, and configuration reviews are conducted in alignment with ENS Medium-level controls.
- **[OS3] Threat Intelligence & Intrusion Detection:** System components employ real-time log monitoring, firewall filtering, and threat intelligence feeds to detect potential intrusions or unauthorized credential usage promptly.
- **[OS4] Rapid Access Revocation:** The platform retains tools and procedures to suspend, modify, or terminate a user's access rights or identity sessions in a timely manner upon receiving notification of compromised credentials or suspicious activity.
- **[OS5] Contactability of Owners & Users:** Contact pathways exist to reach Service Owners (as defined by ITIL) and system users across all member universities whenever operational or security issues arise.
- **[OS6] Incident Response Capability:** An operational security incident response capability exists with explicit authority to contain, isolate, mitigate, and remediate security incidents affecting federated services.

5. Federated Incident Response & Collaboration Workflow [IR]

When a security incident occurs that threatens or involves federated identity transactions, EDUC Alliance executes the following multi-stage incident handling procedure:

5.1 Incident Response Lifecycle

- **Stage 1: Identification & Triage [IR1]:** Incident reports received via csirt@educalliance.eu or automated alerts are acknowledged immediately. Triage determines severity, affected infrastructure, and whether federated credentials are involved. Reporting the incident to the competent authorities within each concerned country is strongly recommended, if not mandatory by local laws.
- **Stage 2: Immediate Containment [OS4]:** The security team isolates affected services, revokes compromised user sessions, and blocks malicious source IPs to prevent lateral spread into federated Identity Providers or Service Providers.

- **Stage 3: External Notification [IR3]:** If an investigation indicates that external SIRTFI-compliant entities (Identity Providers or federated SPs) are involved, the EDUC security contact will promptly notify the security contacts of affected entities and federation operators.
- **Stage 4: Active Assistance & Collaboration [IR2, IR4]:** EDUC Alliance commits to responding to requests for assistance from other SIRTFI participants in a timely manner and actively collaborating in cross-organisational incident investigations.
- **Stage 5: Data Protection & Privacy Compliance [IR5]:** All incident response investigations respect user privacy in accordance with GDPR principles and the EDUC Privacy Policy. Log evidence shared externally is minimized to necessary incident indicators.
- **Stage 6: Remediation & Post-Mortem:** Vulnerabilities are remediated, root causes documented, and lessons learned integrated into system configurations before restoring full operational status.

6. Information Disclosure & Traffic Light Protocol (TLP) [IR6]

In compliance with SIRTFI v2 assertion [IR6], all security incident communications, intelligence sharing, and coordination messages exchanged with external federation members strictly adhere to the FIRST Traffic Light Protocol (TLP v2.0):

TLP Designation	Access / Sharing Restriction	Operational Application
TLP:RED	For official eyes only; strictly restricted to named individual recipients.	Used for sensitive compromise details containing specific credentials or active zero-day exploit details.
TLP:AMBER	Limited disclosure; restricted to organization members & affected partners who need to know.	Shared with specific IdP security teams whose users are impacted by a federated incident.
TLP:GREEN	Community wide; shareable within the Research & Education (R&E) federation community.	Used for general threat indicators, malicious IP lists, or federated vulnerability advisories.
TLP:CLEAR	Public release; no restriction on disclosure.	Published post-incident summaries or general compliance updates.

7. Traceability, System Logging & Data Retention [TR]

To enable accurate forensic investigation into federated security incidents, EDUC Alliance satisfies all SIRTFI traceability requirements:

- **[TR1] Comprehensive System Logging:** The platform records relevant system-generated log data including accurate UTC timestamps (synchronized via Network Time Protocol - NTP), source IP addresses, user identifiers (e.g. eduPersonTargetedID / persistent identifiers), and authentication outcome codes.

- **[TR2] 365-Day Retention Schedule:** In alignment with Section 4 of the EDUC Privacy Policy and ENS audit guidelines, log data is retained for 365 days from the time of the event. After 365 days, log files are automatically purged or permanently anonymised for statistical reporting.
- **Log Integrity & Confidentiality:** Log repositories are stored on secure, restricted-access servers hosted by UJI. Access is strictly limited to authorized system administrators and security analysts exclusively for operational and incident investigation purposes.

8. User Rules & Acceptable Usage Conditions [UR]

Federated access management requires clear communication to end-users regarding acceptable usage and access restrictions:

- **[UR1] Defined Terms of Use:** EDUC Alliance maintains clear rules and conditions governing platform usage, outlined in the platform Terms of Service and Privacy Policy. Unauthorised use, credential sharing, or malicious platform abuse is strictly prohibited and constitutes grounds for access suspension.
- **[UR2] User Notification Process:** Users are informed of usage terms and data handling rules prior to authenticating to https://disco.educalliance.eu/sp. Notification is delivered via mandatory login prompts and accessible privacy notices.