Ontoly

Building Emissions Reduction Standard (BERS)

Registry Security Disclosure Document

Version 1.0 | Final | 2 November 2026

1. Purpose

This document provides a summary of the security architecture, access controls, and incident response procedures for the Ontoly Registry. It is prepared for disclosure to the ICAO Secretariat and the Technical Advisory Body (TAB) upon request, in support of the BERS Program's application for CORSIA eligibility. This document satisfies the registry security disclosure requirements under the CORSIA Emissions Unit Eligibility Criteria.

2. Registry Architecture Overview

2.1 Platform

The Ontoly Registry is a cloud-hosted, web-based platform providing issuance, holding, transfer, cancellation, and retirement functionality for Building Emissions Reduction Units (BERUs). The registry is built on a modern technology stack designed for security, scalability, and auditability.

2.2 Hosting and Infrastructure

- **Cloud provider:** Enterprise-grade cloud infrastructure with SOC 2 Type II and ISO 27001 certified data centres.
- **Geographic redundancy:** Data is replicated across multiple geographic availability zones to ensure continuity of operations.
- **Encryption at rest:** All data stored in the registry database and document storage is encrypted using AES-256 encryption.
- **Encryption in transit:** All communications between users, the registry, and backend services use TLS 1.2 or higher.

3. Access Controls

3.1 Authentication

- **Multi-factor authentication (MFA):** Required for all registry accounts, including Building Representative accounts, buyer accounts, and administrative accounts.

Copyright © 2026 Ontoly. All rights reserved.

- **Password policy:** Minimum 12 characters with complexity requirements; passwords are hashed and salted using industry-standard algorithms (bcrypt/Argon2).
- **Session management:** Automatic session timeout after 30 minutes of inactivity; concurrent session limits enforced.

3.2 Authorization

- **Role-based access control (RBAC):** Access permissions are assigned based on user roles (Building Representative, Buyer, Verifier, Registry Administrator, System Administrator).
- **Principle of least privilege:** Users are granted only the minimum access necessary to perform their functions.
- **Administrative access:** Registry Administrator functions (issuance, label application, cancellation processing) require separate administrative credentials and are logged.
- **Separation of duties:** Critical operations (e.g., BERU issuance, cancellation processing) require approval from at least two authorized personnel.

4. Audit Trail and Logging

- **Immutable audit log:** All registry transactions (issuance, transfer, cancellation, retirement, label changes) are recorded in an append-only audit log that cannot be modified or deleted.
- **User activity logging:** All user logins, failed login attempts, permission changes, and administrative actions are logged with timestamps and IP addresses.
- **Log retention:** Audit logs are retained for a minimum of seven (7) years.
- **Log monitoring:** Automated monitoring alerts for suspicious patterns (e.g., multiple failed login attempts, unusual transaction volumes, out-of-hours administrative access).

5. Data Integrity

- **Database integrity:** Referential integrity constraints enforce consistency of BERU records, ensuring that no unit can exist in multiple states simultaneously (e.g., both active and cancelled).
- **Serial number uniqueness:** System-enforced uniqueness of BERU serial numbers across the entire registry. No duplicate serial numbers can be created.
- **Transaction atomicity:** Registry transactions (transfer, cancellation, retirement) are processed as atomic operations, preventing partial execution.
- **Automated reconciliation:** Daily automated reconciliation checks verify that total issued BERUs equal the sum of active, transferred, cancelled, and retired units.

6. Incident Response

Copyright © 2026 Ontoly. All rights reserved.

6.1 Incident Classification

Severity	Category	Examples
Critical	Data breach / unauthorized access	Unauthorized access to registry accounts; exfiltration of account holder data; unauthorized issuance or cancellation of BERUs
High	System compromise / integrity	Malware detection; unauthorized modification of transaction records; DDoS attack affecting availability
Medium	Suspicious activity	Multiple failed authentication attempts; unusual transaction patterns; policy violation by authorized user
Low	Minor / informational	Non-critical software vulnerability; configuration error; performance degradation

6.2 Response Procedures

- **Detection:** Automated monitoring systems and manual review processes to detect security incidents.
- **Containment:** Immediate containment measures to limit the scope and impact of the incident.
- **Notification:** For incidents affecting CORSIA participant account holders, notification within seventy-two (72) hours of breach confirmation (BERS Standard Section 15.3.2). ICAO Secretariat notification for material incidents.
- **Investigation:** Root cause analysis conducted for all Critical and High severity incidents.
- **Remediation:** Implementation of corrective measures to prevent recurrence.
- **Documentation:** Full incident report documented and retained in the incident log.

7. Business Continuity

- **Recovery Point Objective (RPO):** Maximum of 1 hour of data loss in the event of a system failure.
- **Recovery Time Objective (RTO):** Maximum of 4 hours to restore full registry operations.
- **Backup strategy:** Automated daily backups with geographic redundancy; backups tested quarterly.
- **Disaster recovery plan:** Documented and tested annually; includes failover to secondary infrastructure.

8. Ongoing Security Measures

- **Penetration testing:** Annual third-party penetration testing of the registry application and infrastructure.

Copyright © 2026 Ontoly. All rights reserved.

- **Vulnerability scanning:** Automated vulnerability scanning conducted weekly; critical vulnerabilities remediated within 48 hours.
- **Security updates:** System and application patches applied according to a documented patch management policy.
- **Employee training:** Annual security awareness training for all Ontoly personnel with registry access.

9. Data Retention

In accordance with BERS Standard Section 15.3.3, all documents and data relevant to CORSIA Eligible Emissions Units and cancellations shall be retained on an ongoing basis and for at least three (3) years beyond the end date of the latest compliance period in which the BERS Program is determined to be eligible.

10. Contact

Registry Security Inquiries: security@ontoly.org

General Registry Inquiries: registry@ontoly.org

11. Revision History

Version	Date	Author	Description
1.0	March 2026	Adam Doran	Initial publication for CORSIA TAB 2026 assessment. Republished on 2 November 2026 in the new Ontoly brand, with no change to content.

Copyright © 2026 Ontoly. All rights reserved.