
Certified Emissions Reduction Technologies Foundation

# INFORMATION SECURITY AND DATA PROTECTION POLICIES

*ISO/IEC 27001:2022-Aligned ISMS and GDPR-Baseline Privacy Framework*

Document ID: CERT-GOV-007
Version 1.0 (Draft for Consultation)
Date: 2 July 2026
Classification: Public

## Document Control

| Field | Detail |
|---|---|
| Document ID | CERT-GOV-007 |
| Title | CERT Information Security and Data Protection Policies |
| Version | 1.0 (Draft for Consultation) |
| Status | Draft – pending Board adoption and public consultation |
| Owner | Secretariat (CISO / DPO) |
| Approver | Board of Trustees |
| Review cycle | Annually |
| Related documents | CERT-FDN-001; CERT-GOV-001 (§8); CERT-GOV-006; CERT-REG-001; CERT-TEC-001/002/003 (planned) |

## Version History

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 2026-07-02 | CERT Founding Secretariat | Initial draft for founding Board review and public consultation. |

## Table of Contents

# 1. Purpose, Scope and Standards Alignment

**1.1** The registry ledger is CERT's crown-jewel asset: if issuance, ownership, or retirement records can be manipulated or lost, every credit is suspect. This document establishes (Part A) the Information Security Management System (ISMS) and (Part B) the Data Protection and Privacy framework referenced in the Charter as CERT-GOV-007.

**1.2** Scope. All information assets, systems, personnel, and third parties involved in CERT operations, including the registry platform, MRV data pipelines, document management, corporate IT, and outsourced services.

**1.3** Alignment. Part A is designed for certification against ISO/IEC 27001:2022 (including Annex A controls per ISO/IEC 27002:2022, with cloud and privacy controls); risk assessment follows ISO/IEC 27005 within the GOV-006 framework. Part B complies with India's Digital Personal Data Protection Act, 2023 (DPDP Act) as CERT's mandatory domestic regime, and additionally applies the EU GDPR standard as CERT's global baseline where stricter, given CERT's international participants. Mandatory privacy laws of project host countries are mapped in a compliance annex maintained by the DPO.

# PART A – INFORMATION SECURITY POLICY

## 2. Governance and Responsibilities

**2.1** The Board approves this Policy; the Audit, Risk and Finance Committee oversees security assurance (GOV-001 §8). A Chief Information Security Officer (CISO) owns the ISMS, reports to the Chief Executive with unrestricted escalation to the ARF Committee, and may not simultaneously own platform delivery.

**2.2** Every staff member and contractor completes security awareness training at onboarding and annually; developers receive secure-coding training.

## 3. Asset Classification

| Class | Examples | Baseline handling |
|---|---|---|
| Critical – Registry ledger | Issuance, transfer, retirement, serial records; buffer pool ledger | Immutable audit trail; dual control on privileged operations; cryptographic integrity protection; replicated storage |
| Confidential | Personal data; KYC files; pre-decision case files; security configurations | Encryption at rest and in transit; need-to-know RBAC; access logging |
| Internal | Draft documents, internal correspondence | Standard corporate controls |
| Public | Published standards, registry public views, methodologies | Integrity protection; availability targets |

## 4. Core Control Requirements

**4.1** Identity and access. Role-based access control aligned with segregation of duties (Charter 11.2); multi-factor authentication for all users; phishing-resistant MFA and just-in-time elevation for privileged access; quarterly access reviews; immediate revocation on role change or exit.

**4.2** Registry integrity. Every state-changing registry operation is written to an append-only, cryptographically chained audit log; serial numbers are generated deterministically with collision checks; issuance and retirement require four-eyes approval workflows; ledger reconciliations run daily with automated alerts.

**4.3** Cryptography. TLS 1.2+ for all transport; AES-256 or stronger at rest; keys in managed HSM/KMS with rotation and split ownership; digital signatures on certificates and official documents.

**4.4** Secure development. Version-controlled code; mandatory peer review; SAST/DAST and dependency scanning in CI/CD; segregated dev/test/production; no production data in test environments except anonymised.

**4.5** Vulnerability and patch management. Risk-rated remediation SLAs (critical: 7 days); annual independent penetration test of the registry platform, plus after material architectural change; a coordinated vulnerability disclosure channel for external researchers.

**4.6** Logging and monitoring. Centralised log management; 24/7 monitoring of registry-critical events; retention of security logs for at least 3 years; audit trail records of ledger operations retained permanently.

**4.7** Third parties. Cloud and service providers pass security due diligence proportionate to asset class; contracts include security, audit, breach-notification, and data-location clauses; critical providers reviewed annually.

**4.8** Physical and personnel. Background screening for staff with privileged registry access, to the extent lawful; clean-desk and device encryption; secured facilities for any on-premise assets.

## 5. Incident Response, Continuity and Resilience

**5.1** A documented incident response plan defines severity levels, roles, forensics, communication, and regulator/participant notification. Suspected ledger manipulation is treated as Severity 1: affected operations freeze, ARF Committee and Board Chair are notified within 24 hours, and an independent forensic review is mandatory.

**5.2** Continuity targets (per GOV-006 §7): registry RTO ≤ 24 hours, RPO ≤ 15 minutes; geographically separated replicas; at least annual failover and restore testing; ransomware-resistant (offline/immutable) backups.

**5.3** Material incidents are disclosed in the Annual Governance and Transparency Report; incidents affecting specific credits or accounts trigger direct participant notification under the Rulebook.

# PART B – DATA PROTECTION AND PRIVACY POLICY

## 6. Principles

**6.1** CERT processes personal data lawfully, fairly, and transparently; for specified purposes; minimised to what is necessary; accurately; retained no longer than needed; and protected per Part A (integrity and confidentiality), with demonstrable accountability.

**6.2** Transparency boundary. CERT's registry transparency obligations (Charter 15.1) concern project and credit data, which are published; personal data within project documentation (e.g., signatures, personal contact details, community member identities) is redacted from public versions unless consent or legal basis supports publication. Account-holder legal names of organisations are public; natural-person retail account details are not.

## 7. Roles and Records

**7.1** CERT acts as controller for registry, KYC, HR, and governance data, and documents any processor relationships. A Data Protection Officer (DPO) — who may be combined with the General Counsel function while CERT is small, provided no conflict arises — maintains records of processing activities, advises on impact assessments, and handles data subject requests.

## 8. Processing Requirements

**8.1** Lawful bases are documented per processing purpose (contract for account services; legal obligation for KYC/AML where applicable; legitimate interests for integrity investigations, balanced and documented; consent where relied upon, freely revocable).

**8.2** KYC and identity data. Identity verification data for account holders is collected proportionately, stored encrypted, accessed only by authorised compliance staff, and retained for 5 years after account closure or as legally required, then deleted.

**8.3** Data protection impact assessments are mandatory for new processing likely to create high risk, including satellite/remote-sensing workflows that could identify individuals, AI-assisted review of personal data, and any large-scale monitoring.

**8.4** AI processing. Where AI systems (CERT-TEC-003, planned) process personal data, outputs affecting individuals are subject to human review; models are not trained on confidential participant data without documented legal basis and contractual clearance.

**8.5** International transfers occur only with appropriate safeguards (adequacy, standard contractual clauses, or equivalents), mapped by the DPO.

## 9. Data Subject Rights and Breaches

**9.1** Data subjects may request access, rectification, erasure (subject to registry-integrity retention duties, which are documented exceptions), restriction, portability, and objection. Requests are answered within 30 days.

**9.2** Personal data breaches are triaged under the incident response plan. CERT notifies the Data Protection Board of India and affected data principals as required by the DPDP Act and its rules, and applies the 72-hour authority-notification discipline of the GDPR baseline for breaches affecting individuals in jurisdictions where it applies.

# 10. Compliance, Audit and Review

**10.1** The ISMS undergoes internal audit at least annually and pursues ISO/IEC 27001:2022 certification within 24 months of registry launch. Privacy compliance is reviewed annually by the DPO with findings to the ARF Committee.

**10.2** This document is reviewed at least annually (security threat landscape moves faster than the three-year default). References: ISO/IEC 27001:2022; ISO/IEC 27002:2022; ISO/IEC 27005; EU GDPR; NIST SP 800-61 (incident handling); CERT-GOV-006; CERT-TEC-001/002/003 (planned).