P10 — Resilience, Security and Data Governance

SCD-P10 · Principle 10 of 10
Resilience, Security and Data Governance
“Sovereign data that can be lost is not sovereign.”
Governance Layer

Definition

Sovereign climate data requires an explicit governance framework specifying: (a) who has authority to read, write, modify, and delete data; (b) how data disputes are resolved; (c) backup and disaster recovery procedures; (d) security controls against unauthorised access or manipulation; (e) data retention and archiving policy; and (f) rules for data sharing with third parties. Governance must be documented and reviewed annually.

Rationale

Data sovereignty without governance is operational fiction. The Climate Data Steering Committee's Common Carbon Credit Data Model (2024) and the dMRV Working Group's Phase 2 Roadmap (2025) both identify data governance as the most under-addressed dimension of climate data infrastructure globally. For LATAM organisations, the additional risk is structural: most climate data is held in a single vendor system with no backup, no access log, and no recovery plan — meaning one vendor outage or relationship breakdown causes irreversible data loss.

Implementation Steps

1. Write a Data Governance Policy covering: access control (who can do what), dispute resolution, retention schedule, backup frequency, and sharing rules.
2. Implement role-based access: at minimum, separate read and write permissions.
3. Run automated backups to a system you control at least weekly; test recovery quarterly.
4. Maintain an access log: every read and write to sensitive climate data is recorded.
5. For shared data: use a Data Sharing Agreement (DSA) that specifies permitted uses, attribution requirements, and data return/destruction obligations.

Compliance Checklist

	Criterion	What it means

?	**Data Governance Policy written**	Document covers access control, disputes, retention, backup, and sharing.
?	**Role-based access implemented**	At minimum: separate read vs. write access for climate data systems.
?	**Automated backups running**	Weekly backup to a system you own, with quarterly recovery tests.
?	**Access log active**	All reads and writes to sensitive climate data are recorded with timestamp.

Regulatory References

- Climate Data Steering Committee — Common Carbon Credit Data Model (2024)
- dMRV Working Group Phase 2 Roadmap (Planet2050 × BioCarbon, 2025)
- GDPR Art. 5 (Data integrity and confidentiality) — applicable to EU-adjacent organisations
- ISO/IEC 27001 (Information Security Management) — international baseline

Recommended Tools and Platforms

Infisical (secrets management) Backblaze B2 / Rclone (backup) Keycloak (access control) Audit log frameworks

Keywords

data governance security resilience backup access control data sharing agreement ISO 27001

Related Principles: SCD-P04 · SCD-P08
Document ID: SCD-P10 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Governance and Social Legitimacy | **Source:** CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the Sovereign Climate Data Wiki, maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the BookStack REST API.

Revisión #2
Creado 2026-05-26 22:14:00 UTC por Angelica Diaz
Actualizado 2026-05-27 03:31:36 UTC por Angelica Diaz