

# The Data Governance Policy Model

Let's have a quick look at the Data Governance Policy Model — People, Process, and Technology — exactly as defined in NetHope's "Data Governance Toolkit," and how these three pillars work together to ensure responsible, effective data management.



## Description:

People are the backbone of Data Governance. This component defines the roles, responsibilities, and accountability needed to implement and maintain governance across organizations.

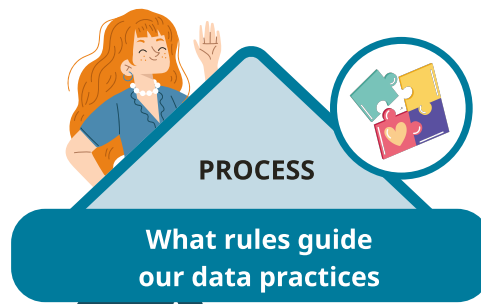
This list is intended as a guideline. Organizations may not have the exact same roles or titles.

## Key Roles:

- **Business Data Owner:** Accountable for a specific data domain; responsible for how data is used and protected.
- **Business Data Steward / Delegate:** Supports the Data Owner; ensures day-to-day implementation of governance controls.
- **Technical Data Owner & Technical Data Steward / Custodian:** Oversees system-level support, access, quality remediation, and data lifecycle safety.
- **Head of Data Governance:** Leads the Data Management Office; ensures governance strategy is applied across all solutions.
- **Data Governance Lead:** Writes and updates policies, standards, and guidelines; monitors good practices and reviews data requirements.

## Why It Matters:

Clear ownership reduces confusion, risk, and data quality issues while ensuring accountability across teams, not just IT. Without defined roles, data governance falls into the "everyone's responsibility means no one's responsibility" trap, leading to workarounds, blame, and disengagement.



## Description:

Process refers to the policies, standards, and guidelines that define how data is accessed, protected, used, shared, and evaluated.

## Core Policy Areas:

- **Data Access & Sharing:** Role-based permissions, conditions for internal & external data sharing.
- **Data Quality:** Ensures data is valid, reliable, precise, integral, and timely. (Aligned with the recognized 5 data quality standards)
- **Data Security:** Standards for protecting data throughout its lifecycle, including privacy and access controls.
- **Data Literacy:** Organization-wide guidelines on how to capture, store, share, and handle data responsibly.

## Why It Matters:

Processes provide consistency, reduce misuse, and align the organization with responsible data and AI practices. However, policies that are too complex, inaccessible, or disconnected from daily work become "shelfware" - ignored by teams who develop informal workarounds instead. Effective processes are designed WITH users, not just FOR them.



## Description:

Technology describes the systems, storage, infrastructure, and software that enable secure and effective data management.

## Key Focus Areas:

- Storage systems (cloud, on-premise, data lake, etc.)
- Metadata tools & data catalogues
- Identity & access management
- Security monitoring & audit logs
- Data validation & quality tools
- Infrastructure aligned with IT architecture

## Why It Matters:

Technology enforces the rules, secures the data, and operationalizes governance standards across the organization.

