Data Governance Framework Template 2026

Enterprise Data Solutions
Comprehensive Data Governance Framework

Version: 3.0 **Last Updated:** January 2026 **Type:** Framework Template

Website: EnterpriseDataSolutions.co.nz
Email: Contact@EnterpriseDataSolutions.co.nz

Table of Contents

Introduction

Purpose of This Framework

This Data Governance Framework Template provides a comprehensive, ready-to-use foundation for establishing and operationalizing data governance within your organization. It encompasses policies, procedures, templates, and best practices aligned with 2026 regulatory requirements and industry standards.

Who Should Use This Framework?

Stakeholder	Primary Use
Chief Data Officer (CDO)	Strategic governance direction and executive reporting
Data Governance Council	Policy approval and governance oversight
Data Stewards	Day-to-day data management and quality assurance
Data Owners	Domain accountability and decision-making
IT/Data Engineering	Technical implementation and infrastructure
Compliance/Legal	Regulatory alignment and audit preparation
Business Units	Understanding data responsibilities and access

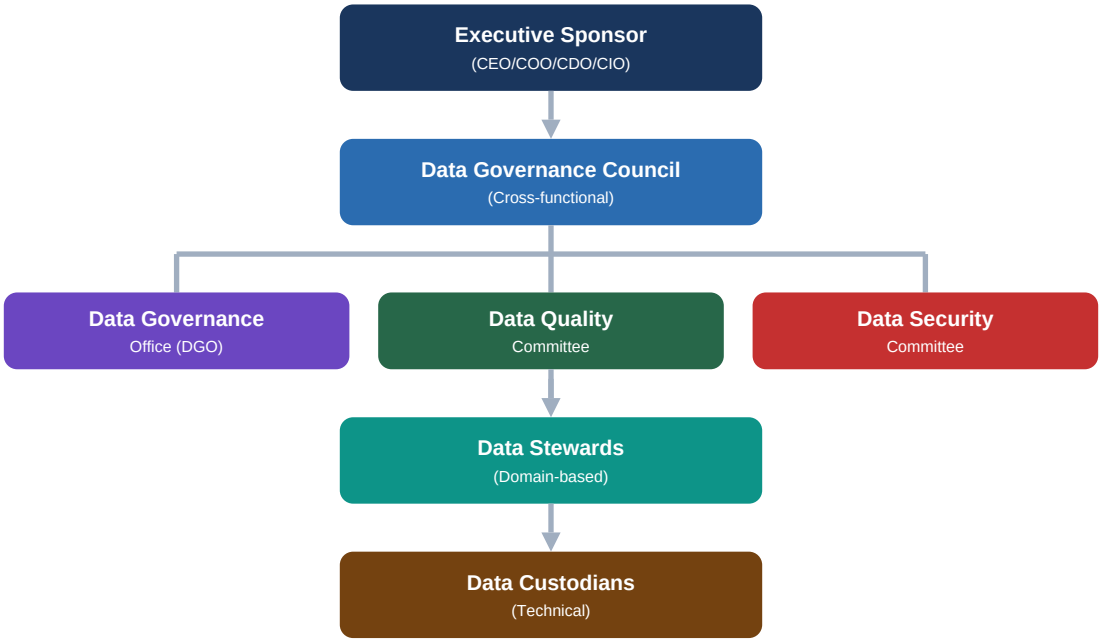
Framework Objectives

This framework enables organizations to:

- **Establish Accountability** - Clear ownership and responsibilities for data assets
- **Ensure Compliance** - Meet regulatory requirements (GDPR, CCPA, HIPAA, NZ Privacy Act)
- **Improve Data Quality** - Consistent standards and monitoring across the enterprise
- **Enable Data-Driven Decisions** - Trusted, well-governed data for analytics and AI
- **Mitigate Risk** - Proactive identification and management of data-related risks
- **Maximize Data Value** - Treat data as a strategic enterprise asset

Data Governance Operating Model

Governance Structure Overview



Governance Bodies

1. Data Governance Council

Attribute	Description
Purpose	Strategic oversight of enterprise data governance program
Membership	CDO (Chair), CIO, CFO, Business Unit Leaders, Legal, Compliance
Meeting Frequency	Monthly
Key Responsibilities	Policy approval, budget allocation, strategic priorities, issue escalation
Quorum	60% of members including Chair
Decision Authority	Policy changes, major investments, cross-functional disputes

2. Data Governance Office (DGO)

Attribute	Description
Purpose	Operationalize and sustain the data governance program
Membership	Data Governance Lead, Data Stewards, Data Architects, Analysts
Meeting Frequency	Weekly
Key Responsibilities	Policy implementation, steward coordination, metrics tracking, training
Reports To	Data Governance Council
Key Deliverables	Governance dashboards, policy updates, training materials

3. Data Quality Committee

Attribute	Description
Purpose	Oversee data quality standards, measurement, and improvement
Membership	Data Quality Lead, Domain Stewards, Data Engineers, Business Analysts
Meeting Frequency	Bi-weekly
Key Responsibilities	Quality standards, issue resolution, root cause analysis
Reports To	Data Governance Office
Key Deliverables	Quality scorecards, remediation plans, quality rules

4. Data Security Committee

Attribute	Description
Purpose	Ensure data protection, privacy, and security compliance
Membership	CISO, Privacy Officer, Data Governance Lead, Security Architects
Meeting Frequency	Monthly
Key Responsibilities	Security policies, access reviews, incident response, privacy compliance
Reports To	Data Governance Council
Key Deliverables	Security assessments, access reports, compliance certifications

Roles and Responsibilities

Role Definitions

Executive Sponsor

Category	Details
Title Examples	CEO, COO, CDO, CIO
Number Required	1 primary sponsor
Time Commitment	2-4 hours/month
Responsibilities	Champion data governance at executive level; Secure budget and resources; Remove organizational barriers; Set strategic direction; Hold leaders accountable
Success Metrics	Budget secured, executive engagement, barrier resolution time
Reports To	Board of Directors

Chief Data Officer (CDO)

Category	Details
Title Examples	Chief Data Officer, VP Data & Analytics, Head of Data
Number Required	1
Time Commitment	Full-time role
Responsibilities	Lead enterprise data strategy; Chair Data Governance Council; Oversee data governance program; Manage Data Governance Office; Report on data value and risks
Success Metrics	Governance maturity score, data quality metrics, compliance status
Reports To	Executive Sponsor / CEO

Data Owner

Category	Details
Title Examples	Business Unit Director, Department Head, Product Owner
Number Required	1 per data domain
Time Commitment	4-8 hours/month
Responsibilities	Accountable for data within their domain; Approve access requests; Define data quality requirements; Resolve data issues; Participate in governance forums
Success Metrics	Domain quality scores, access request turnaround, issue resolution
Reports To	Data Governance Council

Data Steward

Category	Details
Title Examples	Data Steward, Business Data Analyst, Domain SME
Number Required	1-3 per data domain
Time Commitment	20-50% of role
Responsibilities	Day-to-day data management; Define business rules and metadata; Monitor data quality; Coordinate with technical teams; Train business users
Success Metrics	Metadata completeness, quality issue response time, user satisfaction
Reports To	Data Owner

Data Custodian

Category	Details
Title Examples	Data Engineer, Database Administrator, Platform Engineer
Number Required	As needed per system
Time Commitment	Part of technical role
Responsibilities	Technical data management; Implement access controls; Execute data quality rules; Manage data infrastructure; Support data movement and integration
Success Metrics	System uptime, technical quality metrics, implementation velocity
Reports To	IT/Data Engineering Manager

Data Consumer

Category	Details
Title Examples	Business Analyst, Data Scientist, Report Developer, End User
Number Required	All data users
Time Commitment	As needed
Responsibilities	Follow data policies and procedures; Report data quality issues; Use data ethically and appropriately; Complete required training; Maintain data confidentiality
Success Metrics	Policy compliance, training completion, issue reporting
Reports To	Respective manager

Data Domain Ownership Matrix

Data Domain	Data Owner (Title)	Data Steward(s)	Systems of Record
Customer Data	VP Sales & Marketing	Customer Data Steward	CRM, Marketing Platform
Financial Data	CFO / Controller	Finance Data Steward	ERP, GL, AP/AR Systems
Employee Data	CHRO / HR Director	HR Data Steward	HRIS, Payroll System
Product Data	VP Product	Product Data Steward	PIM, PLM, Inventory
Operational Data	COO / VP Operations	Operations Steward	ERP, MES, WMS
Supplier Data	VP Procurement	Procurement Steward	SRM, Procurement System
Transaction Data	VP Finance	Transaction Steward	POS, Payment Gateway
Analytics Data	CDO / Analytics Lead	Analytics Steward	Data Warehouse, BI Platform

RACI Matrix Templates

Template Instructions

RACI Definitions:

- **R (Responsible)** - Does the work to complete the task
- **A (Accountable)** - Ultimately answerable for the task (only one A per row)
- **C (Consulted)** - Provides input before decision/action
- **I (Informed)** - Notified after decision/action

RACI Matrix: Data Governance Activities

Activity	Exec Sponsor	CDO	Data Owner	Data Steward	Data Custodian	Legal/Compliance	Data Consumer
Set data strategy and vision	Accountable	Responsible	Consulted	Informed	Informed	Consulted	Informed
Approve governance policies	Accountable	Responsible	Consulted	Consulted	Informed	Consulted	Informed
Define data domains	Informed	Accountable	Responsible	Consulted	Informed	Informed	Informed
Assign data ownership	Accountable	Responsible	Informed	Informed	Informed	Informed	Informed
Define data quality rules	Informed	Consulted	Accountable	Responsible	Consulted	Informed	Informed
Implement data quality rules	Informed	Informed	Accountable	Consulted	Responsible	Informed	Informed
Monitor data quality	Informed	Informed	Accountable	Responsible	Consulted	Informed	Informed
Remediate data issues	Informed	Informed	Accountable	Responsible	Responsible	Informed	Informed
Manage metadata	Informed	Consulted	Accountable	Responsible	Consulted	Informed	Informed
Approve data access	Informed	Informed	Accountable	Responsible	Responsible	Consulted	Informed
Implement access controls	Informed	Informed	Consulted	Informed	Responsible	Consulted	Informed
Classify data	Informed	Consulted	Accountable	Responsible	Informed	Consulted	Informed
Ensure regulatory compliance	Consulted	Accountable	Consulted	Consulted	Consulted	Responsible	Informed
Conduct data audits	Informed	Accountable	Consulted	Responsible	Consulted	Responsible	Informed
Report on data metrics	Informed	Responsible	Consulted	Consulted	Consulted	Informed	Informed
Train data users	Informed	Accountable	Consulted	Responsible	Consulted	Consulted	Informed
Handle data incidents	Consulted	Accountable	Consulted	Responsible	Responsible	Consulted	Informed

RACI Matrix: Data Lifecycle Activities

Activity	Data Owner	Data Steward	Data Custodian	Data Architect	Security Team	Compliance
Define data requirements	Accountable	Responsible	Consulted	Consulted	Informed	Consulted
Design data structures	Consulted	Consulted	Responsible	Accountable	Consulted	Informed
Create/acquire data	Accountable	Responsible	Responsible	Informed	Informed	Consulted
Validate data at entry	Accountable	Responsible	Responsible	Informed	Informed	Informed
Transform data	Consulted	Consulted	Responsible	Accountable	Informed	Informed
Store data securely	Accountable	Informed	Responsible	Consulted	Responsible	Consulted
Catalog and document data	Accountable	Responsible	Consulted	Consulted	Informed	Informed
Distribute/share data	Accountable	Responsible	Responsible	Informed	Consulted	Consulted
Archive data	Accountable	Consulted	Responsible	Consulted	Consulted	Consulted
Destroy/purge data	Accountable	Consulted	Responsible	Informed	Consulted	Responsible

RACI Matrix: Compliance Activities

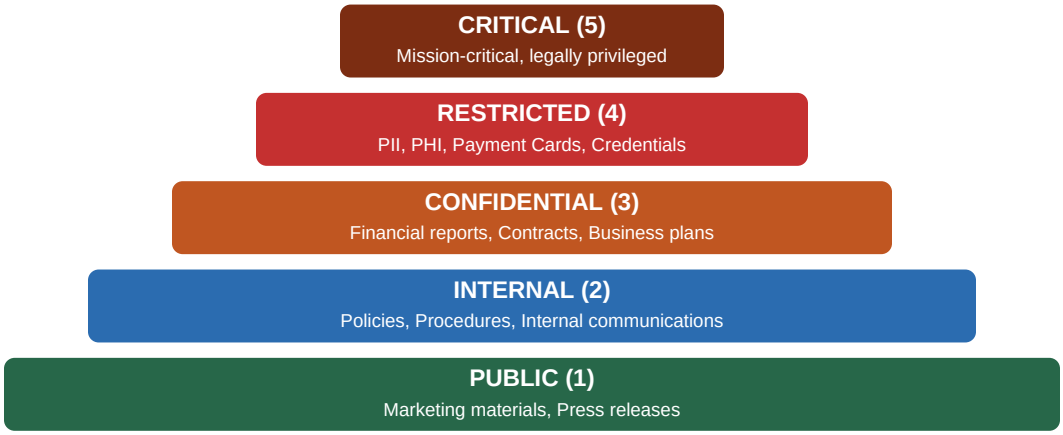
Activity	CDO	Legal	Compliance	Data Owner	Data Steward	Security	IT
Interpret regulations	Informed	Accountable	Responsible	Informed	Informed	Consulted	Informed
Map regulations to data	Consulted	Consulted	Accountable	Responsible	Responsible	Consulted	Informed
Implement compliance controls	Consulted	Consulted	Accountable	Consulted	Responsible	Responsible	Responsible
Process data subject requests	Informed	Consulted	Accountable	Responsible	Responsible	Consulted	Responsible
Conduct privacy impact assessments	Consulted	Accountable	Responsible	Consulted	Consulted	Consulted	Consulted
Manage consent	Informed	Accountable	Responsible	Responsible	Responsible	Consulted	Responsible
Report compliance status	Accountable	Consulted	Responsible	Consulted	Consulted	Consulted	Informed
Handle regulatory inquiries	Consulted	Accountable	Responsible	Consulted	Consulted	Consulted	Informed
Conduct compliance training	Accountable	Consulted	Responsible	Informed	Informed	Consulted	Informed

Data Classification Framework

Classification Levels

Level	Classification	Description	Examples	Handling Requirements
1	Public	Information approved for public release	Marketing materials, press releases, public reports	No restrictions on sharing; standard security controls
2	Internal	General business information for internal use	Policies, procedures, org charts, internal comms	Internal access only; basic access controls
3	Confidential	Sensitive business information	Financial reports, contracts, business plans, IP	Need-to-know access; encryption required; audit logging
4	Restricted	Highly sensitive regulated data	PII, PHI, payment cards, credentials, trade secrets	Strict access controls; encryption at rest and transit; MFA required
5	Critical	Mission-critical or legally privileged	Board materials, M&A; data, legal holds, security keys	Maximum protection; named access only; enhanced monitoring

Data Classification Decision Tree



Classification by Data Type

Data Category	Data Elements	Default Classification	Regulatory Driver
Personal Identifiers	Full name, SSN/TIN, Passport, Driver's License	Restricted (4)	GDPR, CCPA, Privacy Act
Contact Information	Email, Phone, Address (when linked to name)	Confidential (3)	GDPR, CCPA
Financial - Personal	Bank accounts, Credit cards, Income, Tax records	Restricted (4)	PCI-DSS, GLBA
Financial - Corporate	Revenue, P&L;, Forecasts, Budgets	Confidential (3)	SOX, SEC regulations
Health Information	Medical records, Diagnoses, Prescriptions	Restricted (4)	HIPAA, Privacy Act
Authentication	Passwords, API keys, Tokens, Certificates	Critical (5)	Security best practices
Employment	HR records, Performance reviews, Salary	Restricted (4)	Employment law
Customer Transactions	Orders, Payments, Service history	Confidential (3)	GDPR, CCPA
Product/IP	Designs, Patents, Trade secrets, Source code	Restricted (4)	IP law
Operational	Inventory, Schedules, Logistics	Internal (2)	Business sensitivity
Marketing	Published content, Public campaigns	Public (1)	None

Data Handling Requirements by Classification

Requirement	Public (1)	Internal (2)	Confidential (3)	Restricted (4)	Critical (5)
Access Control	Open	Authentication	Need-to-know	Named access	Named + approval
Encryption at Rest	Optional	Recommended	Required	Required (AES-256)	Required (AES-256)
Encryption in Transit	HTTPS	HTTPS/TLS	TLS 1.2+	TLS 1.3	TLS 1.3 + mTLS
Multi-Factor Auth	No	No	Recommended	Required	Required
Audit Logging	Basic	Standard	Enhanced	Full audit	Real-time monitoring
Data Masking	No	No	In non-prod	Required	Required
Retention Limit	None	7 years	Per policy	Minimum necessary	Per legal hold
Disposal Method	Standard	Standard	Secure delete	Certified destruction	Certified + witnessed
Backup Encryption	Optional	Optional	Required	Required	Required + separate keys
Third-Party Sharing	Allowed	With NDA	With DPA	Prohibited (default)	Board approval required
Cloud Storage	Any approved	Approved providers	Approved + encrypted	Restricted regions	On-premise or private cloud
Print Handling	No restrictions	Internal only	Secure print	No printing (default)	Prohibited

Data Classification Label Template

DATA CLASSIFICATION LABEL

Classification Level: ■ Public ■ Internal ■ Confidential ■ Restricted ■ Critical

Data Asset Name: _____

Data Domain: _____

Data Owner: _____

Classification Date: _____

Review Date: _____

Handling Instructions: _____

Regulatory: ■ GDPR ■ CCPA ■ HIPAA ■ PCI-DSS ■ NZ Privacy Act ■ Other

Approved By: _____ Date: _____

Data Governance Policies

Policy Index

Policy ID	Policy Name	Version	Effective Date	Review Cycle	Owner
DGP-001	Data Governance Policy	3.0	2026-01-01	Annual	CDO
DGP-002	Data Classification Policy	2.5	2026-01-01	Annual	CDO
DGP-003	Data Quality Policy	2.0	2026-01-01	Annual	DQ Lead
DGP-004	Data Access Policy	3.0	2026-01-01	Annual	Security
DGP-005	Data Retention Policy	2.5	2026-01-01	Annual	Legal
DGP-006	Data Privacy Policy	3.0	2026-01-01	Annual	Privacy Officer
DGP-007	Data Security Policy	3.0	2026-01-01	Annual	CISO
DGP-008	Master Data Management Policy	2.0	2026-01-01	Annual	CDO
DGP-009	Metadata Management Policy	2.0	2026-01-01	Annual	CDO
DGP-010	Data Sharing Policy	2.5	2026-01-01	Annual	Legal

DGP-001: Enterprise Data Governance Policy

Policy Number: DGP-001

Version: 3.0

Effective Date: January 1, 2026

Policy Owner: Chief Data Officer

Approved By: Data Governance Council

1. Purpose

This policy establishes the framework for managing data as a strategic enterprise asset, ensuring data is accurate, accessible, secure, and compliant with regulatory requirements.

2. Scope

This policy applies to:

- All data created, collected, processed, stored, or transmitted by the organization
- All employees, contractors, vendors, and third parties with access to organizational data
- All systems, applications, and platforms containing organizational data
- All locations and geographies where the organization operates

3. Policy Statements

ID	Statement	Requirement Level
3.1	All data shall have an assigned Data Owner responsible for its governance	Mandatory
3.2	All critical data domains shall have designated Data Stewards	Mandatory
3.3	All data shall be classified according to the Data Classification Framework	Mandatory
3.4	Data quality standards shall be defined and measured for all critical data	Mandatory
3.5	Access to data shall be granted based on business need and least privilege	Mandatory
3.6	All data handling shall comply with applicable laws and regulations	Mandatory
3.7	Data governance metrics shall be reported to leadership monthly	Mandatory
3.8	Data governance training shall be completed by all employees annually	Mandatory
3.9	Data governance policies shall be reviewed and updated annually	Mandatory
3.10	Exceptions to policies require documented approval from the CDO	Mandatory

4. Roles and Responsibilities

Role	Key Responsibilities
Executive Sponsor	Champion governance; secure resources; remove barriers
CDO	Lead governance program; chair council; report to leadership
Data Governance Council	Approve policies; resolve issues; allocate resources
Data Owner	Accountable for domain data; approve access; define requirements
Data Steward	Manage data day-to-day; ensure quality; maintain metadata
Data Custodian	Technical implementation; maintain systems; execute controls
All Employees	Follow policies; report issues; complete training

5. Compliance

Non-compliance with this policy may result in:

- Revocation of data access privileges
- Disciplinary action up to and including termination
- Legal liability for regulatory violations
- Financial penalties for the organization

6. Related Documents

- DGP-002 through DGP-010 (Supporting policies)
- Data Governance Charter
- Data Classification Framework
- RACI Matrices

7. Review and Approval

Version	Date	Author	Changes	Approved By
1.0	2024-01-01	Enterprise Data Solutions	Initial release	DG Council
2.0	2025-01-01	Enterprise Data Solutions	Added AI governance	DG Council
3.0	2026-01-01	Enterprise Data Solutions	Updated compliance requirements	DG Council

DGP-002: Data Classification Policy

Policy Number: DGP-002

Version: 2.5

Effective Date: January 1, 2026

Policy Owner: Chief Data Officer

1. Purpose

This policy establishes requirements for classifying data based on sensitivity and criticality to ensure appropriate protection and handling.

2. Classification Levels

Level	Name	Description	Protection Level
1	Public	Approved for external release	Standard
2	Internal	General business use	Basic
3	Confidential	Sensitive business data	Enhanced
4	Restricted	Regulated/sensitive personal data	High
5	Critical	Legally privileged/mission-critical	Maximum

3. Policy Statements

ID	Statement	Requirement
3.1	All data assets shall be classified within 30 days of creation	Mandatory
3.2	Classification shall be performed by the Data Owner or delegate	Mandatory
3.3	Classification shall be reviewed annually or upon significant change	Mandatory
3.4	Data shall be handled according to its classification level	Mandatory
3.5	Aggregated or derived data inherits the highest classification of source data	Mandatory
3.6	Classification metadata shall be recorded in the data catalog	Mandatory
3.7	Downgrading classification requires Data Owner approval	Mandatory

4. Classification Process

→ 1. IDENTIFY data asset
→ 2. DETERMINE data elements contained
→ 3. EVALUATE against classification criteria
→ 4. SELECT appropriate classification level
→ 5. DOCUMENT in data catalog with justification
→ 6. APPLY appropriate handling controls
→ 7. COMMUNICATE to stakeholders
→ 8. REVIEW periodically (minimum annually)

DGP-003: Data Quality Policy

Policy Number: DGP-003

Version: 2.0

Effective Date: January 1, 2026

Policy Owner: Data Quality Lead

1. Purpose

This policy establishes requirements for measuring, monitoring, and improving data quality across the enterprise.

2. Data Quality Dimensions

Dimension	Definition	Measurement Method
Accuracy	Data correctly represents real-world values	Validation against source; business rules
Completeness	Required data elements are present	Null/blank analysis; field coverage
Consistency	Data values are uniform across systems	Cross-system comparison; format checks
Timeliness	Data is available when needed	Latency measurement; SLA compliance
Validity	Data conforms to defined formats and ranges	Format validation; domain checks
Uniqueness	No unintended duplicate records	Duplicate detection algorithms
Integrity	Relationships between data are maintained	Referential integrity checks

3. Quality Standards by Data Criticality

Data Criticality	Accuracy	Completeness	Consistency	Timeliness
Critical	>= 99.9%	>= 99.9%	>= 99.9%	Real-time
High	>= 99.5%	>= 99.0%	>= 99.0%	< 1 hour
Medium	>= 98.0%	>= 95.0%	>= 95.0%	< 24 hours
Low	>= 95.0%	>= 90.0%	>= 90.0%	< 7 days

4. Policy Statements

ID	Statement	Requirement
4.1	Data quality requirements shall be defined for all critical data	Mandatory
4.2	Data quality shall be measured using automated tools	Mandatory
4.3	Quality issues shall be logged in the issue tracking system	Mandatory
4.4	Root cause analysis shall be performed for recurring issues	Mandatory
4.5	Quality metrics shall be reported monthly to stakeholders	Mandatory
4.6	Data quality SLAs shall be established with upstream providers	Mandatory

DGP-004: Data Access Policy

Policy Number: DGP-004

Version: 3.0

Effective Date: January 1, 2026

Policy Owner: Chief Information Security Officer

1. Purpose

This policy establishes requirements for granting, managing, and revoking access to organizational data.

2. Access Control Principles

Principle	Description
Least Privilege	Users receive minimum access required for their role
Need-to-Know	Access granted only when business need is demonstrated
Segregation of Duties	Critical functions divided among multiple people
Default Deny	Access denied unless explicitly granted
Time-Bound	Access expires and requires periodic re-certification

3. Access Request Process

Step	Action	Responsible	Timeline
1	Submit access request via form	Requester	-
2	Validate business justification	Manager	1 day
3	Review data classification	Data Steward	1 day
4	Approve/deny request	Data Owner	2 days
5	Implement access (if approved)	Data Custodian	1 day
6	Confirm access provisioned	Requester	1 day
Total SLA			5 business days

4. Access Levels

Level	Description	Approval Required
Read	View data only	Manager + Data Steward
Write	Create and modify data	Manager + Data Owner
Delete	Remove data records	Manager + Data Owner + DG Office
Admin	Full system administration	CISO + Data Owner + CDO
Export	Extract data from systems	Data Owner + Compliance

5. Access Review Requirements

Data Classification	Review Frequency	Reviewer
Critical	Quarterly	Data Owner + CISO
Restricted	Quarterly	Data Owner
Confidential	Semi-annually	Data Steward
Internal	Annually	Data Steward
Public	Annually	Data Steward

DGP-005: Data Retention Policy

Policy Number: DGP-005

Version: 2.5

Effective Date: January 1, 2026

Policy Owner: General Counsel

1. Purpose

This policy establishes requirements for retaining and disposing of data in compliance with legal, regulatory, and business requirements.

2. Retention Schedule

Data Category	Retention Period	Legal Basis	Disposal Method
Financial records	7 years	Tax regulations, SOX	Certified destruction
Employee records	Employment + 7 years	Employment law	Certified destruction
Customer PII	Relationship + 3 years or consent withdrawal	GDPR, CCPA, Privacy Act	Certified destruction
Health records	10 years minimum	HIPAA, Health regulations	Certified destruction
Contracts	Term + 7 years	Statute of limitations	Certified destruction
Email - general	3 years	Business need	Secure deletion
Email - legal hold	Until hold released	Legal requirement	Per legal direction
Transaction logs	7 years	Audit requirements	Secure deletion
System logs	1 year	Security requirements	Secure deletion
Marketing data	Consent duration or 2 years	GDPR, CCPA	Secure deletion
Analytics data	5 years (aggregated)	Business need	Standard deletion
Backup data	Active retention + 90 days	Disaster recovery	Overwrite/destruction

3. Legal Hold Procedures

Step	Action	Responsible	Timeline
1	Legal issues hold notice	Legal Counsel	Immediate
2	Identify custodians and data sources	Legal + IT	24 hours
3	Suspend relevant retention schedules	DG Office	24 hours
4	Notify custodians of preservation duty	Legal	48 hours
5	Implement technical holds	IT	72 hours
6	Document hold scope and actions	Legal	1 week
7	Periodic hold review	Legal	Quarterly
8	Release hold when resolved	Legal Counsel	Per matter

DGP-006: Data Privacy Policy

Policy Number: DGP-006

Version: 3.0

Effective Date: January 1, 2026

Policy Owner: Privacy Officer

1. Purpose

This policy establishes requirements for protecting personal information in compliance with privacy regulations globally.

2. Privacy Principles

Principle	Description	Implementation
Lawfulness	Process data only with legal basis	Document legal basis for all processing
Purpose Limitation	Use data only for stated purposes	Define and document purposes
Data Minimization	Collect only necessary data	Review data collection forms
Accuracy	Keep personal data accurate	Implement correction processes
Storage Limitation	Retain only as long as necessary	Apply retention schedules
Security	Protect against unauthorized access	Implement security controls
Accountability	Demonstrate compliance	Maintain documentation and records

3. Data Subject Rights

Right	Description	Response Timeline	Process Owner
Right to Access	Provide copy of personal data	30 days	Privacy Team
Right to Rectification	Correct inaccurate data	30 days	Data Steward
Right to Erasure	Delete personal data	30 days	Privacy Team
Right to Portability	Export data in machine-readable format	30 days	IT + Privacy
Right to Object	Stop processing for certain purposes	30 days	Privacy Team
Right to Restrict	Limit processing temporarily	30 days	Privacy Team
Right to Withdraw Consent	Revoke previously given consent	30 days	Privacy Team

4. Privacy Impact Assessment Triggers

Trigger	PIA Required	Approval Needed
New collection of personal data	Yes	Privacy Officer
New purpose for existing data	Yes	Privacy Officer
New third-party data sharing	Yes	Privacy Officer + Legal
New technology processing PII	Yes	Privacy Officer + CISO
Processing sensitive categories	Yes - Full PIA	Privacy Officer + CDO
Automated decision-making	Yes - Full PIA	Privacy Officer + CDO
Large-scale profiling	Yes - Full PIA	Privacy Officer + CDO + Legal
Cross-border data transfer	Yes	Privacy Officer + Legal

Data Quality Standards

Data Quality Scorecard Template

Domain: _____

Data Owner: _____

Assessment Period: _____

Assessed By: _____

Overall Quality Score

Dimension	Weight	Score (0-100)	Weighted Score	Target	Status
Accuracy	25%			98%	
Completeness	20%			95%	
Consistency	20%			95%	
Timeliness	15%			99%	
Validity	10%			99%	
Uniqueness	10%			99%	
TOTAL	100%			97%	

Quality Rules Inventory

Rule ID	Rule Name	Dimension	Logic/Description	Threshold	Priority
QR-001					
QR-002					
QR-003					
QR-004					
QR-005					

Quality Issue Log

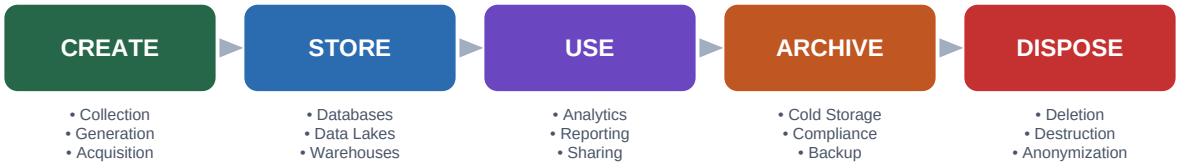
Issue ID	Date Found	Data Element	Description	Severity	Root Cause	Owner	Status	Resolution Date

Quality Trend Analysis

Month	Accuracy	Completeness	Consistency	Timeliness	Overall
Jan					
Feb					
Mar					
Apr					
May					
Jun					
Jul					
Aug					
Sep					
Oct					
Nov					
Dec					

Data Lifecycle Management

Data Lifecycle Stages



Lifecycle Requirements Matrix

Stage	Security	Quality	Privacy	Compliance	Documentation
Create	Input validation; Source authentication	Validation at entry; Format checks	Consent capture; Purpose documentation	Legal basis verification	Source metadata; Lineage start
Store	Encryption; Access controls	Integrity monitoring; Backup verification	Minimization; Geographic controls	Retention alignment	Storage location; Classification
Use	Authorization; Audit logging	Fitness for use verification	Purpose limitation; Anonymization	Usage tracking	Access logs; Usage records
Share	Secure transfer; Data agreements	Quality SLAs; Format standards	Third-party controls; Consent verification	Transfer agreements	Sharing records; Recipient logs
Archive	Encrypted archives; Limited access	Integrity verification	Retention compliance; Access restrictions	Archive policies	Archive metadata; Retrieval procedures
Dispose	Certified destruction; Verification	N/A	Complete removal; Backup cleanup	Disposal certification	Destruction certificates; Audit trail

Data Lineage Template

Attribute	Value
Data Asset	
Source System(s)	
Source Tables/Files	
Transformation Steps	
Target System	
Target Tables/Files	
Update Frequency	
Last Updated	
Data Owner	
Technical Owner	

Visual Lineage Map

Compliance Frameworks

Regulatory Compliance Matrix

Regulation	Jurisdiction	Applicability	Key Requirements	Data Types	Penalties
GDPR	EU/EEA	Processing EU resident data	Consent, data subject rights, DPO, breach notification (72hr), PIAs	Personal data, special categories	Up to 4% global revenue or EUR 20M
CCPA/CPRA	California, USA	CA resident data, revenue >$25M	Right to know, delete, opt-out, non-discrimination	Personal information	$2,500-$7,500 per violation
HIPAA	USA	Healthcare providers, plans, clearinghouses	Privacy Rule, Security Rule, Breach Notification	PHI, ePHI	$100-$50,000 per violation; up to $1.5M/year
NZ Privacy Act 2020	New Zealand	NZ agencies and organizations	13 Privacy Principles, mandatory breach reporting, cross-border controls	Personal information	Complaints, compliance notices, naming
PCI DSS	Global	Card payment processing	Network security, encryption, access control, monitoring	Cardholder data	Fines, increased fees, loss of processing
SOX	USA	Public companies	Internal controls, audit trail, data retention	Financial data	Criminal penalties, fines, imprisonment

GDPR Compliance Checklist

Requirement	Description	Status	Evidence	Owner
Lawful Basis	Documented legal basis for all processing			
Privacy Notices	Clear, comprehensive privacy notices			
Consent Management	Mechanism to capture and manage consent			
Data Subject Rights	Processes for all GDPR rights			
Data Processing Register	Record of processing activities			
DPO Appointment	Data Protection Officer designated (if required)			
Privacy Impact Assessments	PIAs for high-risk processing			
Breach Response Plan	72-hour notification process			
International Transfers	SCCs/adequacy for non-EU transfers			
Vendor Management	DPAs with all processors			
Training	Staff awareness program			
Security Measures	Appropriate technical/organizational measures			

NZ Privacy Act 2020 Compliance Checklist

Principle/Requirement	Description	Status	Evidence	Owner
IPP 1: Purpose of Collection	Only collect for lawful, necessary purposes			
IPP 2: Source of Information	Collect directly from individual where possible			
IPP 3: Collection Notice	Inform individuals about collection and use			
IPP 4: Manner of Collection	Collect lawfully and fairly			
IPP 5: Storage and Security	Protect against loss, misuse, unauthorized access			
IPP 6: Access Rights	Allow individuals access to their information			
IPP 7: Correction Rights	Allow individuals to correct information			
IPP 8: Accuracy Before Use	Take reasonable steps to ensure accuracy			
IPP 9: Retention	Don't keep longer than necessary			
IPP 10: Use Limitation	Use only for purpose collected (or exceptions)			
IPP 11: Disclosure Limitation	Don't disclose without authority			
IPP 12: Cross-Border Disclosure	Controls on international transfers			
IPP 13: Unique Identifiers	Limitations on using unique identifiers			
Breach Notification	Notify Privacy Commissioner of serious breaches			
Compliance Notices	Process for responding to Commissioner notices			

CCPA/CPRA Compliance Checklist

Requirement	Description	Status	Evidence	Owner
Right to Know	Disclose categories and purposes of collection			
Right to Delete	Process for deletion requests			
Right to Opt-Out	"Do Not Sell My Personal Information" link			
Right to Correct	Process for correction requests			
Right to Limit	Limit use of sensitive personal information			
Non-Discrimination	No retaliation for exercising rights			
Privacy Policy	Updated privacy policy with required disclosures			
Service Provider Agreements	Contracts with processors meeting CCPA requirements			
Training	Employee training on consumer requests			
Verification	Process to verify consumer identity			

HIPAA Compliance Checklist

Requirement	Description	Status	Evidence	Owner
Privacy Rule Implementation	Policies limiting PHI use and disclosure			
Security Rule - Administrative	Security management, workforce training, contingency planning			
Security Rule - Physical	Facility access controls, workstation security			
Security Rule - Technical	Access controls, audit controls, encryption			
Breach Notification	Procedures for breach assessment and notification			
Business Associate Agreements	BAAs with all entities accessing PHI			
Risk Assessment	Annual security risk assessment			
Minimum Necessary	Limit PHI access to minimum needed			
Patient Rights	Access, amendment, accounting of disclosures			
Training	HIPAA training for all workforce members			

Audit and Assessment Templates

Data Governance Audit Checklist

Audit Period: _____

Auditor: _____

Date: _____

Governance Structure

Item	Criteria	Met? (Y/N/P)	Evidence	Finding	Recommendation
1.1	Executive sponsor identified and engaged				
1.2	Data Governance Council operational				
1.3	CDO or equivalent role established				
1.4	Data Governance Office resourced				
1.5	Data domains defined with owners				
1.6	Data stewards assigned and trained				
1.7	Governance charter documented				
1.8	RACI matrices defined and current				

Policies and Standards

Item	Criteria	Met? (Y/N/P)	Evidence	Finding	Recommendation
2.1	Core governance policies documented				
2.2	Policies reviewed within past year				
2.3	Policies approved by appropriate authority				
2.4	Policies communicated to stakeholders				
2.5	Policy compliance monitored				
2.6	Exception process defined and followed				

Data Quality

Item	Criteria	Met? (Y/N/P)	Evidence	Finding	Recommendation
3.1	Data quality dimensions defined				
3.2	Quality rules implemented				
3.3	Quality measured and reported				
3.4	Quality issues tracked and resolved				
3.5	Root cause analysis performed				
3.6	Quality SLAs established				

Data Security and Privacy

Item	Criteria	Met? (Y/N/P)	Evidence	Finding	Recommendation
4.1	Data classification implemented				
4.2	Access controls aligned to classification				
4.3	Access reviews conducted per schedule				
4.4	Privacy requirements documented				
4.5	Data subject request process operational				
4.6	Breach response plan tested				

Metadata and Catalog

Item	Criteria	Met? (Y/N/P)	Evidence	Finding	Recommendation
5.1	Data catalog implemented				
5.2	Critical data assets cataloged				
5.3	Business glossary maintained				
5.4	Data lineage documented				
5.5	Metadata standards defined				

Audit Findings Summary

Finding ID	Area	Severity (H/M/L)	Description	Recommendation	Owner	Due Date

Audit Rating Scale

Rating	Description	Criteria
Effective	Controls operating as designed	>= 90% criteria met
Needs Improvement	Minor gaps in controls	70-89% criteria met
Significant Deficiencies	Material gaps in controls	50-69% criteria met
Ineffective	Controls not operating	< 50% criteria met

Implementation Roadmap

Phase 1: Foundation (Months 1-3)

Week	Activity	Deliverable	Owner	Status
1-2	Secure executive sponsorship	Signed charter	CDO	
2-3	Assess current state	Assessment report	DG Lead	
3-4	Define governance structure	Org design document	CDO	
4-6	Identify data domains	Domain inventory	DG Lead	
6-8	Assign data owners	Ownership matrix	CDO	
8-10	Recruit/assign data stewards	Steward roster	Data Owners	
10-12	Draft core policies	Policy drafts	DG Lead	

Phase 1 Success Criteria:

- ■ Executive sponsor confirmed and charter signed
- ■ Governance structure approved
- ■ Data owners assigned for 100% of critical domains
- ■ Core policies drafted

Phase 2: Build (Months 4-6)

Week	Activity	Deliverable	Owner	Status
1-2	Approve and publish policies	Published policies	DG Council	
2-4	Implement data classification	Classification schema	DG Lead	
4-6	Deploy data catalog	Catalog MVP	IT	
6-8	Define data quality rules	Quality rule library	Stewards	
8-10	Implement access request process	Access workflow	IT + DG	
10-12	Launch governance training	Training program	DG Lead	

Phase 2 Success Criteria:

- ■ All core policies approved and published
- ■ Data catalog live with critical assets
- ■ Classification applied to 80% of data assets
- ■ Training completed by 90% of stakeholders

Phase 3: Operate (Months 7-9)

Week	Activity	Deliverable	Owner	Status
1-2	Begin data quality measurement	Quality baseline	Stewards	
2-4	Implement quality dashboards	Quality scorecards	DG Office	
4-6	Conduct first access review	Access review report	Data Owners	
6-8	Process data subject requests	Request metrics	Privacy	
8-10	First governance council review	Council minutes	CDO	
10-12	Refine processes based on feedback	Process improvements	DG Lead	

Phase 3 Success Criteria:

- ■ Data quality measured for all critical domains
- ■ First access review completed
- ■ Governance council meeting regularly
- ■ Data subject request process operational

Phase 4: Optimize (Months 10-12)

Week	Activity	Deliverable	Owner	Status
1-2	Conduct governance audit	Audit report	Internal Audit	
2-4	Address audit findings	Remediation plan	DG Lead	
4-6	Expand catalog coverage	Updated catalog	Stewards	
6-8	Automate quality monitoring	Automated rules	IT	
8-10	Year 1 assessment	Maturity assessment	DG Lead	
10-12	Plan Year 2 roadmap	Year 2 plan	CDO	

Phase 4 Success Criteria:

- Governance audit completed with acceptable rating
- Catalog coverage > 95% of critical assets
- Quality automation in place
- Year 2 roadmap approved

Appendices

Appendix A: Glossary of Terms

Term	Definition
Business Glossary	Controlled vocabulary of business terms with agreed definitions
Data Asset	A collection of data elements that has value to the organization
Data Catalog	An inventory of data assets with searchable metadata
Data Classification	Process of categorizing data by sensitivity and criticality
Data Custodian	Technical role responsible for data storage and infrastructure
Data Domain	A logical grouping of related data (e.g., Customer, Product, Finance)
Data Governance	The exercise of authority, control, and shared decision-making over data
Data Lineage	Documentation of data origins, movements, and transformations
Data Owner	Business role accountable for a data domain
Data Quality	Degree to which data meets requirements for its intended use
Data Steward	Role responsible for day-to-day data management within a domain
DPA	Data Processing Agreement - contract governing processor obligations
DPO	Data Protection Officer - role required by GDPR for certain organizations
Metadata	Data that describes other data (e.g., definitions, formats, lineage)
PIA/DPIA	Privacy/Data Protection Impact Assessment
PII	Personally Identifiable Information
PHI	Protected Health Information (HIPAA term)
RACI	Responsibility matrix: Responsible, Accountable, Consulted, Informed
SLA	Service Level Agreement

Appendix B: Template Forms

Data Access Request Form

Field	Input
Requester Name	
Department	
Manager	
Request Date	
Data Asset(s) Requested	
Data Domain	
Classification Level	
Access Type	[ ] Read [ ] Write [ ] Delete [ ] Admin
Business Justification	
Duration Required	[ ] Permanent [ ] Temporary until: _____
Systems/Tools	

Approvals	Name	Date	Decision
Manager			[ ] Approved [ ] Denied
Data Steward			[ ] Approved [ ] Denied
Data Owner			[ ] Approved [ ] Denied
Security (if required)			[ ] Approved [ ] Denied

Data Quality Issue Report

Field	Input
Issue ID	
Reported By	
Report Date	
Data Domain	
Data Asset/Element	
System Affected	
Issue Description	
Business Impact	[ ] Critical [ ] High [ ] Medium [ ] Low
Quality Dimension	[ ] Accuracy [ ] Completeness [ ] Consistency [ ] Timeliness [ ] Validity [ ] Uniqueness
Sample Records	

Resolution	Details
Root Cause	
Resolution Actions	
Resolved By	
Resolution Date	
Preventive Measures	

Data Subject Request Form

Field	Input
Request ID	
Request Date	
Requester Name	
Contact Information	
Identity Verification	[ ] Verified [ ] Pending
Request Type	[ ] Access [ ] Deletion [ ] Correction [ ] Portability [ ] Restriction [ ] Objection
Description of Request	
Data Categories	
Due Date	

Processing	Details
Assigned To	
Systems Searched	
Data Located	
Action Taken	
Response Sent	
Completion Date	

Appendix C: Governance Metrics Dashboard

Key Performance Indicators

Metric	Target	Current	Trend	Status
Governance				
Policy compliance rate	> 95%			
Domains with assigned owners	100%			
Steward coverage	100%			
Training completion	> 90%			
Data Quality				
Overall quality score	> 95%			
Critical issue resolution time	< 48 hrs			
Quality SLA compliance	> 99%			
Security & Privacy				
Classification coverage	100%			
Access review completion	100%			
DSR response compliance	100%			
Security incidents	0			
Catalog & Metadata				
Catalog coverage	> 95%			
Metadata completeness	> 90%			
Glossary term adoption	> 80%			

Appendix D: Version History

Version	Date	Author	Changes
1.0	2024-01-01	Enterprise Data Solutions	Initial framework release
2.0	2025-01-01	Enterprise Data Solutions	Added AI governance, updated compliance
2.5	2025-06-01	Enterprise Data Solutions	Enhanced privacy sections
3.0	2026-01-01	Enterprise Data Solutions	Major update: NZ Privacy Act, expanded templates, 2026 compliance updates

About Enterprise Data Solutions

Enterprise Data Solutions is New Zealand's trusted partner for data strategy and governance. We help organizations across Australasia and globally transform their data capabilities from strategic planning through implementation.

Our Services

Service	Description
Data Governance Consulting	Design and implement comprehensive governance frameworks
Data Strategy Development	Create actionable data strategies aligned with business goals
Data Platform Implementation	Build modern data infrastructure on leading cloud platforms
Analytics & AI Solutions	Deploy advanced analytics and machine learning capabilities
Compliance Advisory	Navigate GDPR, CCPA, NZ Privacy Act, and industry regulations
Data Quality Programs	Establish measurement and improvement programs

Why Choose Enterprise Data Solutions

- Deep expertise in data governance and compliance
- Proven frameworks refined through real-world implementations
- Local presence with global perspective
- Industry-specific knowledge across sectors
- End-to-end capabilities from strategy to execution

Contact Us

Enterprise Data Solutions

Channel	Contact
Website	https://www.enterprisedatasolutions.co.nz
Email	Contact@enterprisedatasolutions.co.nz
Services	Data Governance, Data Strategy, Analytics, Compliance

Schedule a Consultation

Ready to establish or enhance your data governance program? Contact us to discuss your organization's needs and how this framework can be customized for your context.

Document Control

Attribute	Value
Document Title	Data Governance Framework Template 2026
Version	3.0
Classification	Public
Prepared By	Enterprise Data Solutions
Copyright	2026 Enterprise Data Solutions. This template may be customized for organizational use.

This template is provided by Enterprise Data Solutions. Feel free to adapt it for your organization's specific requirements.