SCOPE Framework: Data Governance & Privacy Control Domain

Table of Contents

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Purpose: The Data Governance & Privacy domain ensures the responsible management, protection, and utilization of data assets throughout the organization. It provides a structured framework for classifying and labeling data, governing its lifecycle, enforcing data residency and sovereignty requirements, and honoring user data rights. This domain ensures that data is treated in alignment with its sensitivity, legal obligations, and user expectations—enabling transparency, accountability, and regulatory compliance. By institutionalizing data stewardship and privacy-by-design principles, the organization reduces data-related risk exposure, enhances trust, and upholds the confidentiality, integrity, and availability of sensitive information.

Section 1. Data Classification & Labeling (DCL)

Effective data classification and labeling form the foundation for data protection, regulatory compliance, and informed access control decisions. This control family ensures organizations implement formal mechanisms to identify, classify, and label data based on sensitivity, criticality, regulatory obligations, and business value. The controls herein are intended to ensure data is handled appropriately throughout its lifecycle, enabling downstream enforcement mechanisms across people, process, and technology layers.

1.1 DCL-01: Data Classification Policy Definition

The organization shall establish, document, and maintain a data classification policy that defines classification levels, criteria for classification, and handling requirements for each classification tier.

1.2 DCL-02: Data Classification Schema Standardization

The organization shall define a standardized data classification schema that includes at minimum: Public, Internal, Confidential, and Restricted classifications, with accompanying descriptions and handling requirements.

1.3 DCL-03: Roles & Responsibilities for Classification

The organization shall assign roles and responsibilities for data classification to data owners, custodians, and stewards, including enforcement and periodic validation of classifications.

1.4 DCL-04: Classification of Structured & Unstructured Data

The organization shall implement procedures to classify both structured and unstructured data across repositories and storage media, including databases, file systems, collaboration platforms, and cloud storage.

1.5 DCL-05: Metadata Tagging for Classified Data

Classified data shall be tagged with metadata indicating its classification level, owner, and any applicable handling or regulatory constraints, using automated or manual tagging mechanisms.

1.6 DCL-06: Automated Classification Tool Integration

The organization shall deploy and maintain automated classification tools to scan and categorize data based on content, context, and source, integrating with DLP and access control solutions.

1.7 DCL-07: Labeling of Digital Assets

The organization shall ensure that digital assets are labeled in accordance with their classification level using visual or embedded indicators (e.g., headers, footers, watermarks, metadata).

1.8 DCL-08: Labeling of Physical Assets

Physical media such as printed documents, USB drives, and backup tapes shall be labeled clearly in accordance with their data classification, using standardized templates or color-coding where feasible.

1.9 DCL-09: Classification at Point of Creation

Where feasible, data creators shall classify information at the point of creation using integrated prompts or defaults in business applications, file storage systems, or content management platforms.

1.10 DCL-10: Classification Validation & Quality Assurance

The organization shall implement periodic validation procedures to ensure the accuracy and consistency of data classifications, including audits and sampling by data stewards or internal audit functions.

1.11 DCL-11: Classification Review Triggers

The organization shall define triggers that require reclassification of data, including changes in business process, ownership, regulatory status, aggregation, or threat landscape.

1.12 DCL-12: Legacy Data Classification Strategy

A defined process shall be implemented to assess and apply appropriate classification to legacy or inherited data sets lacking classification metadata.

1.13 DCL-13: Third-Party Data Classification Alignment

When receiving or transmitting data to third parties, the organization shall require classification labels to be preserved or mapped to internal schema, and establish contractual alignment requirements.

1.14 DCL-14: Classification-Driven Handling Procedures

Procedures for accessing, storing, transmitting, archiving, and disposing of data shall be driven by its classification level, ensuring higher sensitivity data is afforded greater protection.

1.15 DCL-15: End-User Training on Classification & Labeling

Training programs shall be developed and delivered to ensure personnel understand the classification schema, their responsibility in labeling, and the risks of misclassification.

1.16 DCL-16: Classification Exceptions & Escalations

The organization shall define a process for handling classification exceptions, conflicts, or escalation requests, including resolution authority and timeframes.

1.17 DCL-17: Integration with Access Control Systems

Classification metadata shall integrate with access control mechanisms (e.g., RBAC, ABAC) to enforce authorization based on data sensitivity and user clearance.

1.18 DCL-18: Classification Retention & Audit Logging

Systems used for classification shall maintain audit logs of classification changes, who made them, when, and any associated rationale, for accountability and forensic purposes.

1.19 DCL-19: Enforcement of Labeling Before Transmission

Controls shall be implemented to prevent outbound transmission of data without appropriate classification or labeling, particularly for sensitive or restricted data.

1.20 DCL-20: Continuous Improvement of Classification Process

The classification and labeling program shall be periodically reviewed and enhanced to address emerging data types, technologies, regulatory drivers, and lessons learned from incidents or audits.

1.21 DCL-21: Regulatory Classification Mapping

Data classification practices shall be mapped to applicable regulatory classification standards to ensure compliance and support external reporting obligations.

Section 2. Data Lifecycle Management (DLM)

Data Lifecycle Management (DLM) ensures that data is governed and protected throughout each phase of its existence—from creation and usage through storage, archival, and final destruction. These controls focus on the definition, enforcement, and continuous refinement of lifecycle policies that align with business needs, regulatory requirements, and risk tolerance. Unlike classification, DLM emphasizes time-bound custodianship, transitions between phases, and defensible deletion strategies.

2.1 DLM-01: Data Lifecycle Governance Policy

The organization shall develop and maintain a data lifecycle management policy that defines data stages (creation, usage, retention, archival, destruction) and governing principles for each stage.

2.2 DLM-02: Data Lifecycle Stage Definition

Lifecycle stages shall be clearly defined and documented for all major data types (e.g., transactional, operational, analytical, backup), including required handling and retention conditions per stage.

2.3 DLM-03: Lifecycle Assignment Based on Data Type

The organization shall assign appropriate lifecycle requirements to data types based on business function, legal/regulatory requirements, and criticality, ensuring consistent application across systems.

2.4 DLM-04: Retention Schedule Development

Formal data retention schedules shall be developed and approved, specifying timeframes for active use, archival, and destruction, aligned with business needs and legal obligations.

2.5 DLM-05: Data Retention Enforcement Mechanisms

Automated or manual controls shall be implemented to enforce retention periods, prevent premature deletion, and trigger archival or destruction at the appropriate lifecycle stage.

2.6 DLM-06: Data Archival Procedures

Archived data shall be separated from active data and stored in a secure, cost-effective manner that supports retrieval if required by legal, operational, or audit purposes.

2.7 DLM-07: Archival Format & Integrity Requirements

Archived data shall be stored in formats that preserve integrity, usability, and readability for the duration of its retention, with periodic checks for bit rot or format obsolescence.

2.8 DLM-08: End-of-Life Data Destruction Policy

The organization shall define and enforce destruction procedures for data reaching the end of its lifecycle, ensuring methods are secure, irreversible, and appropriate to data sensitivity.

2.9 DLM-09: Automated End-of-Life Triggers

Systems shall be configured to identify and flag data that has reached its retention threshold, automatically initiating archival or destruction workflows in accordance with policy.

2.10 DLM-10: Legal Hold & Litigation Readiness Exception Handling

Lifecycle processes shall include mechanisms for legal hold exceptions, preventing destruction or archival of data subject to investigation, litigation, or regulatory review.

2.11 DLM-11: Backup & Recovery Lifecycle Coordination

Backup copies shall be included in data lifecycle plans, with clear rules on retention duration, rotation frequency, and destruction aligned with primary data lifecycle phases.

2.12 DLM-12: System Decommissioning Data Handling

When decommissioning systems or applications, associated data shall be migrated, archived, or destroyed based on its lifecycle status and business continuity requirements.

2.13 DLM-13: Cross-Border Lifecycle Compliance

Data lifecycle enforcement shall account for regional regulatory requirements, including cross-border transfer constraints and jurisdiction-specific retention/destruction mandates.

2.14 DLM-14: Ownership-Driven Lifecycle Stewardship

Data owners shall be responsible for defining, reviewing, and approving lifecycle requirements for their respective data domains, in coordination with legal and compliance teams.

2.15 DLM-15: Business Process Integration of DLM

Data lifecycle rules shall be embedded into business processes and workflows, ensuring lifecycle actions (e.g., archival, deletion) occur without disruption to operations.

2.16 DLM-16: Data Storage Tiering Based on Lifecycle Phase

The organization shall implement data storage strategies (e.g., hot, warm, cold storage) aligned with the data’s current lifecycle stage to optimize cost, performance, and risk.

2.17 DLM-17: Periodic Lifecycle Policy Review & Updates

Lifecycle policies and schedules shall be reviewed at least annually to reflect changes in regulatory obligations, business requirements, or information systems architecture.

2.18 DLM-18: Shadow IT Lifecycle Control Enforcement

Processes shall be established to identify data stored or processed in unauthorized systems or applications (shadow IT) and apply appropriate lifecycle rules or remediation.

2.19 DLM-19: Lifecycle-Aware Data Migration Planning

When migrating data between systems or platforms, lifecycle stage, retention clock, and destruction requirements shall be preserved, validated, and documented.

2.20 DLM-20: Lifecycle Monitoring & Reporting

The organization shall implement monitoring and reporting mechanisms that track data across lifecycle stages, provide transparency into pending actions, and alert on violations.

2.21 DLM-21: Data Minimization & Lifecycle Entry Validation

Prior to data entering the lifecycle process, mechanisms shall be implemented to evaluate necessity, ensuring data collected or generated is minimal and purposeful for the intended function.

Section 3. Data Residency & Sovereignty (DRS)

The Data Residency & Sovereignty (DRS) control family addresses the geographic and jurisdictional considerations that govern where data is stored, processed, and transmitted. These controls ensure that organizations adhere to legal, contractual, and regulatory requirements specific to national and regional boundaries, while maintaining visibility and accountability for cross-border data flows. DRS emphasizes jurisdictional control, government access risk, and location-aware security postures, independent from classification or lifecycle status.

3.1 DRS-01: Data Residency Policy Development

The organization shall establish and maintain a data residency policy that defines requirements and restrictions for data storage, processing, and transmission based on geographic and jurisdictional constraints.

3.2 DRS-02: Jurisdictional Mapping of Data Assets

The organization shall maintain a current map of all geographic locations where data is stored, processed, or transmitted, including cloud data centers, backups, and third-party platforms.

3.3 DRS-03: Data Sovereignty Impact Assessment

A formal impact assessment shall be conducted to evaluate the legal and regulatory implications of storing or processing data in specific jurisdictions, including government access laws and data localization mandates.

3.4 DRS-04: Residency Requirements for Regulated Data Types

The organization shall define and enforce residency constraints for regulated data types in accordance with applicable laws and industry regulations.

3.5 DRS-05: Cross-Border Data Transfer Controls

The organization shall implement controls to monitor, log, and restrict cross-border data transfers, ensuring compliance with data transfer mechanisms such as SCCs, BCRs, or international agreements.

3.6 DRS-06: Cloud Provider Residency Declarations

Cloud service providers shall be required to disclose physical and logical locations of data storage and processing, and to provide mechanisms for region-specific data localization where applicable.

3.7 DRS-07: Data Sovereignty Clauses in Contracts

Vendor and third-party contracts shall include language that defines permitted data residency locations, handling obligations, and jurisdictional control boundaries.

3.8 DRS-08: Residency Enforcement through Technical Controls

The organization shall deploy technical controls (e.g., geofencing, region-locked storage, traffic routing policies) to enforce data residency requirements at the infrastructure and application layers.

3.9 DRS-09: Sovereignty Risk in Governmental Access Scenarios

The organization shall evaluate and document the risk of foreign government access to data based on where data resides or transits, and implement compensating controls as needed.

3.10 DRS-10: Residency-Aware Data Segmentation

Data shall be segmented logically and/or physically based on residency requirements, ensuring that data subject to localization mandates is isolated from unrestricted data.

3.11 DRS-11: Data Localization Exceptions Process

An approval process shall be established for exception requests to store or process data outside of its mandated jurisdiction, requiring legal, security, and business justification.

3.12 DRS-12: Residency Considerations in M&A and Divestitures

Data residency risks shall be assessed during mergers, acquisitions, or divestitures, with emphasis on inherited data locations, cloud regions, and legal jurisdiction changes.

3.13 DRS-13: Residency Verification in System Procurement

Prior to procuring or deploying new systems or services, data residency and sovereignty considerations shall be evaluated, documented, and approved.

3.14 DRS-14: Residency Constraints in Backup and Disaster Recovery

Data backups and disaster recovery processes shall maintain compliance with residency requirements, including the geographic location of backup sites and recovery systems.

3.15 DRS-15: Real-Time Visibility into Data Location

Systems shall provide real-time visibility into the geographic location of stored and processed data, including alerts on unauthorized movement or region changes.

3.16 DRS-16: International Data Transmission Logging

All international transmissions of sensitive or regulated data shall be logged, monitored, and reviewed for unauthorized transfers or violations of residency policies.

3.17 DRS-17: Role of Local Regulations in Data Lifecycle Planning

Residency and sovereignty requirements shall be factored into data lifecycle planning, particularly for archival, transfer, and destruction phases across multiple jurisdictions.

3.18 DRS-18: Localization for High-Risk Geographies

The organization shall define additional controls for data residing in high-risk jurisdictions, including enhanced encryption, monitoring, or migration strategies to safer regions.

3.19 DRS-19: Residency Review in Compliance Audits

Internal and external audits shall include verification of data residency adherence, including sampling of system logs, infrastructure configurations, and vendor claims.

3.20 DRS-20: Regional Legal Change Monitoring

The organization shall establish a mechanism for monitoring legal and regulatory changes related to data residency and sovereignty across all jurisdictions in which it operates.

3.21 DRS-21: Public Sector & National Contract Compliance

For public sector or national contracts, the organization shall implement controls ensuring strict compliance with country-specific data sovereignty mandates and hosting restrictions.

## Section 4.	User Data Rights Management (UDR)

User Data Rights Management (UDR) focuses on the organizational ability to operationalize and honor data subject rights as defined by privacy regulations, contractual obligations, or internal policy. These rights include—but are not limited to—access, rectification, erasure, restriction of processing, portability, and objection. UDR ensures the organization implements mechanisms that uphold individual autonomy and transparency regarding how their personal data is handled, independent of how that data is classified, where it resides, or its lifecycle status.

### 4.1	UDR-01: Data Rights Management Policy

The organization shall define and document a policy for managing user data rights in alignment with applicable privacy laws and contractual commitments.

### 4.2	UDR-02: Data Subject Rights Cataloging

The organization shall maintain a comprehensive catalog of data subject rights applicable across jurisdictions and business units, and identify overlaps, conflicts, and regulatory precedence.

### 4.3	UDR-03: Right-to-Know Request Mechanism

Mechanisms shall be implemented to allow individuals to submit "right to know" requests that provide visibility into what personal data the organization collects, processes, or shares.

### 4.4	UDR-04: Right-to-Access Fulfillment Workflow

A documented, repeatable workflow shall exist for fulfilling subject access requests (SARs) within legally mandated timeframes, including secure identity verification and audit logging.

### 4.5	UDR-05: Data Portability Protocols

The organization shall implement structured, machine-readable formats (e.g., JSON, CSV, XML) for providing portable copies of personal data to users upon request.

### 4.6	UDR-06: Right-to-Correction Procedures

Procedures shall be in place to allow individuals to request correction of inaccurate or incomplete personal data, with verification of updates across dependent systems and third parties.

### 4.7	UDR-07: Right-to-Erasure (“Right to Be Forgotten”) Enforcement

Where legally applicable, the organization shall implement processes to delete or anonymize personal data upon verified request, including propagation to backups and third-party systems when feasible.

4.8 UDR-08: Restriction of Processing Controls

Upon request and in applicable jurisdictions, personal data shall be flagged or logically segregated to restrict further processing, pending final resolution or verification of claims.

4.9 UDR-09: Objection to Processing Handling

Users shall have the ability to object to certain types of processing (e.g., direct marketing, profiling), and the organization shall evaluate and act on such objections promptly and in compliance with law.

4.10 UDR-10: Consent Management Framework

The organization shall implement mechanisms to collect, record, and manage user consent for data processing activities, including the ability to granularly revoke consent at any time.

4.11 UDR-11: Parental & Guardian Data Rights Support

For data subjects who are minors or legally dependent individuals, the organization shall accommodate data rights requests from parents or legal guardians with proper authorization.

4.12 UDR-12: Data Rights Identity Verification

Controls shall exist to authenticate the identity of users submitting data rights requests to prevent unauthorized access or manipulation of personal data.

4.13 UDR-13: Transparency of Data Rights Processes

The organization shall publish clear, accessible documentation outlining users' data rights, how to exercise them, and what to expect in terms of process and response timelines.

4.14 UDR-14: Localization of Rights Requests

Where data subjects reside in multiple jurisdictions, the organization shall localize the fulfillment of rights requests to reflect the most protective applicable standard.

4.15 UDR-15: Data Rights Training for Fulfillment Teams

Personnel responsible for responding to rights requests shall receive specialized training on regulatory requirements, internal procedures, and how to handle edge cases or escalation.

4.16 UDR-16: Rights Request Lifecycle Logging

Each data rights request shall be tracked from submission through closure, with timestamps, status updates, and responsible personnel logged for compliance and audit purposes.

4.17 UDR-17: Recurring Rights Request Analytics & Trends

The organization shall analyze trends in rights requests to identify systemic issues, improve service efficiency, and flag high-risk business processes or data sets.

4.18 UDR-18: Re-identification Risk Management in Responses

Where anonymized data sets are involved, the organization shall assess and mitigate re-identification risks before fulfilling data access, portability, or erasure requests.

4.19 UDR-19: Data Rights Dispute Resolution Process

A dispute resolution process shall be established for users who believe their data rights requests were denied improperly or handled in violation of policy or law.

4.20 UDR-20: Third-Party Rights Propagation Enforcement

Contracts and integrations with third parties shall include mechanisms for propagating user data rights requests (e.g., erasure, correction) and ensuring timely fulfillment by downstream entities.

4.21 UDR-21: Emergency Request Handling Criteria

The organization shall define criteria and an expedited path for urgent rights requests, such as those involving imminent risk to life, liberty, or safety.

Section 5. Data Loss Prevention (DLP)

The Data Loss Prevention (DLP) control family outlines the safeguards, monitoring, and enforcement mechanisms required to prevent unauthorized access, transfer, or exfiltration of sensitive data. These controls ensure the confidentiality of organizational, customer, and regulated data across endpoints, networks, cloud environments, and storage systems. Emphasis is placed on detection accuracy, policy enforcement, contextual awareness, and minimizing operational disruption while maximizing data protection effectiveness.

5.1 DLP-01: DLP Policy Definition and Classification Alignment

Organizations shall define DLP policies based on data classification schemes, ensuring alignment between DLP enforcement rules and the sensitivity levels assigned to data assets.

5.2 DLP-02: Endpoint DLP Agent Deployment

DLP agents shall be deployed on all managed endpoints with access to sensitive data, enabling monitoring, enforcement, and offline protection capabilities.

5.3 DLP-03: Network DLP Integration

DLP technologies shall be deployed at key network egress points to inspect outbound traffic and enforce policies on data in motion across email, web, and file transfer protocols.

5.4 DLP-04: Cloud DLP Enforcement

Cloud-native or integrated DLP controls shall be implemented to monitor and control data activity within sanctioned SaaS, PaaS, and IaaS environments.

5.5 DLP-05: Contextual DLP Enforcement

DLP solutions shall incorporate contextual attributes (e.g., user role, location, device posture, channel) to enforce adaptive policies and reduce false positives.

5.6 DLP-06: DLP Coverage for Removable Media

All attempts to copy, move, or export sensitive data to USB drives, external hard drives, and other removable media shall be monitored and governed by DLP policies.

5.7 DLP-07: Optical Character Recognition (OCR) for DLP

DLP solutions shall include OCR capabilities to inspect text embedded in images and scanned documents to prevent evasion of content inspection mechanisms.

5.8 DLP-08: Email DLP Rules Enforcement

DLP policies shall be applied to outbound emails, including subject, body, and attachments, with configurable actions for blocking, encryption, quarantining, or alerting.

5.9 DLP-09: Custom Data Identifier Support

Organizations shall define and use custom data identifiers within DLP tools to detect unique patterns, proprietary information, or industry-specific regulated content.

5.10 DLP-10: Shadow IT Discovery for Data Movement

DLP systems shall integrate with cloud access security brokers (CASBs) or other discovery tools to detect unauthorized use of unsanctioned cloud services for data transfers.

5.11 DLP-11: DLP Incident Workflow and Escalation

A defined incident handling workflow shall exist for DLP violations, including triage, impact analysis, escalation paths, and documentation of response actions.

5.12 DLP-12: DLP Exception Management

A formal process shall exist for requesting, approving, and tracking exceptions to DLP policies, with compensating controls and expiration dates applied.

5.13 DLP-13: Print Channel Monitoring

DLP controls shall monitor and optionally restrict printing of sensitive information based on content inspection, user role, or printer classification.

5.14 DLP-14: Data Fingerprinting and Exact Match Detection

DLP solutions shall support fingerprinting of structured and unstructured data sources (e.g., databases, files) for exact data matching and more accurate detections.

5.15 DLP-15: DLP False Positive/Negative Review Process

Organizations shall perform periodic tuning of DLP rules and detection models to minimize false positives and false negatives, informed by incident data and user feedback.

5.16 DLP-16: Offline DLP Enforcement

Endpoint DLP controls shall function in offline mode, enforcing critical policies even when devices are disconnected from the network.

5.17 DLP-17: DLP Control Testing and Simulation

Routine tests and simulations shall be conducted to evaluate the effectiveness of DLP controls in detecting and preventing policy violations across multiple channels.

5.18 DLP-18: Role-Based DLP Policy Differentiation

DLP rules shall be tailored based on user roles, departments, or business units to ensure proportional enforcement aligned with business needs and risk levels.

5.19 DLP-19: DLP Audit Logging and Forensics Readiness

All DLP events and actions shall be logged, time-synchronized, and retained for forensic investigation, compliance reporting, and incident correlation.

5.20 DLP-20: DLP Reporting and Risk Metrics

DLP systems shall generate dashboards and reports that include metrics such as policy violations, blocked events, incident trends, and risk rankings by channel and user.

5.21 DLP-21: Integration of DLP with Identity Context

DLP solutions shall integrate with identity systems to correlate violations with user attributes (e.g., department, clearance level), enabling enriched analysis and response.

5.22 DLP-22: Prohibited File Type Control via DLP

DLP tools shall enforce restrictions on specific file types that are commonly used for exfiltration or obfuscation of sensitive data (e.g., archives, encrypted containers).

5.23 DLP-23: Continuous Improvement of DLP Policies

Organizations shall conduct scheduled reviews of DLP policy effectiveness, adjusting rules and response strategies based on evolving threats, user behavior, and operational feedback.