Defense Information Systems Agency (DISA)

Office of the Chief Data Officer (OCDO)

Data Lifecycle Management Guidebook
Version 1

April 30, 2025

Executive Summary

Effective Data Lifecycle Management (DLM) is crucial for DISA to optimize the value of their data assets, ensure compliance with regulatory standards, data integrity, optimal utility and support strategic decision-making, support mission objectives, and mitigate risks associated with data mismanagement. As stewards of organizational data governance, OCDO's roles and responsibilities which include policy development, compliance enforcement, oversight, and strategic alignment to enable data-driven decision-making while safeguarding the data. The OCDO is responsible for overseeing the creation and implementation of the DLM Guidebook with the key responsibilities including defining the governance framework, ensuring alignment and compliance with regulations and policies, fostering collaboration across teams, providing tools and resources, and performing continuous improvement. The guidebook accompanies the DISAI (pending publication) to ensure the workforce has proactive guidance to follow best practices, processes, and responsibilities essential to managing data throughout the data lifecycle within our organization.

Approved By:

KUHARSKE.CAROLINE.R.1053209064

Digitally signed by KUHARSKE.CAROLINE.R.1053209064
Date: 2025.05.13 14:18:40 -04'00'

CAROLINE KUHARSKE
Director, Office of the Chief Data Officer
DISA Chief Data Officer

Version History

Version	Date	Description
1.0	2025-01-14	Initial Draft
1.1	2025-03-18	Updated Data Retention
1.2	2025-04-28	Added Security Controls

Table of Contents

1 Introduction

Defining, implementing, and overseeing a comprehensive data lifecycle management process is paramount within the Defense Information Systems Agency (DISA) to ensure consistent accuracy, security, and relevance of information assets. As the agency relies increasingly on data-driven decision-making, it is vital to have a clear, comprehensive structured framework that governs how data is created, stored, used, shared, and retired throughout its lifecycle. Without such a framework, data can become fragmented, outdated, or non-compliant, hampering the agency's ability to fulfill its mission and maintain the trust of its stakeholders. Effective data lifecycle management prevents data breaches, enhances operational efficiency, and ensures compliance with laws like the federal data strategy and the DoD Data Strategy. This guide aligns with the Department of Defense (DoD) Data, Analytics, and Artificial Intelligence Adoption Strategy prioritizing data as a strategic asset to enhance operational readiness. The guidebook is intended for all personnel responsible for managing, processing, and securing data within the DoD ecosystem.

In addition to establishing a robust lifecycle process, developing and using a Data Lifecycle Management Guidebook provides a unified point of reference that aligns personnel with best practices, regulatory requirements, and mission needs. This guidebook helps data stewards, data officers, data owners, IT and system administrators' teams, Leadership and decision-makers, data analysts and scientists, program and project managers, legal and compliance officers, cybersecurity personals, data governance teams, end users and operational personnel, external stakeholders and partners, record management officers, training and development teams understand their responsibilities and the standards to which they are expected to adhere. It ensures that all parties consistently apply the same criteria for data quality, classification, security, and accessibility. This consistency reduces confusion, enhances interoperability, and minimizes the risk of errors.

1.1 Purpose

Beyond outlining standardized policies, procedures, and practices, the DLM Guidebook covers the full spectrum of data lifecycle management. This includes planning and preparation, data source identification, assessment and evaluation, ADS approval and designation, implementation and integration of ongoing governance, retirement or redesignation, and training and support. Drawing on DoD, DISA, and federal regulatory requirements, as well as industry best practices, the Guidebook provides templates and decision-making frameworks that mitigate ambiguity and offer a consistent approach for users. The DLM Guidebook helps ensure robust data governance, streamlined compliance, and effective utilization of data assets across DISA.

1.2 Scope

The DLM Guidebook outlines the DoD/DISA/Federal policies, standards, regulatory requirements, and industry best practices related to data management ensuring that users can reliably navigate the complex landscape of data governance and compliance. The guidebook will also provide guidance on classifying and handling data based on sensitivity levels as described below, as well identifying and verifying classification requirements for specific storage and sharing protocols to mitigate risks of

unauthorized access. Additionally, the guidebook will include templates, and decision-making frameworks that reduce ambiguity and support consistent application of the process.

While the guidebook will focus on the principles and procedures needed to achieve effective data management lifecycle, it will not prescribe specific technologies or vendor solutions. Instead, it remains flexible and adaptable, allowing DISA to adjust its data management practices as requirements evolve and new capabilities emerge. Through this approach, the guidebook serves as a living document that continually supports the organization's data-driven operations, drives continual improvement, and fosters a culture of initiative-taking, responsible data stewardship.

1.3 Audience

The Data Lifecycle Management (DLM) Guidebook is intended for a broad spectrum of DISA stakeholders who play essential roles in the creation, handling, oversight, and retirement of data assets. The document is intended for OD1 personnel who establish and enforce data governance policies, and Program Management Offices (PMOs), which oversee the acquisition, implementation, and support of DISA systems, and Data Stewards/Owners, who hold ultimate responsibility for the content and utility of data sets. In addition, the Guidebook should be used by Data Managers, Data Engineers, and Data Analysts, which will interact with data, to ensure data quality, integrity, consistency, and availability throughout various mission-critical processes.

System Security Managers and Privacy SMEs will also use the guidebook to implement robust security controls and privacy safeguards that meet federal and DoD standards throughout the data lifecycle. In addition, Records Liaisons and Compliance Officers will find value, as they are tasked with ensuring that data handling aligns with retention schedules, legal requirements, and DoD/Federal mandates. Furthermore, stakeholders, such as contracting officers and leadership teams, will rely on the DLM Guidebook to inform decision-making, reduce ambiguity, and confirm that data assets are managed from inception to retirement.

1.4 Policy

This policy below guides and constraints the Data Lifecycle and Management Guidebook:

- DISA INSTRUCTION 270-50-9 LIFE CYCLE SUSTAINMENT PLANNING https://disa.mil/-/media/Files/DISA/About/Publication/Instruction/DISAI-270-50-9---Life-Cycle-Sustainment-Planning.ashx
- H.R.3987-National Archives and Records Administration Act of 1984 https://www.congress.gov/bill/98th-congress/house-bill/3987#:~:text=National%20Archives%20and%20Records%20Administration%20Act%20of%201984%20%2D%20Title%20I,the%20Archivist%20of%20the%20United

2 Data Lifecycle Management Process

The DISA Data Lifecycle Management Phases provide a structured approach to handling information assets throughout its entire lifecycle, from their initial planning, creation or acquisition and collection through its final disposal, ensuring alignment with DISA and DoD security requirements, goals, regulatory compliance, best practices and mission objectives. The DLM process includes policies, technologies, and methodologies to govern the flow of data throughout its various stages. It aims to optimize data usage, improve decision-making, and minimize risks while ensuring compliance with data protection and privacy regulations. The following sections describe the Data Lifecycle Management Phases along with the activities required and the expected outcomes.

The following figure outlines the sequence of the critical Data Lifecycle Management Phases:

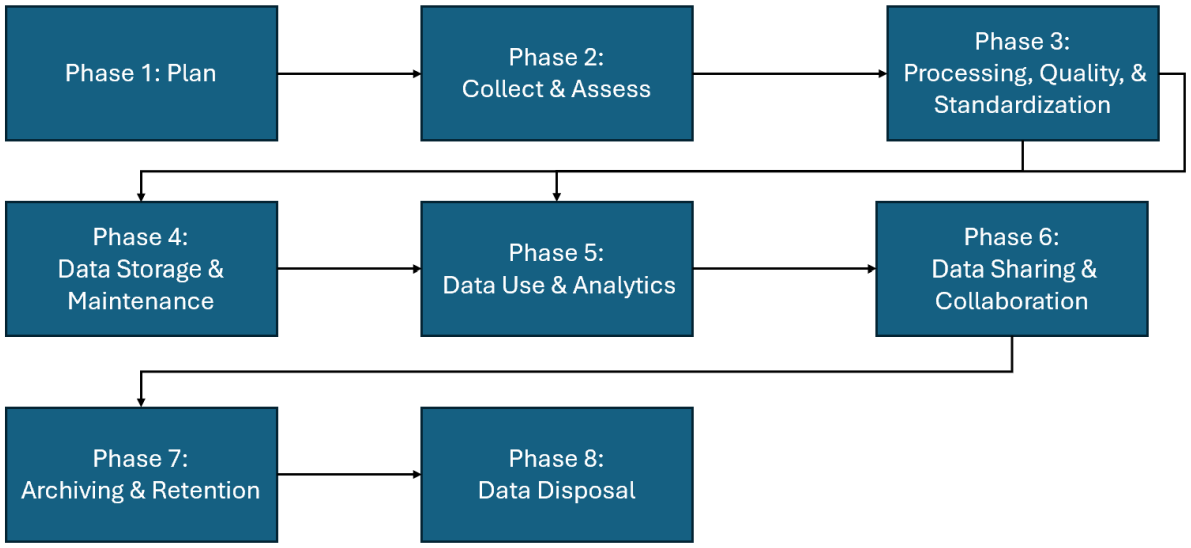

Figure - DISA Data Life Cycle Management Phases

2.1 Data Lifecycle Management Phase 1: Planning

The purpose of the DISA system's Data Lifecycle Management Planning phase is to ensure that every aspect of data handling is deliberately and strategically defined before any data enters the system. During this phase, DISA sets the overall vision and objectives for how the system's data will be governed, secured, and utilized in alignment with DoD directives. Key stakeholders determine data requirements, establish governance engagements, which address the system's unique security, privacy, classification, and performance needs. By conducting these activities upfront, DISA lays a solid foundation for subsequent lifecycle phases—such as data collection, storage, usage, and disposal—and ensures that data initiatives remain mission-focused and compliant.

The intent behind this planning phase is to mitigate risks and avoid costly rework or security breaches later in the lifecycle by integrating requirements from the start. DISA outlines how data will flow within the system, what tools and processes will be used, and how they will be monitored against metrics and Key Performance Indicators (KPIs). The planning phase also formalizes resource allocations—ensuring sufficient funding, technology, and personnel are available to meet mission demands and maintain compliance with regulations. By defining a clear roadmap and governance framework early on, the planning phase paves the way for a secure, efficient, and effective data environment that supports both current and future operational needs.

2.1.1 Planning Activities

1. ***Engage with Data Governance Council***
    - Engage with the Data Governance Council (DGC) to understand the required activities, roles and responsibilities.
    - Identify compliance requirements, applicable mandates and define accountability for data quality, security, and lifecycle decisions within the system context.
2. ***Data Management Plan (DMP) Development***
    - Create a plan that outlines how data will be collected, stored, protected, used, and shared by this specific system.
    - Incorporate references to relevant STIGs (e.g., database STIG, network STIG) and the RMF process, including categorization of the system under **NIST SP 800-53** controls.
3. ***Risk and Compliance Assessment***
    - Identify all applicable standards (DoDI 8500.01, DoDI 8510.01, DISA STIGs, NIST SP 800-53, etc.).
    - Document on how each requirement will be satisfied, noting any potential gaps and planned mitigation actions.
    - Include classification handling procedures (markings, access controls, cross-domain solutions if necessary).
4. ***Define System Data Requirements and Architecture***
    - Determine data formats, schemas, and metadata standards that the system will use.
    - Decide on data flows (how data enters the system, is processed, stored, and eventually disseminated) and cross-system interfaces (System Interface View (SV-1) and System Interface Matrix (SV-6).
5. ***Set Performance Metrics and KPIs***
    - Define how success will be measured: data quality thresholds, availability requirements, incident response times, compliance check frequency, etc.
    - Establish methods for continuous monitoring and reporting to key stakeholders.
6. ***Resource and Budget Planning***
    - Identify hardware, software, and personnel needed to implement the data management plan.
    - Align requests with DISA's budget cycle or existing contracts (e.g., cloud service providers authorized under FedRAMP/DoD SRG).

2.1.2 Outcome

The expected outcome of the DISA Data Lifecycle Planning phase is a well-structured framework that guides how data will be handled from acquisition through disposal and appropriately mitigates risk. By the end of this phase, all stakeholders should share a clear understanding of the data governance requirements, compliance obligations, system architecture, resource needs, and performance measures. This unified roadmap not only integrates security and privacy considerations from the start but also aligns data objectives with broader DISA and DoD strategies, paving the way for efficient, compliant, and mission-focused data operations in the subsequent lifecycle phases.

2.2 Data Lifecycle Phase 2: Collect and Assess

The purpose of the Data Lifecycle Management Data Collection and Assessment phase is to gather information from authorized sources while simultaneously evaluating its quality, security, and relevance.

During this phase, DISA establishes secure and standardized processes—such as ETL pipelines, direct connections, or API integrations—to bring data into controlled environments in accordance with STIGs and DoD directives. Collected data is then assessed for completeness, accuracy, and adherence to classification guidelines, ensuring that it meets both operational needs and federal requirements. Processes used for ongoing assessment and validation should be automated to the maximum extent possible. By conducting thorough quality checks and initial validation at this stage, DISA significantly reduces the risk of propagating errors or vulnerabilities into subsequent data lifecycle phases. This phase identifies where data is created or collected, defines attributes such as data origin, timestamps, and classification levels. Also, establishes protocols for labeling data with sensitivity levels like "Unclassified," "CUI," "Confidential," or "Top Secret." Once data is generated or collected, it moves into storage. Metadata tagging, classification, and organization happen at this stage for easy retrieval and compliance.

The intent behind Data Collection and Assessment is to guarantee that all data is properly acquired and meticulously vetted before it is used to support operations, analyzed, shared, or stored. This involves implementing security protocols such as encryption in transit, identity and access management, and logging mechanisms to maintain traceability and reduce exposure to cyber threats.

Ultimately, by focusing on collection and assessment, DISA establishes a strong foundation for trustworthy, high-quality data that effectively supports mission objectives and compliance obligations.

2.2.1 Collect and Assess Activities

1. ***Identify Authorized Data Sources***
    - Catalog internal DoD systems, external agencies, or sensor networks that are permitted to provide data.
    - Validate each source's legitimacy, security posture, and classification level to ensure compliance with DoD and DISA policies.
2. ***Set Up Secure Data Collection Processes***
    - Implement Extract, Transform, and Load (ETL) processes or real-time integration points (e.g., APIs, message queues) that comply with STIG guidelines.
    - Configure encryption in transit (e.g., TLS) and boundary protection controls to prevent unauthorized access or data tampering.
3. ***Apply Access Controls and Audit Logging***
    - Enforce role-based access and authentication methods consistent with DoD cybersecurity directives (e.g., DoDI 8500.01).
    - Configure comprehensive logging and auditing to capture the details (time stamp, user ID, data source) of each data transfer event for traceability.
4. ***Data Validation and Classification Enforcement***
    - Conduct automated or semi-automated checks (e.g., format validation, schema matching, etc.) to confirm data quality and completeness.
    - Verify alignment with classification guidelines (e.g., Unclassified, CUI, Secret, Top Secret), ensuring the appropriate labeling is carried over into the environment.
5. ***Assess Data Quality and Relevance***
    - Examine the accuracy, completeness, and timeliness of the incoming data against predefined quality metrics or thresholds.

- Determine whether the data meets the system's mission requirements; appropriately handle data that fails validation to prevent contamination of downstream processes.

6. ***Apply Privacy and Compliance Requirements***
   - If personally identifiable information (PII) or other sensitive data is present, ensure that privacy protocols (e.g., Privacy Act, HIPAA if applicable) and DoD rules are followed.
   - Document any special handling instructions or consent requirements that apply to sensitive records.
   - Ensure data is compliant with DISA and DOD standards.
7. ***Document and Track Data Artifacts***
   - Update data inventories, catalogs, or metadata repositories to reflect newly collected datasets, including source details, ingestion date, and classification.
   - Record any issues or anomalies discovered during assessment (e.g., missing fields, duplicates) to drive improvements or remediation.
   - Update DISA Data Catalog with the system's data dictionary and/or other contextual artifacts.
8. ***Feedback to Stakeholders***
   - Communicate data acceptance or rejection decisions, along with any quality issues, to relevant Program Offices and Data Stewards.
   - Provide reports or dashboards summarizing ingestion metrics, error rates, and overall compliance status.

2.2.2 Collect and Assess Outcomes

The outcome of the Data Collection and Assessment phase of the data lifecycle is a validated, securely ingested dataset that meets DoD classification, quality, and compliance standards. Through rigorous source verification, secure ingestion processes, and thorough data checks (e.g., schema validation, classification labeling, privacy, and DoD and DISA standards compliance), any substandard or improperly classified data is appropriately handled before it can impact downstream processes. Consequently, this phase ensures that only trusted, relevant, and properly categorized data enters the agency's environment, establishing a solid foundation for effective analytics, decision-making, and subsequent data lifecycle activities.

2.3 Data Lifecycle Phase 3: Data Processing, Quality, and Standardization

The purpose of the Data Processing, Quality, and Standardization phase is to transform data into a secure, high-integrity state that aligns with DISA and DoD-wide standards and supports operational requirements. During this phase, various cleansing and standardization techniques are employed—such as de-duplication, format conversions, and field validations—to eliminate errors, inconsistencies, and security risks. Simultaneously, the data's classification labels and metadata are updated as needed, ensuring each record remains compliant with both DISA-specific guidelines and broader STIG requirements. By completing these processes, DISA ensures that the data is ready to effectively support mission-critical operations, analysis, and decision-making.

The intent behind Data Processing, Quality, and Standardization is to guarantee that all incoming information, regardless of its original source or format, can be made fit-for-purpose and seamlessly integrated into the DISA environment without introducing quality gaps or security vulnerabilities. This

phase relies on strict adherence to established data standards and governance policies, including defined naming conventions, reference data usage, and alignment with DoD data models. Through continuous quality checks and standardization activities, DISA minimizes the time and resources required in later stages—such as analytics and archiving—while maximizing confidence in the data's accuracy and reliability.

2.3.1 Data Processing, Quality, and Standardization Activities

1. ***Data Cleansing and Validation***
    - Identify and correct incomplete, incorrect, or improperly formatted entries (e.g., null values, invalid data types, out-of-range fields).
    - Verify that data follows existing schema definitions and metadata requirements, rejecting or flagging problematic records for further review.
2. ***Standardization and Transformation***
    - Convert data to standardized formats and units in line with DISA and DoD-wide conventions (e.g., consistent date formats, naming conventions, reference codes).
    - Re-map or restructure fields and/or data format as necessary to align with the system's data model or comply with DISA/DoD data models.
3. ***Data Quality Checks and Metrics***
    - Establish and monitor key quality indicators (e.g., accuracy, completeness, consistency) against predefined thresholds.
    - Produce reports or dashboards that highlight error rates, trends, and ongoing improvement areas, feeding results back to governance bodies and data stewards.
4. ***Master Data and Reference Data Management***
    - Integrate authoritative reference data (e.g., official DoD unit codes, organizational lists) to standardize key fields.
    - Maintain or update master data records (the "single source of truth") to ensure uniformity and reduce redundancy across the agency's systems.
5. ***Security and Classification Adjustments***
    - Confirm that each record carries the correct classification label (Unclassified, CUI, Secret, Top Secret) in accordance with DoD directives and STIG requirements.
    - If necessary, update classification tags when data is combined or transformed, ensuring that no sensitive information is inadvertently downgraded or exposed.
6. ***De-duplication and Consolidation***
    - Identify and merge duplicate entries using defined matching criteria (e.g., unique IDs, system-of-record checks, fuzzy matching techniques).
    - Consolidate overlapping records into a single, authoritative representation, tracking changes for auditability and maintaining data lineage.
7. ***Documentation of Transformation Workflows***
    - Create and maintain detailed logs or metadata describing each transformation step, including mapping rules, applied algorithms, and software tools used.
    - Record versioning information (e.g., scripts, ETL pipelines) to ensure repeatability and transparency for future audits or reviews.
    - Update DISA Data Catalog with any updates made to the system's data dictionary.
8. ***Governance Oversight and Continuous Improvement***
    - Involve DGC or designated data stewards to review processing standards, approve significant changes, and resolve escalated issues.

- Capture lessons learned and best practices for refining future data processing methods or enhancing automation where feasible.

2.3.2 Data Processing, Quality, and Standardization Outcomes

The outcome of the Data Processing, Quality, and Standardization phase of the DISA Data Lifecycle is secure, accurate, and fit-for-purpose data that adheres to DISA and DoD standards. Through targeted cleansing, normalization, classification verification, and rigorous quality checks; any errors, duplicates, or inconsistencies are identified and resolved before they can impact later stages in the lifecycle. As a result, data emerges with improved integrity, clear lineage, and the correct classification labels—thereby reducing operational risks, improving interoperability across DoD components, and ensuring readiness for advanced analytics, sharing, and subsequent phases.

2.4 Data Lifecycle Phase 4: Data Storage and Maintenance

The purpose of the Data Storage and Maintenance phase is to securely house data in a manner that guarantees its availability, integrity, and confidentiality in alignment with DISA and DoD cybersecurity and operational directives. During this phase, datasets—already processed and standardized—are stored in accredited environments that meet DISA's security requirements, such as compliance with relevant STIGs and the Risk Management Framework (RMF). Proper configuration and monitoring of storage systems, along with rigorous backup and disaster recovery procedures, help ensure continuity of operations. By focusing on performance tuning, access controls, and regular maintenance tasks, DISA minimizes the risk of data loss, unauthorized access, and system downtime.

The intent behind Data Storage and Maintenance is to provide a stable and resilient foundation for subsequent phases such as data usage, analytics, and sharing across the broader DISA and DoD enterprise. This includes implementing role-based access controls, encryption of data at rest, and continuous monitoring to detect threats or anomalies. Regular patching, capacity planning, and performance optimization further extend the lifecycle of critical infrastructure while maintaining compliance with DISA, DoD and federal regulations. Ultimately, by treating storage as a dynamic asset that requires vigilant maintenance, DISA strengthens its ability to provide reliable, mission-critical services to the warfighter and national leadership.

2.4.1 Data Storage and Maintenance Activities

1. ***Infrastructure Provisioning and Configuration***
   - Establish or maintain storage environments (e.g., on-premises data centers, DISA cloud environments, IL5/IL6-accredited cloud platforms) that comply with DoD security requirements.
   - Configure operating systems, databases, and file systems in alignment with relevant STIGs (e.g., database STIG, OS STIG) and the Risk Management Framework (RMF) accreditation guidelines.
2. ***Encryption and Access Controls***
   - Implement encryption at rest (e.g., AES-256) and in transit (TLS 1.2+), ensuring that data is protected from unauthorized access.

- Enforce role-based access with strict privilege assignments, multi-factor authentication (MFA), and continuous authorization monitoring to detect unauthorized activities.

3. ***Logging, Monitoring, and Intrusion Detection***
   - Enable comprehensive audit logging for all data-related operations (e.g., reads, writes, administrative changes) to support traceability and incident response.
   - Deploy intrusion detection systems (IDS) and/or intrusion prevention systems (IPS), as well as SIEM tools, to identify anomalies or malicious behavior in real time.
4. ***Backup, Disaster Recovery, and Continuity Planning***
   - Schedule routine backups (full, incremental) of critical datasets and maintain secure offsite or cloud-based copies.
   - Define and test disaster recovery (DR) plans and Continuity of Operations (COOP) scenarios, ensuring alignment with RPO (Recovery Point Objective) and RTO (Recovery Time Objective) metrics.
   - Periodically validate backups to confirm data integrity and restore procedures.
5. ***Capacity Planning and Performance Optimization***
   - Monitor storage usage, I/O performance, and system resource consumption to avoid bottlenecks or resource exhaustion.
   - Conduct performance tuning (e.g., indexing strategies, load balancing) and consider storage tiering (hot/warm/cold) for cost-efficiency.
   - Forecast future storage and determine needs based on expected data growth rates.
6. ***Patch Management and Vulnerability Scanning***
   - Regularly apply security patches and firmware updates to storage infrastructure, operating systems, and supporting components.
   - Conduct vulnerability assessments (e.g., Nessus scans) to identify and remediate potential weaknesses, following DISA STIG compliance guidelines.
7. ***Data Versioning and Lifecycle Tracking***
   - Maintain version histories of key data sets, capturing modifications over time (especially important for mission-critical data sets).
   - Update and manage metadata (e.g., classification, owner, creation date) to track each data set's lifecycle phase and applicable retention periods.
8. ***Ongoing Governance and Compliance Audits***
   - Involve security teams to review storage configurations and adherence to DoD directives and policies.
   - Conduct periodic audits (e.g., IG inspections, RMF continuous monitoring) to verify that data remains secure, accurately classified, and aligned with operational requirements.

2.4.2 Data Storage and Maintenance Outcomes

The outcome of the Data Storage and Maintenance phase is a reliable, secure, and continuously monitored environment where DOD's data is preserved in compliance with DISA and DoD directives. By implementing robust encryption, access controls, backups, and intrusion detection measures, any threats or failures can be quickly identified and mitigated, minimizing disruptions to operations. Simultaneously, capacity planning and performance optimization ensure data remains consistently available, while ongoing governance and compliance checks uphold classification requirements and STIG guidance. Additionally, there should be a storage environment that supports operational requirements. i.e. appropriate storage type, speed of data retrieval, and the ability to integrate with other apps. This

lays the foundation of trust and dependability, which enables subsequent phases—such as analytics, sharing, and archiving—to proceed with confidence in the data's integrity and readiness.

2.5 Data Lifecycle Phase 5: Data Use and Analytics

The purpose of the Data Use and Analytics phase is to extract actionable insights from data in a way that directly supports military and national security objectives. During this phase, information from various DISA and DoD sources is aggregated and leveraged to enable operational capabilities such as data visualization, business intelligence, and AI/ML. Continuous development and integration of these capabilities is critical to operationalizing data and leveraging data as a strategic asset.

The intent behind the Data Use and Analytics phase is to ensure that data realizes its full potential in bolstering mission readiness and strategic planning. To achieve this, analytics must be conducted within a secure environment that complies with DISA and DoD classification and privacy regulations, while still delivering rapid insights relevant to respective stakeholders. This often involves role-based access to analysis tools and continuous performance monitoring of data and AI/ML pipelines. In addition to the optimization of existing capabilities, this phase requires continuous commitment to research, development, and adoption of emerging analytic and information technologies. Successful execution of this phase will maximize the value extracted from data and enhance the DoD's overall capacity to respond effectively to mission challenges.

2.5.1 Data Use and Analytics Activities

1. ***Data Provisioning and Preparation***
    - Identify the specific data sets needed for each analytical project or use case, pulling from secure repositories or data warehouses maintained in previous phases.
    - Apply additional filtering, aggregation, or metadata tagging if required by the analytical requirements.
    - Apply feature engineering, preprocessing, and/or any other technical processes required to prepare data for its respective use case(s).
    - Version control processes and actions taken to prepare data.
2. ***Analytics Environment Setup***
    - Ensure that all analytical tools (e.g., business intelligence (BI) platforms, data science notebooks, AI/ML frameworks) are configured in accordance with DISA STIG requirements and risk management guidelines.
    - Establish sandboxes or development environments as needed for personnel to experiment with new algorithms, ensuring strict segmentation and classification controls.
3. ***Role-Based Access Controls and User Training***
    - Assign and manage access privileges so that only authorized personnel, and when required, only those with valid access and the correct security clearance—can use specific datasets or analytics tools.
    - Provide training or documentation on how to leverage available dashboards, self-service analytics, and reporting features securely, emphasizing the importance of adhering to classification and sharing rules.
4. ***Descriptive, Diagnostic, and Predictive Analytics***

- Perform descriptive analytics (reports, dashboards) to summarize historic events, helping leadership and stakeholders understand the data.
- Use diagnostic analytics (root-cause analysis, anomaly detection) to uncover patterns, correlations, or potential issues that contribute to events or outcomes.
- Develop and train AI/ML models from feature datasets to predict information and/or prescribe actions.

Implement AI/ML inference pipelines to transform data and integrate AI/ML models and their outputs with production processes and tools.

5. ***Visualization and Reporting***
   - Develop dashboards, charts, and visual narratives to present information in a format and level of granularity appropriate for respective stakeholders. Automate reporting and/or alerts for recurring processes (e.g., network performance monitoring, security incident detection).
6. ***Collaboration and Sharing***
   - Share insights or analytical results with designated stakeholders—such as mission commanders, joint staff, or coalition partners—using approved communication channels and classification boundaries.
   - Conduct review sessions or briefings to discuss outcomes, gather feedback, and refine analytical models or assumptions for continuous improvement.
7. ***Performance Monitoring and Continuous Improvement***
   - Track information such as AI/ML model metrics, user adoption, and system resource usage.
   - Regularly evaluate the effectiveness of analytical approaches, develop new features, retrain AI/ML models as needed, and integrate lessons learned into future data use strategies.
8. ***Governance and Compliance Oversight***
   - Keep appropriate stakeholders informed of any data usage issues, model biases, or compliance concerns that arise during analytics.
   - Document and version control methodologies, transformations, and outputs to maintain transparency, support audits, and ensure compliance with DISA and DoD regulations, privacy and data standards.

2.5.2 Data Use and Analytics Outcomes

The outcome of the Data Use and Analytics phase is a suite of actionable insights and improved capabilities that support DISA's operational and strategic objectives. Leveraging advanced analytical methods—ranging from descriptive reporting to prescriptive modeling will enable DISA to operationalize data and facilitate an information advantage throughout the broader DoD environment.

2.6 Data Lifecycle Phase 6: Data Sharing and Collaboration

The purpose of the Data Sharing and Collaboration phase is to enable the secure and efficient exchange of information across the DoD and with approved external partners, and allied organizations. In this phase, data is made accessible to stakeholders at the speed of mission relevance—ensuring, insights and

data can be shared, integrated, or aggregated for operational use. Strict compliance with classification levels, encryption protocols, and role-based access controls are maintained, preventing unauthorized disclosure or tampering. By bridging previously siloed information sources, this phase significantly improves cross-functional collaboration, reduces redundancy, and supports unified mission planning and execution.

The intent behind Data Sharing and Collaboration is to maximize the value and interoperability of DISA's data assets, in alignment with DISA and DoD directives for transparency and combined operations. The phase requires the establishment and enforcement of data sharing agreements, such as Memoranda of Understanding (MOUs) or Service-Level Agreements (SLAs). These agreements articulate the conditions under which data can be shared, reused, or integrated. Secure cross-domain solutions may be employed to handle information at different classification levels while ensuring that all security measures remain intact. By focusing on controlled data dissemination and teamwork, this phase facilitates a more cohesive, timely, and informed decision-making process across the DoD ecosystem.

2.6.1 Data Sharing and Collaboration Activities

Below is a set of detailed activities that occur in the Data Sharing and Collaboration phase. These activities focus on enabling secure, controlled information exchange between authorized stakeholders—both within and outside the DoD—while strictly adhering to classification, privacy, and policy requirements.

1. ***Identify Approved Sharing Partners and Agreements***
    - Determine which internal DoD components, external agencies, allied nations, or commercial partners are authorized to receive or contribute data.
    - Develop or reference Memoranda of Understanding (MOUs), Data Sharing Agreements, Service-Level Agreements (SLAs), or other appropriate artifacts that specify the specific data being shared, roles, responsibilities, classification boundaries, and acceptable use conditions.
2. ***Implement Secure Data Transfer Mechanisms***
    - Configure secure file transfers, APIs, or web services that comply with DISA STIGs and encryption standards (e.g., TLS 1.2 or higher).
    - For data moving between domains of different classification levels (e.g., Unclassified to Secret), implement cross-domain solutions (CDS) that meet DoD requirements for data sanitization and inspection.
3. ***Enforce Classification and Access Controls***
    - Ensure that data retains its correct classification markings (e.g., CUI, Secret, Top Secret) throughout the sharing process.
    - Map role-based access controls (RBAC) and multi-factor authentication (MFA) to each sharing partner, limiting data access to those with a legitimate need-to-know and the correct clearance.
4. ***Metadata and Cataloging for Discoverability***
    - Publish metadata and data descriptions in the DISA Data catalog or that authorized stakeholders can query to locate relevant datasets.
    - Include classification labels, data provenance, contact information for data stewards, and usage restrictions in the metadata to avoid misuse or confusion.
5. ***Compliance Checks***

- Use security monitoring and intrusion detection tools to log and scrutinize data transfers, ensuring they comply with STIGs, classification policies, and data handling rules.
- Conduct periodic manual reviews or compliance audits to confirm that data-sharing activities match approved agreements and do not violate privacy or security regulations.

6. ***Auditing and Traceability***
   - Maintain comprehensive logs of data access, sharing events, and any transformations performed to facilitate the transfer (e.g., anonymization, format conversions).
   - Retain these logs for compliance with DoD or legal requirements, enabling rapid investigation of anomalies or potential incidents.
7. ***Determine Collaboration Tools and Platforms***
   - Provide secure collaboration environments (e.g., DISA and DoD cloud portals, mission-specific websites, SharePoint sites) where authorized users can co-edit and discuss shared data.
   - Configure these tools to align with each dataset's classification level, preventing unauthorized cross-contamination or disclosure of sensitive information.
8. ***Ongoing Governance and Stakeholder Engagement***
   - Keep DGC and other data governance boards and security officers updated on new or revised sharing agreements, tool integrations, and potential risks.
   - Gather stakeholder feedback on data usability, quality, and timeliness, feeding any lessons learned back into continuous improvement efforts for sharing processes.

2.6.2 Data Sharing and Collaboration Outcomes

The outcome of the Data Sharing and Collaboration phase is a secure, well-coordinated environment in which information flows seamlessly to authorized partners—both within and beyond DISA and DoD—while adhering to classification, privacy, and policy controls. By effectively implementing role-based access, encryption, cross-domain solutions, and detailed data-sharing agreements, DISA minimizes unauthorized disclosures and enhances interoperability across diverse systems. As a result, stakeholders gain timely access to accurate data, enabling more effective collaboration and decision-making that strengthens mission execution and readiness throughout the broader DoD.

2.7 Data Lifecycle Phase 7: Archive and Retention

The purpose of the Archive and Retention phase is to preserve records and information in accordance with DISA, DoD and federal mandates, ensuring data remains accessible and secure throughout its lifecycle. During this phase, data is migrated across appropriate storage solutions, whether on-premises or cloud-based. Policies around storage solutions (i.e., hot/cold) should balance operational requirements with cost-optimization and should be configured to migrate information automatically. This phase includes implementing approved records retention schedules that align with National Archives and Records Administration (NARA) guidelines, DISA and DoD policy, thereby upholding compliance and reducing the risk of inadvertent data destruction. By *archiving* data responsibly, DISA fulfills regulatory obligations and improves the overall performance and manageability of active systems.

The intent behind Data Archive and Retention is to safeguard valuable knowledge, maintain clear audit trails for operational and legal requirements, and ensure the appropriate information is available to support operations at a speed of mission relevance. Proper classification, metadata tagging, and indexing of archived datasets enable authorized personnel to retrieve essential records rapidly for future use—such as historical analysis, legal discovery, or policy review. At the same time, the process ensures that irrelevant or outdated data is not retained indefinitely, minimizing security vulnerabilities and storage costs. Overall, this phase is crucial in promoting efficient data governance, risk mitigation, and the long-term continuity of DISA's mission-critical information.

2.7.1 Archive and Retention Activities

Below is a set of detailed activities that occur in the Data Archive and Retention phase. These activities ensure that data is retained according to federal, DoD, and DISA-specific regulations, while remaining accessible if required for future reference or legal obligations.

1. ***Identify Data for Archive and Retention Schedules***
    - Review data within active repositories or databases to determine if they meet criteria for long-term storage or reduced access.
    - Apply approved DoD/DISA retention schedules (aligned with National Archives and Records Administration [NARA] guidelines) to classify data as temporary or permanent records.
    - Consult DGC and other data governance and legal teams to confirm any special exceptions for records under litigation holds or ongoing operational use.
2. ***Archive Storage Planning and Configuration***
    - Choose a cost-effective, secure long-term storage solution (e.g., on-premises cold storage, IL5/IL6-accredited cloud) that meets DISA's and DoD's security requirements.
    - Configure appropriate encryption at rest, access controls, and logging for the archival environment, ensuring continued compliance with STIG and RMF directives.
3. ***Metadata Tagging and Cataloging***
    - Assign or update metadata and classification labels to reflect the archived status, retention period, and disposition instructions.
    - Record relevant details—such as data owner, origin, creation date, and next review date—in the appropriate records management system for discoverability.
    - Update the DISA Data Catalog based on updated classification labels and metadata.
4. ***Data Migration and Integrity Checks***
    - Execute secure data transfers from primary storage to the archival environment, applying encryption in transit (e.g., TLS) and validating integrity through checksums or hashing.
    - Perform quality checks post-migration to confirm completeness, accuracy, and compliance with security policies before finalizing archival storage.
5. ***Access and Retrieval Processes***
    - Define procedures and privileges for authorized personnel to retrieve archived data if required for audits, historical analytics, or legal discovery.
    - Implement role-based or attribute-based access controls, ensuring only users with the correct clearance and need-to-know can view sensitive archived data.
6. ***Monitoring and Lifecycle Management***

- Monitor the archived data for integrity over time, running periodic integrity checks and verifying storage media health.
- Track the retention schedule for each dataset, generating automated alerts when data is due for further retention reviews or final disposition.

7. ***Compliance and Governance Reviews***
   - Conduct periodic audits to ensure adherence to NARA, DoD, and DISA records management policies, addressing any gaps or inconsistencies.
   - Update DGC and other governance bodies—such as Data Stewardship Councils or Records Management Boards—on archival status, volumes, and any challenges encountered.

2.7.2 Archive and Retention Outcomes

The outcome of the Data Archive and Retention phase is a legally compliant, systematically organized, and readily retrievable collection of historical records and data. By carefully classifying and securing these datasets in long-term storage—while maintaining detailed metadata, audit trails, and applicable retention schedules, DISA ensures that information remains available for future operational needs, legal discovery, or historical analysis. This phase also optimizes active system performance and reduces storage costs by removing obsolete data, thereby promoting efficient resource utilization and strengthening overall data governance.

2.8 Data Lifecycle Phase 8: Data Disposal

The purpose of the Data Disposal phase is to securely and permanently remove data that has reached the end of its lifecycle or is no longer needed for operational, legal, or historical purposes preventing unauthorized access or misuse. Following established DISA, DoD and federal records management guidelines, DISA identifies data eligible for disposal and employs approved methods—such as secure wiping, degaussing, or physical destruction—to prevent unauthorized recovery of sensitive information. By carrying out data disposal in a controlled, auditable manner, DISA mitigates the risk of inadvertent disclosures, decreases cyber exposure, and optimizes storage costs. This phase ensures that the agency retains only the data required to fulfill the current mission and compliance mandates.

The intent behind Data Disposal is to maintain a lean and secure data footprint while upholding the stringent security requirements demanded by DISA and DoD operations. By enforcing precise disposal schedules, documenting destruction events, and adhering to all legal obligations—such as the Federal Records Act and relevant NIST standards, DISA prevents over-retention of data that no longer serves a valid purpose. This disciplined approach not only addresses potential compliance issues but also strengthens overall data governance and reduces the threat surface of the agency's information systems, preserving the integrity and confidentiality of mission-critical operations.

2.8.1 Data Disposal Activities

Below is a set of detailed activities that typically occur in the Data Disposal phase. These activities ensure that data is no longer needed—whether due to expiration of retention periods, end of operational usefulness, or resolution of legal obligations, and is securely and permanently removed from DISA's active and archived environments.

1. ***Identify Data Eligible for Disposal***
    - Review all datasets with expired retention schedules or those deemed non-essential based on mission, legal, or regulatory criteria (e.g., Federal Records Act, agency policies).
    - Confirm that no litigation holds, investigations, or ongoing operational requirements apply to the data in question.
2. ***Verify Classification and Disposal Requirements***
    - Determine the classification level of the data (e.g., Unclassified, CUI, Secret, Top Secret) and whether special handling rules apply (e.g., SCI compartments, cryptographic keys).
    - Consult DoD, DISA, or NIST guidelines (e.g., NIST SP 800-88 for media sanitization) to select disposal methods appropriate to the data's sensitivity.
3. ***Secure Removal or Sanitization***
    - Carry out destruction or sanitization processes in accordance with DISA STIG requirements and DoD media sanitization policies. Methods may include secure overwriting, degaussing, encryption key destruction, or physical destruction (e.g., shredding, incineration) for highly classified or sensitive materials.
    - Ensure that any storage media used (e.g., magnetic tapes, hard drives, SSDs, optical discs) undergoes thorough sanitization, so that data remnants cannot be retrieved.
4. ***Documentation and Audit Trail***
    - Record each disposal event with detailed logs, including the data type, classification level, disposal date, method used, and personnel involved.
    - Maintain certificates of destruction or equivalent proof that data and media were handled according to established procedures, preserving traceability for audits or inspections.
5. ***Post-Disposal Compliance Checks***
    - Conduct internal or third-party verification to confirm that no recoverable data remains on the sanitized media or in the environment (e.g., caches, backups, cloud snapshots).
    - Conduct quality assurance checks to ensure disposal processes comply with standards.
    - Report final disposal activities to DGC and other data governance boards or records management officials as necessary, ensuring full alignment with DISA, DoD and federal regulations.
6. ***Update Inventories and Metadata***
    - Remove or update any entries in the DISA data catalog, asset inventories, or records management systems to reflect that the dataset or media has been permanently disposed.
    - Ensure metadata is updated to show that the data no longer exists.
    - Notify data owners and custodians that disposal is complete, closing the loop on the data's lifecycle.

2.8.2 Data Disposal Outcomes

The outcomes of the DISA Data Management Lifecycle Data Disposal phase are secure destruction of data, regulatory compliance, optimized data management, enhanced organizational trust and irreversible removal of data that has met its retention or operational requirements. Through approved destruction methods—such as degaussing, secure overwriting, or physical destruction, DISA prevents unauthorized retrieval of sensitive or classified information, while comprehensive disposal documentation and audit logs maintain clear evidence of regulatory adherence. As a result, the

organization reduces both storage overhead and risk exposure, ensuring that only mission-critical or legally mandated data remains active in the environment.

2.9 Data Lifecycle Management Training Requirements

A comprehensive training program is essential to ensure that all users and stakeholders are involved in the DISA Data Lifecycle Management (DLM) process thoroughly understand the policies, procedures, and best practices governing each phase. This includes everyone from DISA Chief Data Officer Office personnel, Data Stewards and System Administrators to Program Managers and Compliance Officers, all of whom play critical roles in maintaining the accuracy, security, and availability of DISA's data assets. By structuring training content to align with the DLM phases, stakeholders can see exactly how their responsibilities integrate into the broader lifecycle.

The following are the different types of training that will be provided for the various roles that are part of the DLM process:

Planning the Training Program

1. ***Needs Assessment and Role Identification***
    - Begin by identifying the various roles involved in the DLM process (e.g., Data Stewards, System Admins, Program Managers, Security/Privacy SMEs, Records Liaisons).
    - Conduct a skills gap analysis to determine existing knowledge levels and the areas where training is needed most.
    - Develop a training matrix that maps roles to the specific lifecycle phases and tasks for which they are responsible.
2. ***Learning Objectives and Curriculum Roadmap***
    - Define clear learning objectives for each role, focusing on what participants must be able to do upon completing the training (e.g., "apply data retention policies," "execute security controls," "approve new ADS designations").
    - Structure the curriculum around key DLM phases—data identification, assessment/evaluation, ADS approval, implementation/integration, maintenance, and retirement/re-designation—to provide a lifecycle-driven narrative.
3. ***Resource and Logistics Planning***
    - Establish budgets, timelines, and logistics for in-person or virtual training sessions.
    - Identify trainers and subject matter experts (SMEs) who will lead or support the instruction.
    - Plan for training materials (slides, handouts, interactive tools, sandbox environments, etc.) and ensure they are readily accessible to learners.

Developing Targeted Training Content

1. ***Core Knowledge Modules***
    - Create a foundational module that covers overarching policies, regulations, and best practices governing DoD and DISA data management (e.g., DoD Data Strategy, DISA policies, security/privacy directives).
    - Emphasize the importance of data lifecycle management: how it mitigates risk, ensures compliance, and enables better decision-making.

2. ***Role-Specific Modules***
    - Data Stewards: Instruction on data quality metrics, metadata standards, and ADS evaluation criteria.
    - System Administrators: Guidance on storage, backup, archiving, and security controls that align with DLM mandates.
    - Program Managers: Insight into governance processes, compliance requirements, and resource allocation for DLM projects.
    - Security/Privacy SMEs: Deep dive into encryption standards, role-based access, incident response, and risk assessment as they relate to data lifecycle management.
    - Records Liaisons: Detailed instruction on record-keeping policies, retention schedules, auditing, and disposition processes.
3. ***Hands-On Tools and Techniques***
    - Demonstrate the specific software or data management platforms (e.g., dashboards, analytics tools, change-management systems) used to implement DLM activities.
    - Provide step-by-step guides and real-world examples (case studies, simulations) for tasks like ADS registration, compliance checks, data classification, and retirement workflows.

Delivering the Training

1. ***Blended Learning Methods***
    - Combine in-person workshops (where feasible) with virtual sessions to accommodate a dispersed workforce.
    - Use e-learning modules or a learning management system (LMS) for self-paced study, complemented by scheduled live Q&A sessions.
2. ***Interactive and Practical Exercises***
    - Incorporate scenario-based role-plays and hands-on labs to reinforce concepts in a realistic environment.
    - Use group discussions or breakout sessions that challenge participants to problem-solve typical DLM scenarios (e.g., evaluating a new data source for ADS approval).
3. ***Assessment and Feedback***
    - Implement quizzes, knowledge checks, or final assessments to evaluate learners' understanding and retention.
    - Gather feedback from participants to continuously refine training materials, focusing on areas where learners report difficulties or request more depth.

Ongoing Support and Continuous Improvement

1. ***Reference Materials and Help Desk***
    - Provide quick-reference guides, FAQ documents, and contact points for ongoing support.
    - Maintain a dedicated DLM help desk or support channel where users can ask questions and get clarifications in real time.
2. ***Periodic Refresher Courses***
    - Offer annual or semi-annual refresher sessions to cover updates to policies, tools, or best practices (especially relevant as security threats and DoD directives evolve).
    - Encourage cross-functional knowledge sharing by inviting SMEs from different domains (security, privacy, data analytics) to present lessons learned and emerging trends.

3. ***Metrics and Continuous Improvement***
    - Track completion rates, assessment scores, and user feedback to measure training effectiveness.
    - Use these metrics to identify gaps or bottlenecks and iterate on the curriculum to maintain up-to-date, high-quality training content.

2.10 Data Management Plan

The DISA Data Management Plan (DMP) is a formal document or framework that outlines how data will be handled throughout its lifecycle—from planning, collection and storage to usage, *archive*, and eventual disposal. Within the DoD and specifically DISA, a DMP also details the policies, roles, and processes that govern the protection of sensitive information, ensuring compliance with STIGs, RMF guidelines, and other federal mandates. By capturing the scope of data, applicable security classifications, and the responsibilities of Data Stewards and stakeholders, a DMP lays the groundwork for transparent and coordinated data handling, enabling stakeholders to understand both the operational and security requirements from the outset.

In the context of the DISA Data Lifecycle Management, the DMP serves as the central reference point at each phase—beginning in the planning phase, where it is originally crafted or updated to reflect the system's mission objectives and regulatory considerations. As data moves through the lifecycle (collection, processing, storage, usage, sharing, archiving, and disposal), the DMP ensures that all required controls and activities, such as role-based access management, encryption standards, or backup schedules, are consistently applied. Regular reviews and updates of the DMP help maintain alignment with evolving policies, new mission requirements, and emerging technologies, fostering a proactive stance toward data governance and security.

Ultimately, a well-structured DMP is not a static artifact; instead, it is a living document that guides decision-making and risk management throughout the data's entire lifespan. By documenting responsibilities, establishing performance metrics, and detailing the necessary steps to protect data at every juncture, the DMP enables DISA to maintain a robust and adaptable approach to data management. This, in turn, promotes mission readiness, compliance with federal mandates, and effective collaboration across the DoD enterprise.

Appendix A: Data Management Plan Template

Department of Defense Data Management Plan Template

[This plan is based on the "Department of Defense (DOD)" template provided by United States Department of Defense (DOD) - (version: 4, pub: 2021-10-25).]

DATA MANAGEMENT PLAN

3 Types of Data Produced

3.1 The Types of Data, Software, Curriculum Materials, and Other Materials That Will Be Produced During the Project Are Publicly Releasable.

Guidance for answering this question:

- Give a summary of the data you will collect or create, noting the content, coverage and data type, e.g., tabular data, survey data, experimental measurements, models, software, audiovisual data, physical samples, etc.
- Consider how your data could complement and integrate existing data, or whether there are any existing data or methods that you could reuse.
- Indicate which data are of long-term value and should be shared and/or preserved.
- If purchasing or reusing existing data, explain how issues such as copyright and IPR have been addressed. You should aim to minimize any restrictions on the reuse (and subsequent sharing) of third-party data.

4 Data and Metadata Standards

The standards are to be used for data and metadata format and content.

Guidance about data format:

- Clearly note what format(s) your data will be in, e.g., plain text (txt), comma-separated values (.csv), geo-referenced TIFF (.tif,. tfw).
- Explain why you have chosen certain formats. Decisions may be based on staff expertise, a preference for open formats, the standards accepted by data centers, or widespread usage within a given community.
- Using standardized, interchangeable, or open formats ensures the long-term usability of data; these are recommended for sharing and archiving.
- See DataONE Best Practices for file formats.

Guidance about metadata format:

- What metadata will be provided to help others identify and discover the data?

- Researchers are strongly encouraged to use community metadata standards where these are in place. The Research Data Alliance offers a Directory of Metadata Standards. Data repositories may also provide guidance about appropriate metadata standards.
- Consider what other documentation is needed to enable reuse. This may include information on the methodology used to collect the data, analytical and procedural information, definitions of variables, units of measurement, any assumptions made, the format and file type of the data, and software used to collect and/or process the data.
- Consider how you will capture this information and where it will be recorded, e.g., in a database with links to each item, in a "readme" text file, in file headers, etc.

5 Conditions for Access and Sharing

Conditions for access and sharing include provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements.

Guidance on Ethics & Privacy:

- Investigators carrying out research involving human participants should request consent to preserve and share the data. Do not just ask for permission to use the data in your study or make unnecessary promises to delete it at the end.
- Consider how you will protect the identity of participants, e.g., via anonymization or using managed access procedures.
- Ethical issues may affect how you store and transfer data, who can see/use it, and how long it is kept. You should demonstrate that you are aware of this and have planned accordingly.
- See ICPSR approach to confidentiality and Health Insurance Portability and Accountability Act (HIPAA) regulations for health research.

Guidance about Intellectual Property Rights:

- State who will own the copyright and IPR of any existing data as well as new data that you will generate. For multi-partner projects, IPR ownership should be covered in the consortium agreement.
- Outline any restrictions needed on data sharing, e.g., to protect proprietary or patentable data.
- Explain how the data will be licensed for reuse. See the DCC guide on How to license research data and EUDAT's data and software licensing wizard.

Guidance with Storage & Security:

- Describe where the data will be stored and backed up during research activities. This may vary if you are doing fieldwork or working across multiple sites so explain each procedure.
- Identify who will be responsible for the backup and how often this will be performed. The use of robust, managed storage with automatic backup, for example, that provided by university IT

teams, is preferable. Storing data on laptops, hard drives, or external storage devices alone is very risky.
- See the DataONE Best Practices for storage.
- Also consider data security, particularly if your data is sensitive e.g., detailed personal data, politically sensitive information, or trade secrets. Note the main risks and how these will be managed. Also note whether any institutional data security policies are in place.
- Identify any formal standards that you will comply with, e.g., ISO 27001. See the DCC Briefing Paper on Information Security Management - ISO 27000 and UK Data Service guidance on data security.

Guidance about Data Sharing:

- How will you share the data, e.g., deposit in a data repository, use a secure data service, handle data requests directly, or use another mechanism? The methods used will depend on a number of factors such as the type, size, complexity, and sensitivity of the data.
- When will you make the data available? Research funders expect timely release. They typically allow embargoes but not prolonged exclusive use.
- Who will be able to use your data? If you need to restrict access to certain communities or apply data sharing agreements, explain why.
- Consider strategies to minimize restrictions on sharing. These may include anonymizing or aggregating data, gaining participant consent for data sharing, gaining copyright permissions, and agreeing to a limited embargo period.
- How might your data be reused in other contexts? Where there is potential for reuse, you should use standards and formats that facilitate this and ensure that appropriate metadata is available online so your data can be discovered. Persistent identifiers should be applied so people can reliably and efficiently find your data. They also help you to track citations and reuse.

Conditions and provisions for reuse, redistribution, and derivatives

Conditions and provisions for reuse, redistribution, and the creation of derivative works.

Guidance above for Access & Sharing is also applicable to this section

6 Plans for Archiving and Preservation

Plans for archiving datasets, or data samples, and other digitally formatted scientific data, and for preservation of access thereto. Explicitly describe how the data that underlies scientific publications will be available for discovery, retrieval, and analysis. In accordance with OSTP Memorandum, digitally formatted scientific data resulting from unclassified, publicly releasable research supported wholly or in part by DoD funding should be stored and publicly accessible to search, retrieve, and analyze to the extent feasible and consistent with applicable law and policy; agency mission; resource constraints; and U.S. national, homeland, and economic security.

Consider the Storage & Security guidance above.

Data repository:

- Where will the data be deposited? If you do not propose to use an established repository, the data management plan should demonstrate that the data can be curated effectively beyond the lifetime of the grant.
- It helps to show that you have consulted with the repository to understand their policies and procedures, including any metadata standards, and costs involved.
- An international list of data repositories is available via re3data and some universities or publishers provide lists of recommendations, e.g., PLOS ONE recommended repositories.

Data preservation:

- Outline the plans for data sharing and preservation - how long will the data be retained and where will it be archived? Will additional resources be needed to prepare data for deposit or meet any charges from data repositories?
- See the DataONE Best Practices for Identifying data with long-term value.

7 Justification for the Restriction of Data

If, for legitimate reasons, the data cannot be preserved and made available for public access, the plan will include a justification citing such reasons.