



Data Management Plan (DMP) and Data Access Policy



RDM Outreach Team
INFLIBNET Centre
Gandhinagar



Coverage

What is Data Management Plan (DMP)?

Benefits of Data Management Plan

Research Data Life Cycle

Key Elements of Data Management Plan

DMP Tools / Example Plan

Data Access Policy

Key Elements of Data Access Policy

Data Access Policy: Example



What is a Data Management Plan (DMP)?

A Data Management Plan (DMP) is a formal document that outlines how data will be handled throughout the lifecycle of a research project. It typically includes detailed information on how data will be

- collected,
- organized,
- stored,
- shared, and
- preserved.

Why Data Management Plan



01

Funder Mandates

Many funding agencies requires researchers to submit DMPs as part of their grant proposals. Recognize the importance of good data management practices for maximizing the impact and sustainability of research outcomes.

Promotes transparency by making research data accessible and understandable to other researchers. facilitates the reproducibility of research findings, allowing others to verify and build upon the work.



02

Transparency and Reproducibility



03

Data Sharing and Re-Use

DMPs often include plans for sharing research data with other researchers, which can accelerate scientific progress by enabling others to reuse and build upon existing data. Fostering data sharing also promotes collaboration and interdisciplinary research.

Research data is a valuable scholarly asset that should be preserved for the long term. DMPs typically include strategies for preserving data beyond the duration of a specific project, ensuring accessibility and usability



04

Preservation of Research Outputs

Why Data Management Plan



05

Compliance with Regulations

DMPs help researchers comply with legal and regulatory requirements related to data management, such as data protection laws, IPR, and funder policies. essential for ethical and responsible conduct of research.

By addressing issues such as data security, confidentiality, and backup procedures, DMPs help mitigate risks associated with data loss, unauthorized access, or data breaches. This protects the integrity and confidentiality of research data.



06

Risk Mitigation

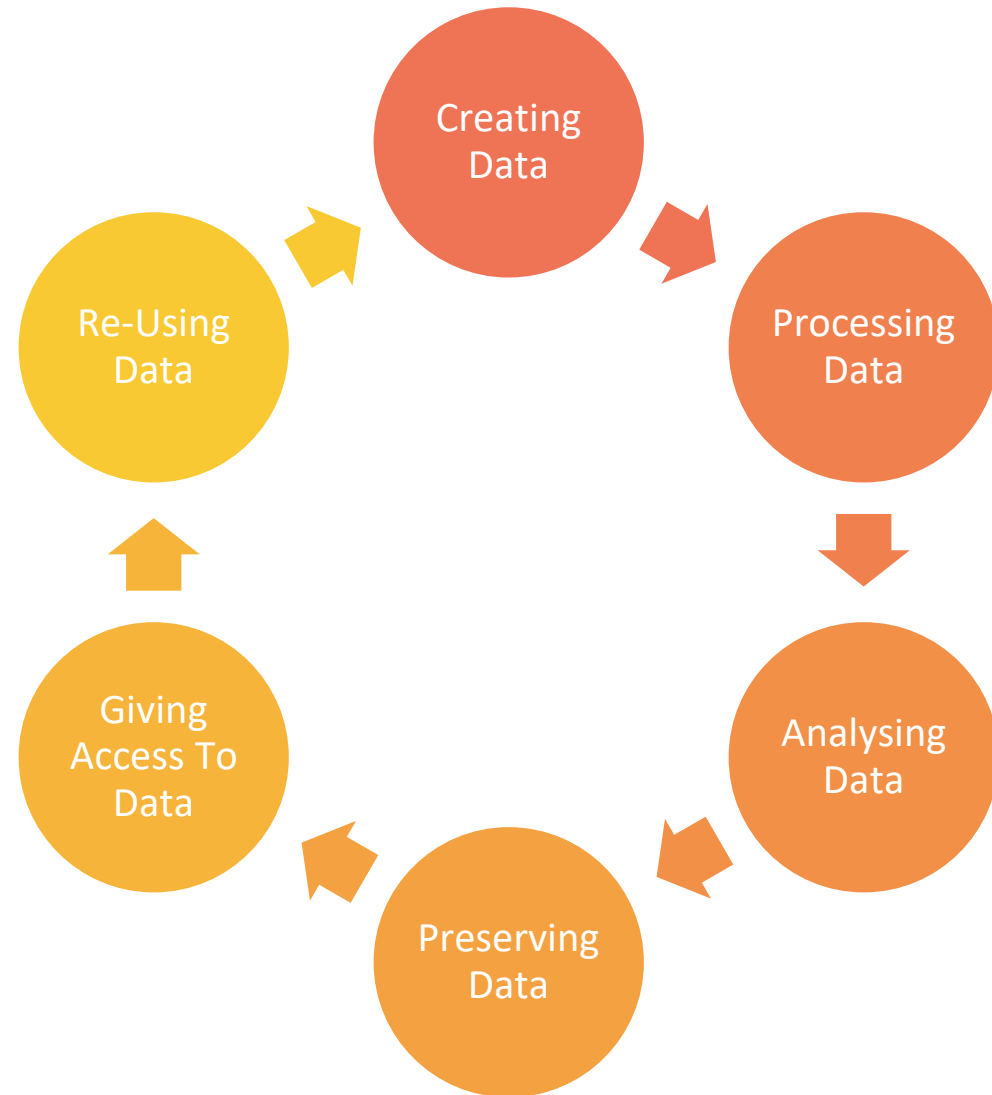


07

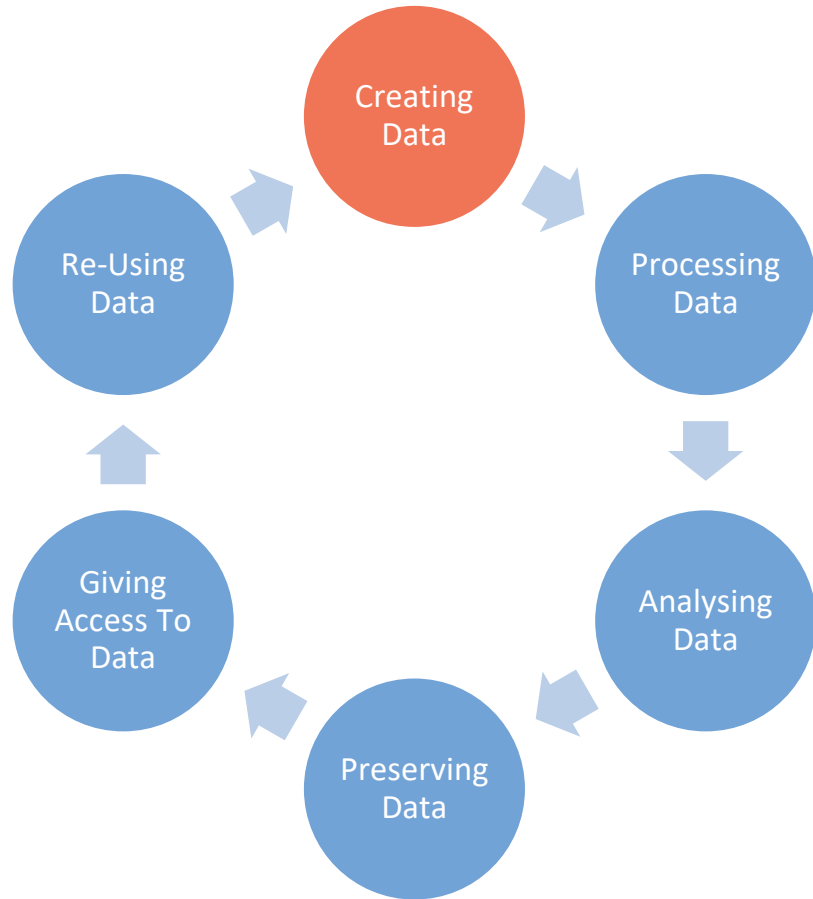
Efficiency and Cost Effectiveness

Properly managing research data from the outset can save time and resources by reducing the need to re-collect or reprocess data, improving data quality, and streamlining workflows for data analysis and interpretation

Research Data Lifecycle



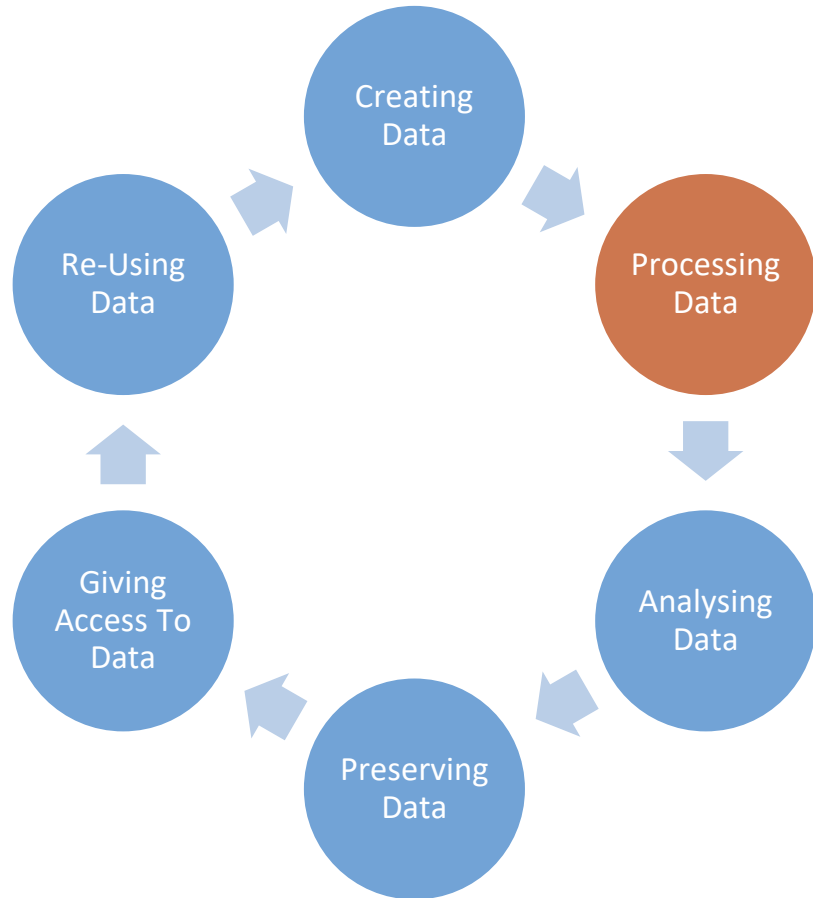
Research Data Lifecycle



Creating Data

- Design Research
- Plan Data Management (Format, Storage etc)
- Locate Existing Data
- Collect Data (Experiment, Observe, Measure, Simulate)
- Capture and Create Metadata
- Plan Consent for Sharing

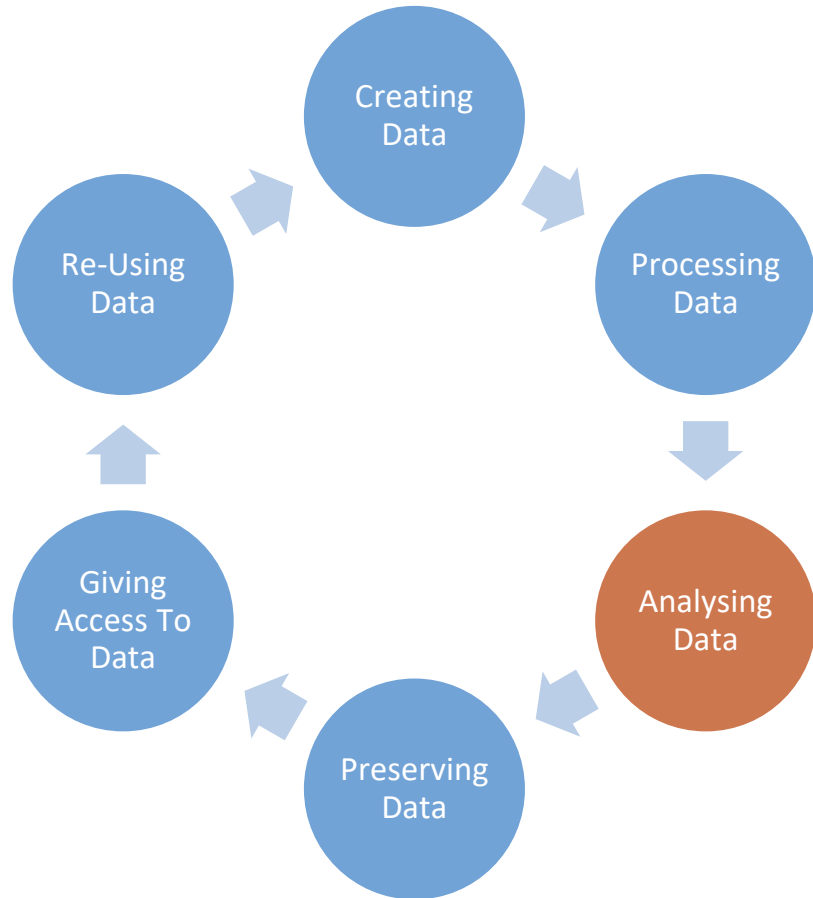
Research Data Lifecycle



Processing Data

- Enter Data, Digitize, Transcribe, Translate
- Check, Validate, Clean
- Anonymise (If Required)
- Describe Data
- Manage and Store

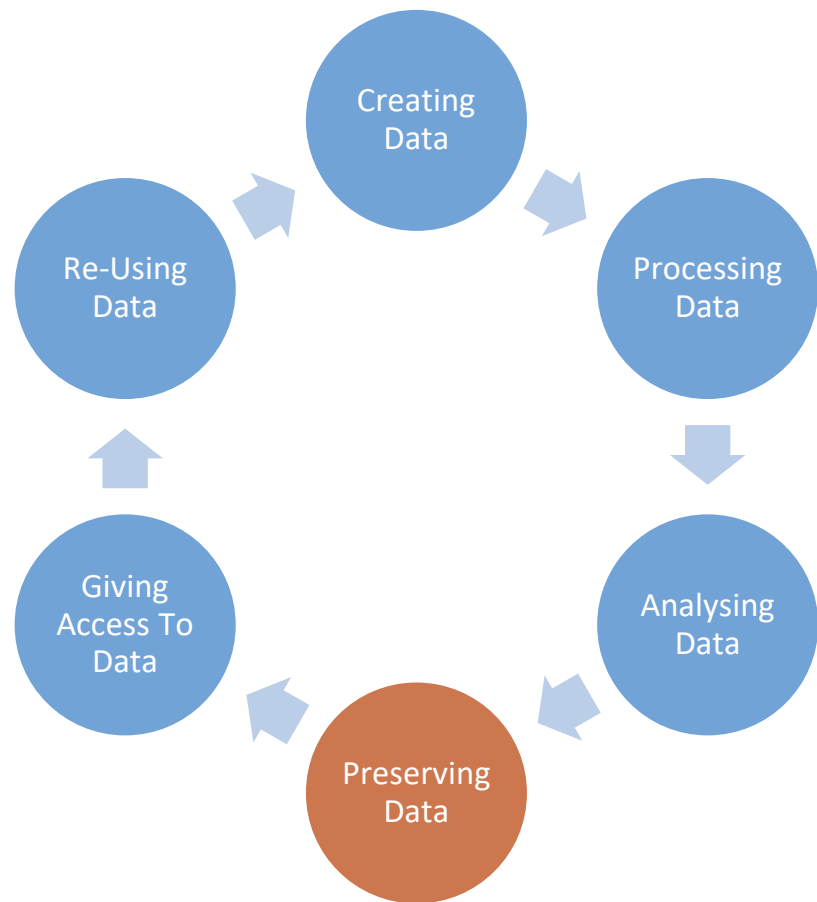
Research Data Lifecycle



Analysing Data

- Interpret Data
- Derive Data
- Produce Research Outputs
- Author Publications
- Prepare Data for Preservation

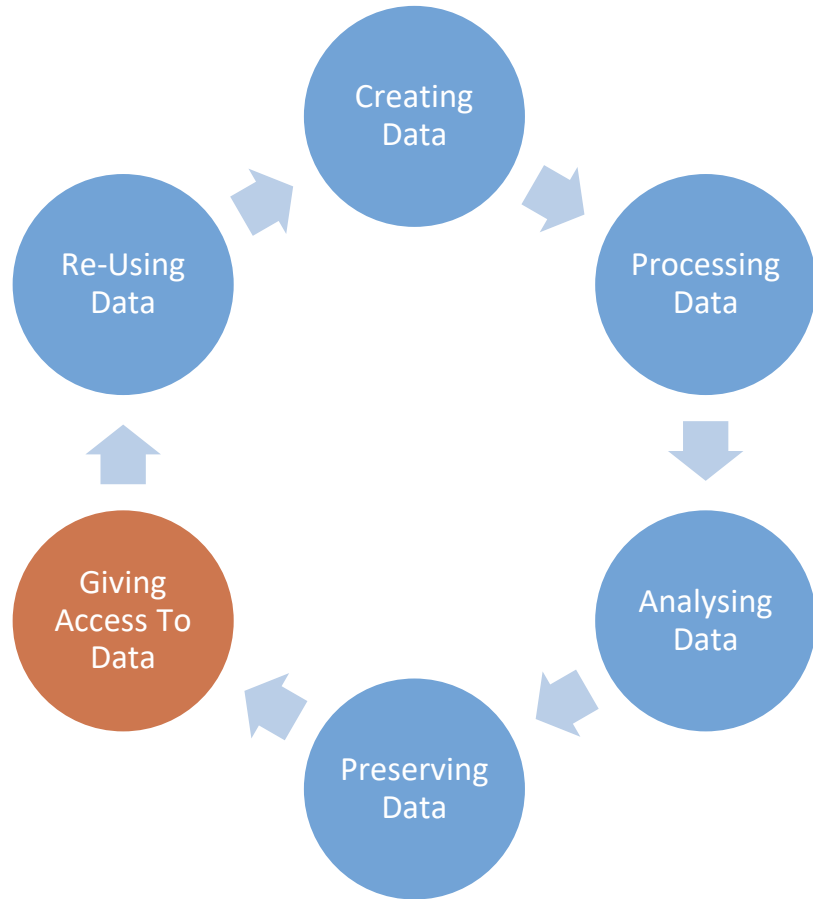
Research Data Lifecycle



Preserving Data

- Migrate Data to best format
- Migrate Data to suitable medium
- Backup and Store Data
- Create Metadata and Documentation
- Archive Data

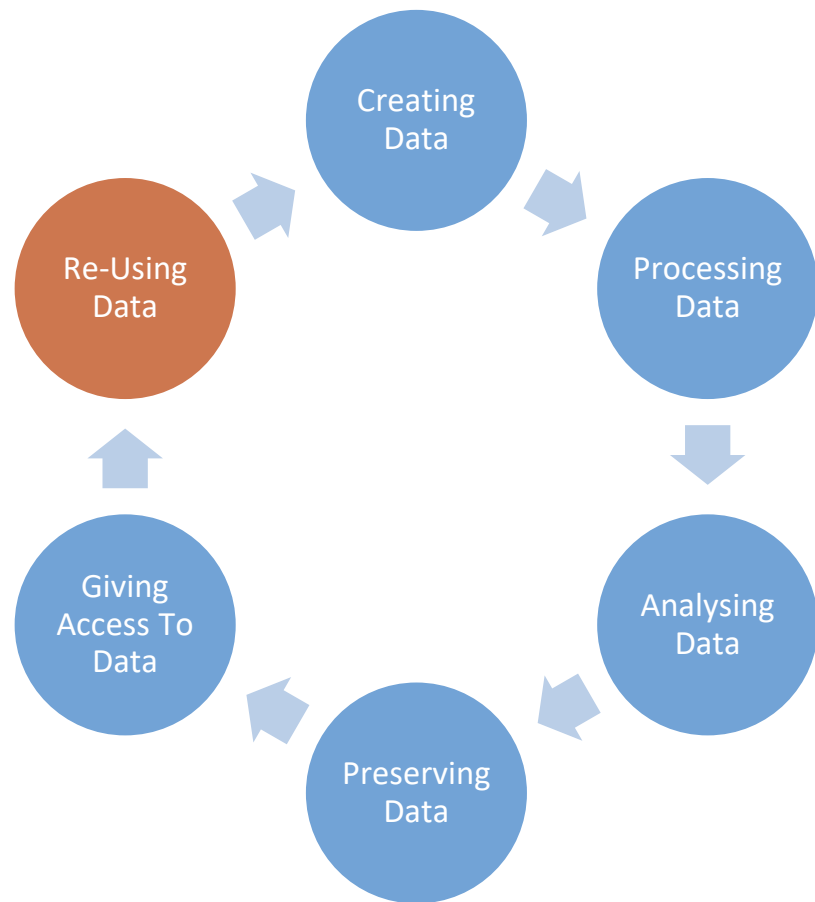
Research Data Lifecycle



Giving Access to Data

- Distribute Data
- Share Data
- Control Access
- Establish Copyright
- Promote Data

Research Data Lifecycle



Re-Using Data

- Follow up research
- New Research
- Undertake Research Reviews
- Scrutinize Findings
- Teach and Learn

The Data Management Plan

Data Reuse & Repurpose

Maximizing the value of research data through reuse
Discoverability and citation of research data
Data sharing agreements and licenses

Data Preservation & Archiving

Long-term data preservation strategies
Data archiving standards and practices
Ensuring data accessibility and availability

Data Sharing & Publication

Ethical and legal considerations in data sharing
Choosing appropriate data repositories
Preparing data for publication and sharing



Data Analysis

Different data analysis techniques (quantitative, qualitative)
Software tools and resources for data analysis
Ensuring reproducibility and transparency in analysis

Planning and Design

Preparing a DMP
Identifying research objectives and data requirements
Selecting appropriate data collection methods

Data Collection

Different methods of data collection (surveys, interviews, experiments, questionnaires)
Ensuring data quality and validity
Ethical considerations in data collection

Data Organization & Documentation

Creating a data management system
Organizing and storing research data effectively
Metadata and data documentation best practices



- Compliance / Legal
- Roles and Responsibilities

DMP Policies by Funding Agencies

- National Science Foundation (NSF) Data Management Plan (USA)
- Tri-Agency Research Data Management Policy (Canada)
- European Commission Horizon 2020 Data Management Plan
- Wellcome Trust Data Management and Sharing Policy (UK)
- Indian Council of Medical Research (ICMR) Data Sharing Policy (India)
- National Data Sharing and Access Policy (NDSAP) – India
- Biological Data Storage Access and Sharing Policy (BDSAP)- DBT India

Online Tools to Create DMP

- <https://dmponline.dcc.ac.uk/>
- <https://dmptool.org/>
- <https://service.dirisa.ac.za/>
- https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm -ERC DMP Template
- <https://dmp-pgd.ca/>
- <https://argos.openaire.eu/splash/>
- <https://ds-wizard.org/data-management-plans>
- <https://ezdmp.org/index>
- <https://dmponline.be/>

Let's have a quick and brief demo of DMP tool



DMP Tool... (Write Plan)



Project Details

Collaborators

Write Plan

Research outputs

Finalize

Download

This plan is based on the "Digital Curation Centre" template provided by Digital Curation Centre (dcc.ac.uk) - (ver: 2, pub: 2021-10-25).

expand all | collapse all

0/13

+ Data Collection (0 / 2)



+ Documentation and Metadata (0 / 1)



+ Ethics and Legal Compliance (0 / 2)



+ Storage and Backup (0 / 2)



+ Selection and Preservation (0 / 2)



+ Data Sharing (0 / 2)



+ Responsibilities and Resources (0 / 2)






Data Access Policy

A data access policy is a set of rules and guidelines that dictate how data can be accessed, used, and shared within an **organization or among authorized parties**.

It defines the procedures and controls necessary to ensure that sensitive or confidential information is appropriately handled and protected.



Data Access Policy – Key Components



Access Control

Specifies who has access to certain types of data and under what circumstances. This can involve user authentication, role-based access control (RBAC), and other mechanisms to limit access to authorized individuals..



Data Classification

Defines categories or levels of data sensitivity or confidentiality and determines the appropriate access controls for each category. For example, data may be classified as public, internal, confidential, or restricted, with corresponding access restrictions..



Authentication & Authorization

Outlines the procedures for verifying the identity of users and determining their level of access to data. This can include username/password authentication, multi-factor authentication (MFA), and access approval processes.



Data Sharing & Transfer

Specifies how data can be shared or transferred between users, departments, or external parties. This may include encryption requirements, secure file transfer protocols, and data sharing agreements.

Data Access Policy – Key Components



Data Usage Policy

Defines acceptable uses of data within the organization, including restrictions on copying, modifying, or distributing data without proper authorization. It may also address data retention and disposal requirements.



Monitoring & Auditing

Describes how data access activities will be monitored and audited to ensure compliance with the policy. This can involve logging access events, conducting regular security assessments, and investigating suspicious activities



Training & Awareness

Ensures that researchers are aware of their responsibilities regarding data access and security. This may involve providing training on data handling procedures, security best practices, and the consequences of policy violations

Example: Data Access Policy



- ICSSR Data Access Policy

<http://www.icssrdataservice.in/files/ICSSR%20Data%20Service-Policy%20Guidelines.pdf>



Thank You!

rdm.outreach@inflibnet.ac.in

This presentation is compiled from various sources available over the internet.

