Data Breach and Confidentiality Management

GRID Council

Standard Operating Procedure (SOP)

SOP for Data Breach and Confidentiality Management
Version 1.0; January 2026

Data Breach and Confidentiality Management, GRID Council

Standard Operating Procedure (SOP)

A. SOP Details

Organization Name:	Generating Research Insights for Development (GRID) Council
GRID Council- SOP Name	Data Breach and Confidentiality Management
Document Number:	Policy/HR/021
Policy effective date (DD-MM-YYYY):	01-01- 2026;
Last Revised on (DD-MM-YYYY):	-
Version Number:	1.0
Total number of pages	02
Total number of annexures	00

B. SOP Prepared by

Name & Designation	Signature
Hamza Salah (Senior research assistant)	Hamza salah

C. SOP Reviewed by

Name & Designation	Signature
Ritika Mukherjee (Deputy director)	Ritika mukherjee

D. SOP Approved by

Name & Designation	Signature
Archisman Mohapatra (Executive Director)	Archisman mohapatra

Table of Contents

1. Purpose

This SOP outlines GRID Council's approach to preventing, identifying, managing, and reporting data breaches and breaches of confidentiality in the context of research and programmatic activities involving personal or health-related data. The SOP aims to ensure timely response, harm minimization, and compliance with applicable Indian laws and ethical guidelines.

2. Scope

This SOP applies to all GRID Council–led or GRID Council–affiliated projects involving: Collection, storage, processing, or sharing of personal or health-related data; Electronic or physical data records; All staff, consultants, and collaborators with authorized data access.

3. Definition of a Data Breach

A data breach includes, but is not limited to: Unauthorized access to personal or health data; Accidental or unlawful disclosure of data; Loss, theft, or destruction of data or devices containing data; Any event that compromises confidentiality, integrity, or availability of data.

4. Principles

GRID Council follows the principles of:

- **Confidentiality:** Data accessed only by authorized individuals
- **Integrity:** Data protected from unauthorized alteration
- **Availability:** Data accessible to authorized users when required
- **Accountability:** Clear responsibility for breach response and documentation.

5. Breach Identification and Immediate Actions

Upon identification or suspicion of a data breach:

1. The incident must be reported immediately to the Principal Investigator or designated Data Manager.
2. Access to affected systems or datasets will be restricted or suspended, where necessary.
3. Immediate steps will be taken to contain the breach and prevent further unauthorized access.

Breach Notification Timelines

- Initial assessment: Within 24 hours of detection
- Internal escalation: Within 12 hours to Principal Investigator
- Ethics committee notification: Within 72 hours for breaches involving sensitive health data
- Individual notification: Where significant harm risk exists

6. Assessment and Documentation

The Data Manager, in consultation with the Principal Investigator, will: Assess the nature and scope of the breach; Determine the type of data involved and potential risk of harm; Document the incident, actions taken, and outcomes.

7. Notification and Reporting

- Relevant institutional authorities and ethics committees will be informed as required.
- Where applicable under the Digital Personal Data Protection (DPDP) Act, 2023, appropriate notifications will be made to regulatory authorities.
- International collaborators will be informed if shared datasets are affected.

Notifications will be proportionate to the risk and severity of the breach.

8. Corrective and Preventive Actions

Following a breach, GRID Council will: Implement corrective measures to address identified vulnerabilities; Review and strengthen technical, organizational, or procedural safeguards; Provide additional training or guidance to personnel, if required.

9. Confidentiality Obligations

- All personnel with data access are bound by confidentiality obligations.
- Unauthorized disclosure or misuse of data may result in disciplinary action and other remedies as per applicable law and institutional policies.

10. Review and Updates

This SOP will be reviewed periodically and updated in line with changes in legal requirements, ethical guidance, or organizational practices.