Updated: July 2025

HIMAT CONSULTING
Private Limited

Data Governance and Protection Policy

Office 023, Ground Floor, Khudadad Heights, Margalla Road, E-11/4, Islamabad
Email: himatullah@himatconsulting.com - Phone: 051-6131366

Data Governance and Protection Policy

HIMAT Consulting Pvt Ltd
Effective Date: 1st July 2025
Review Cycle: Annual
Approved By: CEO

---

1. Purpose

The purpose of this policy is to ensure the effective governance, protection, and ethical use of data collected, stored, processed, and shared by HIMAT Consulting. This policy outlines how data is managed to ensure integrity, confidentiality, availability, and compliance with applicable data protection laws, particularly within the development sector.

2. Scope

This policy applies to:

- All HIMAT Consulting employees, contractors, interns, and consultants.
- All data owned, processed, or managed by HIMAT Consulting.
- All systems and platforms used to store or manage data (on-premises or cloud-based).
- All data shared with third-party partners, clients, or service providers.

3. Definitions

- **Data Governance**: The framework for managing data assets to ensure they are trustworthy, accessible, secure, and used appropriately.
- **Personal Data**: Any data that can identify an individual, including names, contact details, demographic information, and sensitive identifiers.
- **Sensitive Data**: Data that includes personal data and other categories such as health, financial, gender-based violence (GBV), or project-sensitive information.
- **Data Subject**: Any individual whose data is collected or processed.
- **Data Steward**: Individual(s) responsible for ensuring the quality and proper handling of specific datasets.

4. Principles of Data Governance

HIMAT Consulting follows the following principles for effective data governance:

1. **Accountability**: Clear roles and responsibilities for data management across the organization.
2. **Transparency**: All data collection and use activities must be transparent and communicated to relevant stakeholders.
3. **Integrity**: Data must be accurate, complete, and kept up to date.
4. **Security**: Appropriate technical and organizational measures must protect data from unauthorized access, loss, or misuse.
5. **Compliance**: Adherence to applicable data protection laws, including GDPR, national laws, and donor requirements.
6. **Ethical Use**: Data must be used in ways that respect the dignity, rights, and interests of individuals and communities.

5. Data Classification

HIMAT classifies data into the following categories:

- **Public Data**: Information that can be shared without restriction (e.g. annual reports).
- **Internal Data**: Operational data used within HIMAT but not for public release.
- **Confidential Data**: Information shared under non-disclosure agreements or involving partner/donor data.
- **Sensitive Data**: Includes personal, health, financial, or vulnerable population data.

6. Data Lifecycle Management

All data must be managed through its full lifecycle:

1. **Collection**
    - Only data necessary for specific business or programmatic purposes should be collected.
    - Consent must be obtained where required.
2. **Storage**
    - Data must be stored securely using password-protected systems and encrypted storage where appropriate.
    - Physical records must be stored in locked cabinets with limited access.
3. **Access and Use**
    - Access to data is role-based and limited to those who require it for their work.
    - All users must follow the organization's Acceptable Use Policy.
4. **Sharing and Transfer**
    - Data may only be shared with third parties if necessary, and with appropriate agreements in place (e.g. Data Sharing Agreements, NDAs).
    - Cross-border data transfers must comply with relevant legal requirements.
5. **Retention and Disposal**
    - Data will be retained only as long as necessary for operational, legal, or donor compliance reasons.
    - Secure disposal methods (e.g., digital wiping, shredding) will be used when data is no longer needed.

7. Roles and Responsibilities

Role	Responsibility
CEO	Ultimate accountability for data governance and protection.
Data Protection Officer (if applicable)	Ensures compliance with data protection laws; point of contact for data subjects.
IT Lead	Implements technical safeguards and manages secure systems.
Data Stewards	Maintain data quality and proper documentation within their domain.
All Staff	Comply with this policy and attend relevant training.

8. Data Security Measures

- **Access Control**: Role-based access with multi-factor authentication where applicable.
- **Encryption**: Data at rest and in transit should be encrypted.
- **Regular Backups**: Weekly backups of critical data, with offsite or cloud redundancy.
- **Incident Response**: A data breach protocol must be in place, including prompt notification to affected parties and regulators where required.

9. Compliance and Training

- All staff must complete mandatory data protection training annually.
- Periodic audits will be conducted to ensure compliance.
- Non-compliance may result in disciplinary action, up to and including termination of employment or contract.

10. Breach Notification

Any data breach or suspected breach must be reported immediately to the CEO or the designated Data Protection Officer. A formal investigation will be conducted, and if necessary, affected stakeholders and regulators will be notified within 72 hours of confirmation.

11. Review and Revisions

This policy will be reviewed annually or sooner if:

- Legal or regulatory requirements change.
- There is a significant change in HIMAT's operations or data handling practices.
- An internal or external audit recommends revision.

12. Related Policies and Documents

- Acceptable Use Policy
- IT Security Policy
- Data Sharing Agreement Template
- Consent Form Template
- Incident Response Plan

Signed:

Himatullah
CEO
HIMAT Consulting Private Limited
Date: 1st July, 2025

Acceptable Use Policy (AUP)

Purpose
This policy defines acceptable use of HIMAT Consulting's information systems and data resources to ensure integrity, confidentiality, and responsible use.

Scope
Applies to all employees, contractors, interns, and consultants using HIMAT-owned or -managed systems.

Acceptable Use
- Use HIMAT devices and systems for authorized work-related activities only.
- Access only data or systems relevant to your role.
- Use secure, complex passwords and multi-factor authentication where required.
- Store sensitive data only on approved systems.
- Comply with applicable laws and regulations, including data protection laws.

Prohibited Use
- Sharing login credentials or leaving devices unattended and unlocked.
- Using HIMAT resources for personal gain, harassment, or illegal activity.
- Installing unauthorized software or bypassing security controls.
- Copying or distributing sensitive data without authorization.

Enforcement
Violations may result in disciplinary action up to and including termination, and legal action where applicable.

IT Security Policy

Purpose
To safeguard HIMAT Consulting's digital infrastructure, data, and assets from threats and unauthorized access.

Scope
Applies to all hardware, software, cloud systems, mobile devices, and users. Aligns with ISO/IEC 27701 and NIST CSF.

Key Provisions
- **Access Control**: Role-based access; user accounts deactivated upon departure.
- **Password Policy**: Minimum 12 characters, changed every 90 days.
- **Device Security**: All devices must have antivirus software and disk encryption.
- **Network Security**: Use firewalls, VPNs, and secure Wi-Fi only.
- **Monitoring**: Systems may be monitored for security purposes.

Incident Response
Follow the HIMAT Incident Response Plan in case of breach or security anomaly.

Data Sharing Agreement Template

[Organization Name]
Data Sharing Agreement
Parties Involved:

- Data Provider: HIMAT Consulting
- Data Recipient: [Partner Organization Name]

Purpose
To govern the secure, lawful, and ethical sharing of data between the parties.

Data Covered
[List dataset or types, e.g., survey data, demographic records]

Legal Basis
Each party confirms the legal basis for collecting and sharing the data (e.g. consent, legitimate interest).

Responsibilities

- HIMAT will ensure data is accurate and anonymized where possible.
- Recipient will use data solely for agreed purposes and keep it secure.

Duration
[Insert duration or project end date]

Breach Protocol
Recipient must notify HIMAT within 24 hours of any breach.

Signed by:

_____ (HIMAT Representative)

_____ (Partner Representative)

Date: [Insert]

Consent Form Template

HIMAT Consulting – Informed Consent Form

Purpose of Data Collection:
We are collecting your data to [describe purpose, e.g., understand community needs for development planning].

What We Will Collect:
[List of data points – e.g., age, gender, location, opinions]

Your Rights:

- You can withdraw consent at any time.
- Your data will be kept secure and confidential.
- You can ask us to delete your data.

Do you consent to this?
☐ Yes, I consent
☐ No, I do not consent

Name: _____

Signature: _____

Date: _____

Incident Response Plan

Purpose
To ensure prompt, coordinated, and effective response to data breaches or cybersecurity incidents.

Scope
Incorporates ISO 27701's privacy breach management.
Includes mandatory breach notification timelines (e.g. PECA fines; PDP Bill may require 72-hour notification for serious breaches).
Applies constitutional privacy protections and anticipates regulatory body engagement (e.g., NCPDP once operational).

Incident Categories
- Unauthorized access
- Malware or ransomware attack
- Data leakage/loss
- System compromise

Response Team
- Incident Manager [IT Lead]
- Chief Executive Officer

Steps
1. **Detect & Identify**: Log and verify the incident.
2. **Contain & Mitigate**: Disconnect affected systems; limit spread.
3. **Notify**: Inform internal team and, if needed, external stakeholders (e.g. partners, data subjects). Report to regulators if required within 72 hours.
4. **Investigate**: Conduct a root cause analysis.
5. **Recover**: Restore systems, review policies.
6. **Report**: Final incident report with recommendations.
