# BISAP DATA BREACH POLICY

## Bangladesh Integrated Social Advancement Programme (BISAP)

Address: House # 02, Road # 01
Lake Valley R/A, Nuria Madrasah Road
Foy's Lake,Khulshi, Chattogram, Bangladesh
Mobile: 880 1740995872, 880 01814427016
Facebook : https://www.facebook.com/s.m.tareque.jabed
Twitter: https://twitter.com/tareque_jabed
Linkedin: https://www.linkedin.com/in/bisap-bangladesh
Email: info@bisapbd.org, bisapbd@gmail.com,
Website: www.bisapbd.org

# BISAP Data Breach Policy

## 1. Purpose and Scope

At the **Bangladesh Institute of Social Advancement Programmes (BISAP)**, we recognize that safeguarding personal and sensitive information is a cornerstone of dignity, trust, and accountability. This policy sets out how BISAP responds to **security incidents (SI)** and **personal data breaches**, ensuring compliance with Bangladesh's ICT Act (2006), Digital Security Act (2018), and the Draft Data Protection Act (2022), as well as aligning with global best practices (e.g., GDPR, UN privacy standards).

This policy applies to:

- All BISAP staff, volunteers, contractors, and partners.
- All data formats (digital, paper, audiovisual).
- Both **accidental** and **malicious** incidents involving personal or sensitive data.

## 2. Definition of a Data Breach

A **data breach** occurs when there is:

- Unauthorized access to personal data.
- Accidental or unlawful disclosure, alteration, or loss of personal data.
- Failure of systems, human error, or malicious actions that compromise data integrity or confidentiality.

Examples: sending beneficiary data to the wrong recipient, losing devices containing personal data, hacking, or mishandling of financial records.

## 3. Legal and Ethical Framework

BISAP upholds the following principles:

- **Compliance with Bangladesh law** (ICT Act, DSA, Data Protection Act).
- **Global best practices** such as the GDPR principle of "privacy by design and by default."
- **Rights-based approach** – respecting the dignity, safety, and empowerment of beneficiaries and stakeholders.
- **Accountability** – every breach is taken seriously, investigated thoroughly, and documented transparently.

## 4. Responsibilities

- **All staff and volunteers**: must immediately report suspected breaches.
- **Line Managers**: ensure containment actions are taken and notify the Data Protection Lead (DPL).
- **Data Protection Lead (DPL)**: leads investigations, maintains breach records, advises on notification, and reports to senior management.
- **Senior Information Risk Owner (SIRO)**: provides oversight and escalates matters to regulators, donors, or law enforcement when necessary.
- **HR**: supports disciplinary or remedial processes fairly and consistently.

## 5. Immediate Response – The CARE Model

BISAP manages every incident using the **CARE framework**:

- **Contain**: Stop the breach immediately (secure devices, recall emails, restrict access).
- **Assess**: Identify the type of data, scope of exposure, and risks to individuals.
- **Respond**: Notify relevant authorities, donors, and affected individuals as required.
- **Evaluate**: Document the incident, analyze root causes, and implement corrective measures.

## 6. Reporting Obligations

- Staff must report breaches **immediately** to their Line Manager and the DPL.
- The **DPL must begin an investigation within 24 hours**.
- If a breach poses **high risk to individuals' rights or freedoms**, notification to regulators must occur **within 72 hours**.

- Affected individuals will be informed promptly, with details on what happened, what data was affected, risks involved, and mitigation steps.

## 7. Severity Assessment

BISAP classifies breaches into three levels:

- **Low Risk**: Minor inconvenience, no real harm (e.g., wrong meeting invite).
- **Medium Risk**: Distress but not severe harm (e.g., salary details disclosed internally).
- **High Risk**: Significant damage (financial, reputational, or safety-related risks, e.g., loss of beneficiary medical records).

Every breach, regardless of level, is logged in the **BISAP Data Breach Register**.

## 8. Investigation and Follow-Up

Within one week, the DPL must prepare a full report including:

- Nature, timeline, and cause of the breach.
- Individuals/data affected.
- Risk assessment.
- Immediate and long-term corrective actions.
- Recommendations on training, system upgrades, or process reforms.

The findings will be shared with **Senior Management** and, if required, donors and regulators.

## 9. Communication and Transparency

BISAP values **honesty and openness**. In the event of a breach:

- Beneficiaries or partners affected will be contacted directly with a clear explanation.
- Donors and partners will be notified if their data or funding processes are impacted.
- External communications will be managed responsibly to maintain trust while protecting sensitive information.

## 10. Disciplinary and Remedial Action

- Breaches caused by negligence or failure to follow procedure may lead to **disciplinary action**, ranging from retraining to warnings, depending on severity.
- Malicious or intentional breaches may result in **termination, legal action, or referral to law enforcement**.
- Every breach will trigger a **learning review** to strengthen BISAP's culture of accountability and care.

## 11. Record-Keeping and Continuous Improvement

- All breaches are logged in the **BISAP Data Breach Register**, maintained by the DPL.
- HR keeps records of disciplinary or remedial measures.
- BISAP commits to **quarterly reviews** of breach incidents to identify patterns and improve systems.
- Findings are integrated into staff training and policy upgrades to build a **resilient, future-ready data protection culture**.

## 12. BISAP's Commitment

At BISAP, data protection is not just a compliance requirement—it is a **moral responsibility** and an extension of our mission to empower communities with dignity and safety.
By adopting a **proactive, transparent, and globally aligned** breach response framework, BISAP ensures that every stakeholder—from vulnerable beneficiaries to international partners—can trust us with their most sensitive information.

Mohammad Dostagir
Chairman - BISAP

S M Tareque Jabed
Chief Executive - BISAP