SOP on Data Breach Response Procedure

1. Purpose

This procedure outlines GK's approach to identifying, reporting, investigating, and responding to actual or suspected data breaches. It is designed to ensure that incidents are handled swiftly, transparently, and in compliance with applicable data protection laws.

2. Scope

This procedure applies to all GK employees, contractors, consultants, and third-party service providers who handle personal or sensitive data on behalf of GK.

3. Definition of a Data Breach

A Data breach is an incident that results in:

- Unauthorized access to personal or sensitive data;
- Loss or theft of data;
- Accidental or unlawful destruction, alteration, or disclosure of data;
- Compromise of data availability or integrity.

Examples including:

- Hacking or ransomware attacks;
- Loss of a laptop, phone, or storage device containing sensitive data;
- Emails sent to the wrong recipient;
- Misconfigured cloud storage exposing data publicly.

4. Roles and Responsibilities

Role	Responsibility
All Staff	Immediately report any suspected or confirmed data breach to the designated authority.
Data Protection Focal (DPF)	Oversee breach investigations, determine notifiability, and liaise with regulators and affected parties.
IT Unit	Assess technical impact, contain breaches, and support investigation.
Management	Support response and communication, and oversee preventing actions.

5. Breach Response Procedure

Step 1: Identification and Reporting

- Any individual who suspects a data breach must report it **immediately** to the DPF at:

  [Name: Shafiul Azam Azad; Designation: Senior IT Officer; Email ID: azad@gkcox.org; Contact No: +880 1885 945 181]

- The report should include:
    - Date and time of incident (if known)
    - Description of the breach
    - Type of data affected
    - Systems or individuals involved

Step 2: Containment

- The DPF and IT team will take urgent steps to contain the breach:
    - Disconnect affected systems if needed
    - Revoke access credentials
    - Secure physical or digital data sources
    - Stop further data loss

Step 3: Assessment

- An internal investigation is launched within **24 hours** of the report.
- The DPF will assess:
    - Nature and sensitivity of the data
    - Number of individuals or records affected
    - Potential harm to individuals or the organization
    - Whether the data was encrypted or protected
    - Applicable legal/regulatory obligations

Step 4: Notification (If Required)

- **Regulatory Authorities:** It legally required (e.g., under GDPR or local laws), the breach will be reported to the appropriate authority within **72 hours.**
- **Affected Individuals:** If the breach poses a high risk to the rights and freedoms of individuals, they will be notified promptly with:
    - A description of the breach
    - What data was involved
    - What actions they can take
    - What GK is dong to mitigate harm

Step 5: Documentation

- A **Data Breach Report** will be completed and stored securely, including:
    - Root cause analysis
    - Actions taken
    - Decision on whether to notify regulators or individuals
    - Preventive recommendations

- All breaches, whether notifiable or not, will be logged.

Step 6: Remediation and Review

- The DPF and relevant departments will implement corrective actions.
- A post-incident review will be conducted to:
  - Assess effectiveness of response
  - Improve systems, training, or procedure
  - Reduce risk of recurrence

6. Communication Guidelines

- All external communications regarding the breach must be approved by the **DPF and senior management.**

7. Training and Awareness

- All staff receive regular training on data protection and breach response.
- Breach response procedures are reviewed and updated **annually** or after a major incident.

8. Compliance and Enforcement

Failure to report or respond to a breach in accordance with this procedure may result in disciplinary action and may have legal consequences.

9. Contacts

Data Protection Focal: [*[Name: Shafiul Azam Azad; Designation: Senior IT Officer; Email ID: azad@gkcox.org; Contact No: +880 1885 945 181].*

- **IT Security Team:**

Name: Shafiul Azam Azad

Designation: Sr. IT Officer

Email ID: azad@gkcox.org

Contact No: 01885-945181

Name: A H M Iftekhar Uddin Chowdhury

Designation: Sr. Program Officer

Email ID: iftekhar@gkcox.org

Contact No: 01885-945176

Name: Md. Mahmud Hasan

Designation: IT Assistant, GK-MI

Email ID: mahmud@gkcox.org

Contact No: 01679-488258

****

Dr. Manzur Kadir Ahamed
Senior Director
Gonoshasthaya Kendra
Cox's Bazar.