Data Breach Policy and Procedures

Version 9

REZOLVE.ai

Document Information

Name of the document	Data Breach Policy and Procedures
Release date	19-Dec-2018
Owned by	Boopathi
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	02-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	02-Mar-2023	Reviewed and no change
7	21-Jul-2024	Updated DocumentInformation
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	08-May-2026	Reviewed and no change

Reviewerand Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder&CTO	Approved	13-May-2026

Table of Contents

Introduction and Scope

Introduction

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
This procedure provides general principles and approach model to respond to, and mitigate breaches of personal data.
The procedure lays out the actions for successfully managing the response to a data breach as well as comply with the regulations.
The purpose of this procedure is to ensure that a standardized approach is implemented in the event of a personal data breach.

Scope

The procedure applies to:

- all personal data created or received by the company in any format (including paper), whether used, stored on portable devices and media, transported from the company physically or electronically or accessed remotely;
- personal data held on all IT systems; and
- any other IT systems on which data is held or processed.

Categories of Data Breach

Data breaches can be categorised based on the nature of the incident, the type of data involved, and the method used to gain unauthorized access. Here are some common categories:

1. Based on Nature of Incident

- **Accidental Exposure:** Data is inadvertently exposed to the public or unauthorized individuals, often due to human error, misconfiguration, or oversight.
- **Malicious Breach:** Deliberate attacks by cybercriminals or insiders to steal sensitive information.
- **System Glitches:** Technical issues or bugs in software systems that inadvertently expose data.

2. Based on Type of Data Involved

- **Personally Identifiable Information (PII):** Information that can be used to identify an individual, such as names, addresses, Social Security numbers, and dates of birth.
- **Payment Card Information (PCI):** Credit and debit card information, including card numbers, expiration dates, and security codes.
- **Protected Health Information (PHI):** Medical records and other health-related information protected under laws like HIPAA.
- **Intellectual Property (IP):** Trade secrets, proprietary business information, and other types of confidential intellectual property.
- **Credentials:** Usernames, passwords, and other login information.

3. Based on Method of Breach

- **Phishing:** Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communications.
- **Malware:** Malicious software designed to infiltrate, damage, or disable computer systems and steal data.
- **Ransomware:** A type of malware that encrypts data and demands a ransom to restore access.
- **Hacking:** Unauthorized access to computer systems, networks, or devices by exploiting vulnerabilities.
- **Insider Threat:** Breaches caused by employees, contractors, or other insiders, either intentionally or unintentionally.
- **Physical Theft:** Physical theft of devices like laptops, smartphones, or storage media containing sensitive data.

- **SQL Injection:** A code injection technique that exploits vulnerabilities in web applications to gain access to the database.

Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Categories of Personal Data Breach

All the below breaches are considered personal data breach:

- **Confidentiality breach:** the disclosure of, or access to, the data by an unauthorised person;
- **Availability breach:** the loss of access to, or destruction of, the data; and
- **Integrity breach:** an alteration of the data

Response and Prevention

1. Response to Data Breach

Containment:

- Immediately isolate the affected systems to prevent further unauthorized access.
- Disable the compromised accounts or services to contain the breach.

Assessment:

- Identify and evaluate the extent of the breach, including the data affected, duration of the breach, and the method of attack.
- Analyse server logs, network traffic, and server configurations.

Notification:

- Inform stakeholders, including customers, partners, and regulatory bodies (if necessary), about the breach.
- Provide a transparent communication plan detailing the nature of the breach, affected data, potential risks, and the steps being taken to mitigate the issue.

Mitigation:

- Patch vulnerabilities that were exploited during the breach.
- Reset passwords and generate new API keys as appropriate.

Review and Improve:

- Conduct a post-breach analysis to understand what went wrong.
- Update security policies and response plans based on the lessons learned.

2. Prevention Measures

Data Encryption:

- Use strong encryption mechanisms such as AES for data storage and transmission to make it unreadable to unauthorized users.

- Use strong secure communications protocols like HTTPS/TLS/SSL.

Access Control:

- Implement Role-Based Access Control (RBAC) to restrict access based on predefined roles within the organization.
- Identity and Access Management (IAM) involves managing user identities and their access to resources. IAM systems often include features like Single Sign-On (SSO) and Multi-Factor Authentication (MFA).

Vulnerability Management:

- Regularly scan for and address vulnerabilities in the application and underlying infrastructure.
- Implement continuous monitoring and threat detection mechanisms to identify and respond to potential threats promptly.

Security Best Practices:

- Keep all software and systems up to date with the latest security patches.
- Educate employees and users about security best practices and phishing scams.

Formal Contracts and Policies:

- Ensure that formal contracts with customers clearly define the roles and responsibilities related to information security.
- Commit to contractual obligations and ethical principles to protect privacy and avoid breaches of contractual clauses.

By combining immediate response actions with robust preventive measures, organizations can effectively manage and mitigate the consequences of data breaches in applications.

Data Breach Process and Management

It is the policy of the company that in the event of an information/data breach occurring, the subsequent breach management plan is stringently adhered to. There are key components to the breach management plan namely:

- **Identification and Classification**
- **Notification of Breach**
- **Containment and Recovery**
- **Evaluation and Response**

Identification and Investigation of a Data Breach

Personal data breaches will be identified through manual and automated procedures.

Identification

Manual Procedures

- **Incident Reporting** procedures allow internal employees to report identified actual or a potential breach.
- **Client Reporting** to a common email ID allows clients and external parties to report a potential data breach to the Company.

Automated Procedures

Automated procedures such as log analysis, firewall log reviews, and antivirus report reviews will enable the company to identify potential data breaches.

Real-Time Monitoring

- **Intrusion Detection Systems (IDS):** Automatically monitor network traffic and application activities to detect suspicious behavior that might indicate a data breach.
- **Security Information and Event Management (SIEM):** Aggregates and analyzes security data from various sources in real-time to identify anomalies and potential threats.

Behavioral Analytics

- **Anomaly Detection:** Uses machine learning and statistical models to detect unusual patterns or deviations from normal behavior that may suggest a breach.
- **User and Entity Behavior Analytics (UEBA):** Monitors user and entity activities for signs of malicious or unauthorized behavior, providing insights into potential breaches.

Automated Alerts

- **Event Correlation:** Automatically correlates events from different sources to identify complex attack patterns that might indicate a breach.
- **Alerting Systems:** Generates alerts based on predefined criteria or detected anomalies, enabling rapid response to potential incidents.

Data Loss Prevention (DLP)

- **Content Inspection:** Automatically scans and analyses data flows to detect and prevent unauthorized data access or leakage.
- **Policy Enforcement:** Applies data security policies automatically to prevent the transfer or access of sensitive information by unauthorized users.

Vulnerability Management

- **Automated Scanning:** Regularly scans applications for known vulnerabilities and weaknesses that could be exploited in a breach.
- **Patch Management:** Automatically deploys patches and updates to address vulnerabilities and reduce the risk of exploitation.

Access Control Enforcement

- **Automated Provisioning and De-Provisioning:** Manages user access rights automatically based on role changes or employment status, reducing the risk of unauthorized access.
- **Real-Time Access Monitoring:** Monitors and enforces access policies in real-time to detect and respond to unauthorized access attempts.

Data Breach Response Team

A Data Breach Response Team (BRT) must be a multi-disciplinary team. The team's mission is to provide an immediate, effective response to any potential or actual personal data breaches affecting the Company.

At Actionable Science, the BRT consists of:

- CEO
- DPO
- Head of IT / CISO
- Head of Applications

Responsibilities of BRT

Once a personal data breach is reported, the BRT or the BRT Leader must implement the following:

- Validate the personal data breach
- Investigate the breach
- Notify senior management immediately
- Coordinate with internal and external resources
- Carry out daily / weekly reporting of the issue

1. Notification of a Data Breach

When a personal data breach has occurred, the Company needs to establish the **likelihood and severity** of the resulting risk to people's rights and freedoms. If it is **likely that there will be a risk**, then the Company **must notify the regulator**.

However, if the company decides **not to report the breach**, it needs to be **justified and documented** in the **Breach Register**.

Breaches **need not be reported to the regulator** if there is **unlikely a high risk**.

Notification from Data Processor to Data Controller

- If the Company acts as a **processor**, then any data breach needs to be **reported to the Controller** and **not to the Supervisory Authority**.
- Once the breach is confirmed, the **DPO** will send notification to the **controllers listed in the Data Inventory Sheet**, and will include the necessary details required for them to report to the **Supervisory Authority**.
- For this purpose, the **Breach Notification Template applicable for Supervisory Authority** may be used and shared with the Controllers.
- The processor shall notify the controller **without undue delay after becoming aware of a personal data breach**.

Notification to the Supervisory Authority

The following information needs to be included in the **notification of data breach to the Supervisory Authority**. (*Refer Data Breach Notification Template - Regulator*)

A Description of the Nature of the Personal Data Breach

Including, where possible:

- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Timelines for Reporting

- All personal data breaches must report a notifiable breach to the Supervisory Authority without undue delay, but not later than **72 hours** after becoming aware of it.
- **Becoming aware of it is different from the date of the breach.** The 72-hour window starts from the point the senior management has concluded that an actual breach has occurred.
- If the initial investigation is likely to take longer, an initial notification with whatever information is possible may be considered, and a **follow-up notification** may be done once all information is available. In such cases, the Company must give **reasons for the delay**.
- **Failure to notify on a timely basis may result in huge financial fines.**

Notification to Data Subjects

If the breach is likely to result in a **high risk of adversely affecting individuals' rights and freedoms**, the Company must inform those individuals **without undue delay**. In other words, this should take place **as soon as possible**.

One of the main reasons for informing individuals is to **help them take steps to protect themselves** from the effects of a breach.

The following information needs to be included in the notification of data breach to the Data Subjects, in clear and plain language:

(Refer Data Breach Notification Template – Data Subject)

- The nature of the personal data breach
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects

When Is Notification to Data Subject Not Required?

- Personal data is rendered unintelligible to any person who is not authorised to access it, such as by encryption
- Subsequent measures taken reduce risk to below **high risk**
- It would involve **disproportionate effort**. In such a case, there shall instead be a **public communication** whereby the data subjects are informed in an **equally effective manner**

Containment and Recover

Containment comprises restricting both the scope and impact of the breach. If a breach occurs, the company should:

- Decide on who will take the lead in investigating the breach and ensure that the appropriate resources are available to the nominated officer for investigation
- The nominated officer will then establish whether there is anything that can be done to recoup losses and/or limit the damage the breach may cause
- Details of the facts relating to the breach, its effects, and remedial action taken are then entered in the **Data Breach Register**

Risk Assessment

In assessing the risk arising from the breach, the company should consider what would be the potential adverse

consequences for individuals. In assessing the risk, the company will consider the following:

- Nature of information/data involved?
- Sensitivity of the information/data?
- Any security mechanisms in place (e.g. password, encryption)?
- What could the information/data convey to a third party about the individual?
- How many individuals are affected by the breach?

Evaluation and Response

Subsequent to any information/data security breach, a thorough review of the event should be undertaken by the DPO who will consider:

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies, procedures or reporting lines need to be amended to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are all officers, voluntary assistants and employees cognisant of their responsibilities for information security and adequately trained?
- Is additional investment required to lessen exposure and if so what are the resource implications?

Any recommended changes to policies and/or procedures must be documented and implemented as soon as possible thereafter by the Board of Directors / Privacy Committee.

Handling Employee Misbehavior Leading to a Data Breach

Handling employee misbehavior that leads to a data breach involves several steps to ensure accountability, mitigate damage, and prevent future incidents.

1. Immediate Response

- **Contain the Breach:** Quickly isolate the compromised systems to prevent further unauthorized access or data loss
- **Investigate the Incident:** Conduct a thorough investigation to understand how the breach occurred, identify the employee(s) involved, and determine the extent of the damage
- **Notify Relevant Parties:** Inform affected individuals, regulatory authorities, and other stakeholders as required by law and company policy

2. Disciplinary Action

- **Assess Intent and Impact:** Evaluate whether the employee's actions were intentional or accidental and consider the severity of the breach
- **Apply Appropriate Consequences:** Based on company policies and the nature of the misbehavior, take disciplinary actions which may include warnings, retraining, suspension, or termination

3. Preventive Measures

- **Policy Review and Update:** Revisit and strengthen data protection policies, ensuring they clearly outline acceptable behaviors and consequences for violations
- **Employee Training:** Provide regular training on data security best practices, including how to recognize and avoid risky behaviors
- **Access Controls:** Implement or tighten access controls to ensure employees only have access to the data necessary for their roles

4. Monitoring and Auditing

- **Regular Audits:** Conduct regular security audits and monitoring to detect any unusual activities or potential threats
- **Implement Monitoring Tools:** Use software tools to monitor employee activities, especially those with access to sensitive data

5. Support and Counseling

- **Employee Support Programs:** Offer counseling or support programs for employees to help them understand the importance of data security and to address any underlying issues that might lead to misbehavior
- **Encourage Reporting:** Foster a culture where employees feel comfortable reporting suspicious activities without fear of retaliation

6. Legal and Regulatory Compliance

- Ensure all handling of employee-related breaches complies with relevant labor laws, data protection regulations, and industry standards

Consult Legal Counsel: Ensure all actions taken comply with labor laws and data protection regulations. Seek legal advice when necessary.
Document Everything: Keep detailed records of the incident, investigation, disciplinary actions, and preventive measures for compliance purposes and future reference.

1. **DataBreachRecordKeeping**
   DataBreachRegister
   The Company needs to record all breaches, regardless of whether or not they need to be reported to the regulators.
   The Company needs to maintain a data breach register in the format as per Annexure A- Breach Register.
   Article 33(5) requires documenting the facts relating to the breach, its effects and the remedial action taken.
2. **Annexure:ExamplesofPersonalDataBreach**
   Data security breaches can occur for a number of reasons including: access by an unauthorised third party; deliberate or accidental action (or inaction) by a controller or processor; sending personal data to an incorrect recipient;
   computing devices containing personal data being lost or stolen; alteration of personal data without permission; and
   loss of availability of personal data.
   The disclosure of confidential data to unauthorised individuals;
   improper disposal of documents leaving personal data deposited in a bin that can be accessed by the general public;
   loss or theft of data or equipment on which data is kept; loss or theft of paper records;
   inappropriate access controls allowing unauthorised use of information; suspected breach of the Company's IT security and related policies;
   attempts to gain unauthorised access to computer systems, e.g., hacking; viruses or other security attacks on IT equipment systems or networks;
   breaches of physical security;
   confidential information left unlocked in accessible areas; and
3. **Annexure:DeterminationofDatabreachresultinginRisk**
   Use this Annexure for determining if a breach results in risk to data subjects.
   Almost anything could present a risk to the rights and freedoms of natural persons. The addition of one external factor may turn a non-risk into a risk.
   The standard for risk triggering notification obligation to the Supervisory Authority is required is a relatively low bar.
   Conversely, the standard for high risk triggering an additional report to the affected individuals, is a relatively high bar.
   The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing.
   The risk assessment, at the very least, should take into account the following factors:

No.	Factor	FurtherGuidance
1.	**ThetypeofPersonalData Breach**	For example, a confidentiality breach whereby medical informationhas been disclosed to unauthorized parties may have a different set of consequences for an individual to a breach where individuals' medical details have been lost, and are no longer available.
2.	**Thenatureandsensitivityof Personal Data**	Usually, the more sensitive the data is, the higher the risk of harm will be to the people affected. However, consider the following: • **the context**: the name and address of a person is not seen as sensitive, however, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child. Conversely, other personal data which is clearly public may not constitute a likely risk to individuals in other contexts. • **the potential uses of the data**: Personal Data Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft.
3.	**ThevolumeofPersonalData**	Note that a small amount of highly sensitive Personal Data can have a high impact on an individual; and a combination of details can reveal a greater range of information about that individual. Also, a Breach affecting large volumes of Personal Data about many individuals can have an effect on a corresponding large number of individuals.
4.	**Whether "SpecialCategories"ofPersonalData or data relating to criminal convictionsandoffencesare involved**	Damage should be considered likely to occur when the Personal Data Breach involves personal data that reveals or includes: • racialorethnicorigin, political • opinion, • religionorphilosophicalbeliefs, • trade union membership, genetic • data, • biometric data for the purposes of uniquely identifying an individual, • dataconcerninghealthordataconcerningsexlife, • criminalconvictionsandoffencesorrelatedsecuritymeasures.
5.	**Ease of identification of individuals using the Personal Data, or by matchingthedatawithother information**	Considerwhether,forexample: • identification could be possible directly from the Personal Data breached with no special research needed; • it would be extremely difficult to match Personal Data to a particular individual, but it could still be possible under certain conditions. • identification may be indirectly possible from the breached data, using context and/or publicly available personal details. Note that pseudonymized data can reduce the likelihood of individuals being identified, but on their own, pseudonymization techniques arenot regarded as making the data unintelligible (See row 7, below).
6.	**Severityofconsequencesfor individuals**	Considerthefollowingcriteria: • **Type of consequence** - Especially severe consequences include: identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. • **Permanence of the consequences** - the impact may be viewed as greater if the effects are long-term.

7.	**Whomayhaveaccessedthe Personal Data**	Considerwhomayhaveaccessedthedata: • If the Personal Data is in the hands of people whose intentions are unknown or possibly malicious, this can have a bearing on the level of potential risk. • The recipient may be considered "trusted" (*e.g.*, where Personal Data is sent accidentally to the wrong department of an organization, or to a commonly used supplier organization).
		Evenifthedatahasbeenaccessed,Companycouldstillpossibly trust the recipient not to take any further action with it and to return the data promptly. Note: the fact that the recipient is trusted may eradicate the severity of the consequences of the Personal Data Breach butdoes not mean that a Personal Data Breach has not occurred.
8.	**Whether negative consequencesarepossible**	Regulatory guidance provides a number of examples of breaches which are or are not likely to result in a notifiable Personal Data Breach: If a confidentiality breach of encrypted data occurs (e.g., an encrypted USB device is lost), it is possible that this is unlikely to result in risk to individuals if the encryption is state-of-the-art and theencryptionkeyhasnotbeencompromised(i.e.,thedatais in principle unintelligible). Other types of negative consequences may arise - e.g., if Company has no back-ups (or Company has back-ups, but they cannot be restored in good time) and the information is thus not accessible in a way which could case negative effects to individuals.
9.	**Specialcharacteristicsofthe individual**	APersonal Data Breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result of their special characteristics.
10.	**Specialcharacteristicsof Company**	The special characteristics of the Company should also be taken into account when assessing risk. To the extent that the Company has particular characteristics which may have an impact, these should be part of the assessment. One example may be if Company is involved in "risky processing activity" including but not limited to: using "new technologies" to process data, large-scale processing (e.g. regional, national, supranational), or systematic and extensive evaluation of personal aspect based on automated processing on which decisions regarding individuals are based.

1. **Annexure:KeydifferencebetweenEU&USASOPs**

   RegulatoryFramework: The EU follows GDPR, which has strict notification requirements and timelines, while the USA has a patchwork of state laws and industry-specific regulations.
   NotificationTimelines: GDPR requires notification within 72 hours, while US state laws generally require notification within 30-60 days.
   ScopeofData: GDPR applies broadly to all personal data, while US regulations may be more specific to certain types of data (e.g., health information under HIPAA).

2. **AnnexureA-BreachRegister**
   Data breach incidents are created under Incident Management Jira project. The register typically includes the following information:
   Date and Time of Breach: When the breach occurred or was discovered.
   Description of the Breach: Detailed information about what happened, how it was detected, and the type of data involved.
   ImpactAssessment: Analysis of the potential or actual impact on individuals and the organization, including the extent of data exposure.
   Action Taken: Steps taken to contain and mitigate the breach, including any immediate response and long-term measures.
   Notifications: Information on whether affected individuals, regulatory bodies, or other relevant parties were notified, and the details of such notifications.
   Investigation Findings: Results from any investigations conducted to understand the cause and extent of the breach.
   Lessons Learned: Insights gained from the breach and any changes made to policies, procedures, or security measures to prevent future incidents.

3. **Annexure-DataBreachNotificationtemplate-Regulator**
   [Your Organization's Letterhead]
   [Date]
   [Regulator's Name]
   [Regulatory Body]
   [Address]
   [City, State, ZIP Code]

   Subject: Notification of Data Breach

   Dear **[Regulator's Name]**,

   We are writing to inform you of a data breach incident that has occurred within our organization, **[Your Organization's Name]**. We are committed to maintaining the highest standards of data protection and transparency, and as such, we are providing you with the details of this incident in accordance with applicable data protection regulations.

   1. **Date and Time of Breach**
      The data breach occurred on **[Date and Time of Breach]** and was discovered on **[Date and Time of Discovery]**.
   2. **Description of the Breach**
      The breach involved unauthorized access to **[describe the type of data involved, e.g., personal, financial, medical information]** of **[number]** individuals. The unauthorized access was identified when **[briefly describe how the breach was detected]**.
   3. **ImpactAssessment**
      Our preliminary assessment indicates that the breach may have **[describe the potential or actual impact on individuals, e.g., exposed sensitive personal information, risk of identity theft, etc.]**. We are currently conducting a detailed investigation to fully understand the extent and implications of the breach.
   4. **Action Taken**
      Upon discovering the breach, we took immediate steps to contain and mitigate its effects, including:

[Describe steps taken, e.g., isolating affected systems, resetting passwords, etc.]
[Notify affected individuals, if applicable, and provide details of how they were notified]

5. **Notifications**
   We have notified the affected individuals on **[Date]** and provided them with information on the steps they can take to protect themselves. Additionally, we have communicated with relevant stakeholders and are working closely with cybersecurity experts to address the issue.
6. **Investigation Findings**
   [If available, provide details of initial findings from the investigation, e.g., root cause, vulnerabilities exploited, etc.]
7. **Lessons Learned and Preventive Measures**
   To prevent future incidents, we are implementing the following measures:
   [Describe preventive measures, e.g., enhanced security protocols, employee training, regular security audits, etc.]

We take this incident very seriously and are committed to taking all necessary actions to protect the data of our customers and employees. We will continue to update you as our investigation progresses and we implement additional safeguards.

Should you require any further information or have any questions, please do not hesitate to contact [Contact Person's Name, Title] at [Contact Information].
Sincerely,
[Your Name]
[Your Title]
[Your Organization's Name]
[Contact Information]

1. **Annexure-DataBreachNotificationtemplate-DataSubject**
   [Your Organization's Letterhead]
   [Date]
   [Recipient's Name]
   [Recipient's Address]
   [City, State, ZIP Code]

   Subject: Important Information Regarding a Data Breach

   Dear **[Recipient's Name]**,

   We are writing to inform you of a data breach that has occurred within our organization, **[Your Organization's Name]**. We take the protection of your personal information very seriously and are committed to being transparent about what has happened and what we are doing to address the situation.

   1. **What Happened**
      On **[Date of Breach]**, we discovered that **[describe the nature of the breach, e.g., unauthorized access, data theft, etc.]** had occurred. The breach was identified on **[Date of Discovery]**, and we have since been working diligently to investigate and contain the situation.
   2. **What Information Was Involved**
      The breach involved the following types of your personal information:
      - **[Type of Data 1, e.g., name, address, etc.]**
      - **[Type of Data 2, e.g., Social Security number, financial information, etc.]**
   3. **What We Are Doing**
      Upon discovering the breach, we immediately took the following steps to mitigate its impact and secure your information:
      [Describe actions taken, e.g., isolating affected systems, resetting passwords, etc.]
      We have engaged cybersecurity experts to assist in our investigation and strengthen our security measures.
   4. **What You Can Do**
      While we are taking every step to protect your information, we recommend that you also take the following precautions:
      - **Monitor Your Accounts**: Regularly check your bank, credit card, and other accounts for any unusual activity.
      - **Report Suspicious Activity**: If you notice any unauthorized transactions or activities, report them immediately to your financial institution.

- **Change Passwords**: Change your passwords for any online accounts that may have been affected and use strong, unique passwords.
- **Credit Monitoring**: Consider placing a fraud alert on your credit files and enrolling in a credit monitoring service.

5. **Contact Information**
   We understand the concern and inconvenience this incident may cause. If you have any questions or need further assistance, please do not hesitate to contact our support team at **[Contact Information]** or email us at **[Email Address]**.
6. **Further Information**
   We are committed to keeping you informed as our investigation progresses and we implement additional safeguards to protect your information.

Thank you for your understanding and cooperation.

Sincerely,
[Your Name]
[Your Title]
[Your Organization's Name]
[Contact Information]

NOTE - Next review cycle for this policy is March-2027. Management can review policy any time and can make changes depending on the situation.
All documents related to policies and procedures any reference to Actionable Science is as good as Rezolve.ai.