

## Data Breach Response and Notification Policy

### 1. Introduction

Inazuma.co recognizes the paramount importance of protecting the personal and sensitive data entrusted to it by its stakeholders, including customers, employees, and business partners. The Company is committed to maintaining the confidentiality, integrity, and availability of this data. This Data Breach Response and Notification Policy ("Policy") establishes a comprehensive framework for responding to and notifying affected parties in the event of a data breach. This Policy is designed to ensure compliance with all applicable data protection laws and regulations, including but not limited to the Digital Personal Data Protection Act, 2023, and to minimize the impact of any data breach on the company and affected individuals. It outlines the procedures for identifying, containing, investigating, and remediating data breaches, as well as the responsibilities of various stakeholders within the organization. Inazuma.co believes that a robust and well-defined data breach response plan is crucial for maintaining trust, mitigating potential harm, and ensuring business continuity.

### 2. Purpose and Objectives

The purpose of this Policy is to:

- Define a data breach and establish detailed procedures for identifying, containing, investigating, and remediating such breaches in a timely and effective manner.
- Clearly outline the roles and responsibilities of individuals and teams involved in the data breach response process, ensuring accountability and efficient coordination.
- Establish clear guidelines for notifying affected parties, including individuals, regulatory bodies, and other stakeholders, in strict accordance with legal requirements and best practices. This includes specifying the content, timing, and method of notifications.
- Ensure the timely and effective response to data breaches to minimize potential harm and financial loss, both to the company and to affected individuals. This includes setting specific timeframes for key response activities.
- Prevent future data breaches by identifying and addressing the root causes of incidents, and by implementing appropriate security measures and controls. This includes a commitment to

- continuous improvement of the company's security posture.
- Provide a framework for post-breach analysis and review, to identify areas for improvement in the company's data security practices and incident response procedures.
  - Maintain the trust and confidence of stakeholders by demonstrating the company's commitment to data protection and its ability to respond effectively to security incidents.

### 3. Scope

This Policy applies to all Inazuma.co employees, directors, officers, contractors, and any other individuals or entities that have access to the company's data, including personal data, sensitive data, and confidential business information, regardless of their employment status, location, or the format of the data (electronic or physical). For the avoidance of doubt, this includes:

- All data stored on Inazuma.co's servers, networks, and systems.
- Data stored on employee-owned devices that are used for company business.
- Data processed by third-party vendors on behalf of Inazuma.co.
- All information assets owned, leased, or controlled by Inazuma.co.

- Data in any format, including electronic records, paper documents, and other media.
- Any data that is accessed, processed, or stored by employees or contractors, whether on-site or remotely.

### 4. Definitions

- **Data Breach:** Any unauthorized access, acquisition, disclosure, loss, destruction, or alteration of any personal data, sensitive data, or confidential business information that compromises the confidentiality, integrity, or availability of such information. A data breach can occur due to intentional actions, accidental events, or system failures. Examples include, but are not limited to:
  - Hacking or cyberattacks
  - Unauthorized access to systems or data
  - Loss or theft of devices containing data
  - Accidental disclosure of data to unauthorized parties
  - Malware or ransomware infections
  - Insider threats (e.g., unauthorized access by employees)
  - Physical breaches of security
  - System errors or malfunctions
- **Personal Data:** Any information that relates to a living individual

- who can be identified, either directly or indirectly, from that information. This includes, but is not limited to:
- Name
  - Address
  - Email address
  - Phone number
  - Date of birth
  - Identification numbers (e.g., PAN, Aadhaar)
  - Location data
  - Online identifiers (e.g., IP address, cookies)
  - Any other information that can be used to identify an individual.
- **Sensitive Data:** A subset of Personal Data, including, but not limited to, information relating to:
    - Financial information (e.g., bank account details, credit card numbers, investment information)
    - Health information (e.g., medical records, health conditions, treatment information)
    - Biometric data (e.g., fingerprints, facial recognition data)
    - Password and authentication credentials (e.g., passwords, PINs, security questions)
    - Religious or philosophical beliefs
    - Political opinions
  - Sexual orientation
  - Racial or ethnic origin
  - Trade union membership
  - Any other data classified as sensitive under applicable law, including the Digital Personal Data Protection Act, 2023.
- **Confidential Business Information:** Non-public information that gives Inazuma.co a competitive advantage, and which the company takes steps to protect from unauthorized disclosure. This includes, but is not limited to:
    - Trade secrets
    - Business plans and strategies
    - Financial information (e.g., revenue, profits, forecasts)
    - Customer lists and information
    - Supplier information
    - Pricing information
    - Marketing plans
    - Research and development data
    - Intellectual property
  - **Data Controller:** The entity that determines the purposes and means of the processing of personal data (Inazuma.co). Inazuma.co is responsible for ensuring that data is collected and processed in accordance with applicable laws and regulations.
  - **Data Processor:** An entity that processes personal data on behalf of the Data Controller. Inazuma.co

- will ensure that any Data Processors it engages have adequate security measures in place to protect the data.
- **Affected Individual:** Any person whose personal data has been involved in a data breach. This includes customers, employees, and any other individuals whose data is processed by Inazuma.co.
  - **Regulatory Body:** Any government agency or authority responsible for enforcing data protection laws and regulations. In the context of this Policy, this primarily refers to the Data Protection Board of India, as established under the Digital Personal Data Protection Act, 2023, and any other relevant authorities.
  - **Incident Response Team (IRT):** A designated team responsible for managing and responding to data breaches. The IRT is responsible for coordinating the company's response, investigating the breach, and implementing corrective actions.
- ## 5. Data Breach Response Team (IRT)
- **5.1 Composition:** Inazuma.co shall establish a standing Incident Response Team (IRT) comprising individuals with the necessary expertise and authority to handle data breaches effectively. The IRT will be a multi-disciplinary team, with representatives from various departments within the organization. The specific composition of the IRT may be adjusted based on the nature and severity of the data breach, but will typically include representatives from the following departments:
    - **Information Security:** Responsible for the technical aspects of the breach response, including identifying the source of the breach, containing the incident, and implementing security measures to prevent future breaches.
    - **Legal:** Provides guidance on legal obligations, notification requirements, and potential liabilities, and ensures compliance with applicable laws and regulations.
    - **IT:** Assists in the technical investigation, data recovery, and system restoration, and provides support for the implementation of security measures.
    - **Human Resources:** Handles internal communications related to the breach, addresses employee-related issues, and ensures that employee data is protected.
    - **Public Relations/Communications:**

- Develops and executes communication plans for external stakeholders, including customers, the media, and the public, and manages the company's reputation.
- **Operations:** Ensures business continuity during and after the breach, and coordinates operational activities related to the response.
  - **Compliance:** Ensures adherence to all regulatory and legal requirements, and works with the Legal department to address any compliance issues.
  - **Company Secretary:** Acts as the nodal officer for the breach, and is the primary point of contact for reporting to the Board of Directors and regulatory authorities. The Company Secretary is responsible for ensuring that all reporting requirements are met.
- **5.2 Roles and Responsibilities:**
- **Team Leader:** The Team Leader will be a senior manager with overall responsibility for coordinating the data breach response efforts, managing communications, and ensuring compliance with this Policy and applicable laws. Specific responsibilities include:
    - Activating the IRT and overseeing the response effort.
    - Coordinating the activities of the various IRT members.
    - Serving as the primary point of contact for senior management and the Board of Directors.
    - Making critical decisions regarding containment, investigation, notification, and remediation.
    - Ensuring that all actions taken are documented.
    - Approving all external communications.
    - Ensuring that the company complies with all applicable legal and regulatory requirements.
  - **Information Security:** Responsible for the technical investigation, containment, and remediation of the breach, including:
    - Identifying the source of the breach.
    - Containing the incident to prevent further data loss.
    - Analyzing affected systems and data.
    - Implementing security measures to prevent future breaches.
    - Working with IT to recover

- data and restore systems.
- ■ Preserving evidence for legal and forensic purposes.
- **Legal:** Provides guidance on legal obligations, notification requirements, and potential liabilities, including:
  - Interpreting applicable laws and regulations.
  - Advising on notification requirements to regulatory bodies and affected individuals.
  - Assessing potential legal risks and liabilities.
  - Working with external legal counsel, if necessary.
  - Ensuring that all actions taken are legally sound.
- **IT:** Assists in the technical investigation, data recovery, and system restoration, including:
  - Providing technical support to the Information Security team.
  - Recovering lost or corrupted data.
  - Restoring affected systems.
  - Implementing security patches and updates.
  - Ensuring the availability of necessary resources.
- **Human Resources:** Handles internal communications related to the breach and addresses employee-related issues, including:
  - Communicating with employees about the breach.
  - Addressing employee concerns and questions.
  - Ensuring that employee data is protected.
  - Investigating any employee involvement in the breach.
  - Providing support to affected employees.
- **Public Relations/Communications:** Develops and executes communication plans for external stakeholders, including customers, the media, and the public, and manages the company's reputation, including:
  - Developing key messages and communication materials.
  - Coordinating with the media.
  - Responding to inquiries from customers and other stakeholders.
  - Managing the company's online reputation.
  - Ensuring that communications are consistent and accurate.
- **Operations:** Ensures business

continuity during and after the breach, including:

- Assessing the impact of the breach on business operations.
- Developing and implementing business continuity plans.
- Coordinating with other departments to ensure that critical business functions are maintained.
- Managing any disruptions to services.
- **Compliance:** Ensures adherence to all regulatory and legal requirements, including:
  - Identifying applicable laws and regulations.
  - Monitoring compliance with those laws and regulations.
  - Working with the Legal department to address any compliance issues.
  - Ensuring that all required reports are filed with regulatory bodies.
- **Company Secretary:** Acts as the nodal officer for the breach and is responsible for reporting to the Board of Directors and regulatory authorities, including:
  - Serving as the primary point of contact for regulatory bodies.
  - Ensuring that all required

notifications are made in a timely manner.

- Providing updates to the Board of Directors on the status of the breach and the response efforts.
- Maintaining records of all communications with regulatory bodies.
- **5.3 Contact Information:** The IRT shall maintain up-to-date contact information for all team members, including primary and secondary contact details. This information shall be readily accessible in case of a data breach, both in electronic and hard copy formats. In addition, the IRT shall maintain a list of contact information for external experts, such as:
  - Forensic investigators
  - Legal counsel specializing in data breach response
  - Cybersecurity firms
  - Public relations firms
  - Relevant regulatory bodies, including the Data Protection Board of India
  - Law enforcement agencies
- **5.4 Training:** The IRT members will receive regular and up-to-date training on data breach response protocols, relevant laws and regulations, and best practices. Training will be provided at least annually, and more frequently as needed, to ensure that IRT

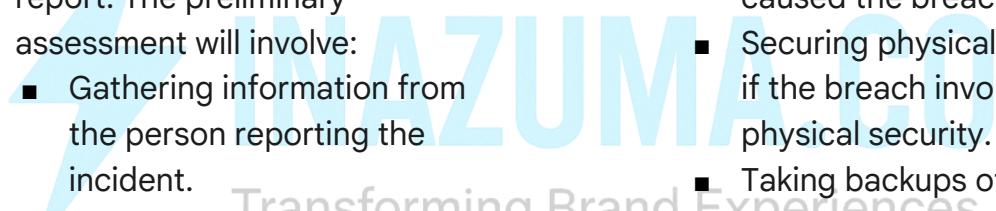
members are prepared to handle data breaches effectively. The training program will cover:

- The contents of this Policy
  - The roles and responsibilities of IRT members
  - Data breach detection and containment techniques
  - Forensic investigation procedures
  - Notification requirements and procedures
  - Risk assessment methodologies
  - Data recovery and system restoration procedures
  - Communication strategies
  - Legal and regulatory compliance
  - Post-incident analysis and reporting
  - Tabletop exercises and simulations to test the IRT's response capabilities
  - Updates on the latest threats and vulnerabilities
  - Specific requirements of the Digital Personal Data Protection Act, 2023
- Training will be documented, and records of attendance will be maintained.

## 6. Data Breach Response Procedure

The following procedure outlines the steps to be taken in the event of a data breach:

- **6.1 Detection and Initial Assessment:**
  - Any employee or contractor who suspects a data breach must immediately report the incident to their supervisor or the designated contact person (Company Secretary). Employees should be trained to recognize the signs of a potential data breach, which may include:
    - Unusual system activity
    - Unauthorized access to data
    - Suspicious emails or phishing attempts
    - Missing files or data
    - Unexpected system outages
    - The discovery of malware or other malicious software
  - The initial report should include all available information, such as:
    - The date and time of the suspected breach
    - The type of data involved (e.g., personal data, sensitive data, confidential business information)
    - The potential cause of the breach (if known)
    - The location of the data
    - The systems or devices affected
    - Any observed impact on

- 
- systems or data
  - The names of any individuals involved (if known)
  - Contact information of the person reporting the incident
  - The IRT will conduct a preliminary assessment to determine if a data breach has occurred and to evaluate the potential severity and scope of the incident. This assessment must be completed as quickly as possible, and in no more than 24 hours from the initial report. The preliminary assessment will involve:
    - Gathering information from the person reporting the incident.
    - Reviewing system logs and audit trails.
    - Conducting interviews with relevant personnel.
    - Consulting with technical experts, if necessary.
    - Documenting the findings of the assessment.
  - **6.2 Containment:**
    - The IRT will take immediate steps to contain the breach and prevent further data loss or damage. These steps may include:
      - Isolating affected systems or networks from the rest of the network to prevent the breach from spreading.
      - Changing access credentials, including passwords and access codes, for affected systems and accounts.
      - Disabling compromised accounts or user access.
      - Implementing temporary security measures, such as firewall rules, intrusion detection systems, and other security controls.
      - Stopping the unauthorized activity or process that caused the breach.
      - Securing physical locations, if the breach involves physical security.
      - Taking backups of affected systems and data.
  - The containment measures shall be documented in detail and preserved for forensic analysis. The documentation should include:
    - The specific actions taken
    - The date and time of each action
    - The individuals responsible for taking the actions
    - The systems or data affected
    - The results of the containment efforts
  - **6.3 Investigation:**

- The IRT will conduct a thorough investigation to determine the root cause of the breach, the extent of the data compromise, and the systems and individuals affected. The investigation will be conducted in a systematic and thorough manner, and may involve:
    - Forensic analysis of affected systems, including servers, workstations, and mobile devices.
    - Reviewing logs and access records to identify unauthorized access or activity.
    - Interviewing relevant personnel, including employees, contractors, and any other individuals who may have information about the breach.
    - Engaging external experts, such as forensic investigators or cybersecurity firms, if necessary, to provide specialized expertise.
    - Analyzing malware or other malicious software.
    - Examining network traffic and data flows.
    - Identifying vulnerabilities in systems or software.
    - Determining the timeline of the breach.
  - All investigation activities shall be documented in detail, and evidence shall be carefully preserved in accordance with legal and forensic best practices. The documentation will include:
    - A detailed description of the investigation process
    - The findings of the investigation
    - A list of all evidence collected
    - The chain of custody for all evidence
    - The individuals involved in the investigation
    - Dates and times of all investigative activities
    - Any tools or techniques used in the investigation
- **6.4 Risk Assessment:**
- The IRT will conduct a comprehensive risk assessment to evaluate the potential risks and harm to affected individuals and the company. The risk assessment will be conducted as soon as possible after the breach is contained, and will consider factors such as:
    - The type and sensitivity of the data involved, including whether the data is personal data, sensitive data, or confidential

- business information.
- The amount of data involved
  - The likelihood of misuse of the data, including the potential for identity theft, fraud, or other harm.
  - The potential impact on individuals, including financial loss, reputational damage, emotional distress, and physical harm.
  - The potential impact on the company, including financial loss, reputational damage, legal liabilities, regulatory fines, and business disruption.
  - The ease with which the data can be accessed and used.
  - The security measures that were in place at the time of the breach.
  - Any mitigating factors that may reduce the risk of harm.
- The risk assessment will be documented, and will be used to determine the appropriate response and notification strategy.
- **6.5 Notification:**
    - Inazuma.co will comply with all applicable legal and regulatory requirements regarding the notification of data breaches, including the Digital Personal Data Protection Act, 2023. The company will also adhere to any contractual notification obligations.
    - **Notification to Regulatory Bodies:** The company shall notify the relevant regulatory bodies, such as the Data Protection Board of India, within the timeframe specified by law (if applicable). The notification will include all information required by law, and will be made in the manner prescribed by the regulatory body.
    - **Notification to Affected Individuals:** The company shall notify affected individuals if the data breach is likely to result in significant harm to them. The decision to notify will be based on the risk assessment conducted by the IRT, and will be made in consultation with legal counsel. The notification will be:
      - **Timely:** Notifications will be made as soon as practicable after the determination that notification is required.
      - **Clear and Conspicuous:** Notifications will be written in plain language and will be easy to understand.

- They will be delivered in a manner that is likely to be noticed by the recipient.
- Accurate: Notifications will provide accurate and complete information about the breach.
  - Individualized: To the extent possible, notifications will be tailored to the specific circumstances of each affected individual.
  - Delivered through appropriate communication channels, such as:
    - Email
    - Mail
    - Telephone
    - Public notice (if individual notification is not feasible)
    - Website posting
  - The notification to affected individuals shall include:
    - A description of the data breach, including the date, time, and location of the breach.
    - The type of data involved, including the specific types of personal data that were compromised.
    - The steps the company has taken to contain and investigate the breach.
    - The potential risks and consequences of the breach, including the likelihood of harm to affected individuals.
    - The steps affected individuals can take to protect themselves, such as changing passwords, monitoring their accounts, and reporting any suspicious activity.
    - Contact information for further inquiries, including a telephone number and email address.
    - Any other information required by law.
- **Notification to Other Stakeholders:** The company may also notify other stakeholders, such as:
- Business partners: If the breach involves data shared with business partners.
  - Credit reporting agencies: If the breach involves financial data.
  - Law enforcement agencies: If the breach involves criminal activity.
  - Vendors: If the breach involves data processed by vendors.
  - Insurance providers: As required by the company's insurance policies.

- All notifications shall be approved by the Team Leader and senior management, in consultation with legal counsel.
- **6.6 Remediation:**
  - The IRT will develop and implement a comprehensive remediation plan to address the root causes of the breach, prevent future incidents, and restore affected systems and data. The remediation plan will be tailored to the specific circumstances of the breach, and may include:
    - Implementing security enhancements, such as:
      - Stronger passwords
      - Multi-factor authentication
      - Encryption of data in transit and at rest
      - Firewall upgrades
      - Intrusion detection and prevention systems
      - Access controls, including the principle of least privilege
      - Security patches and updates
    - Patching vulnerabilities in systems and software.
    - Improving data security policies and procedures.
    - Providing additional training to employees on data security best practices.
  - Recovering lost or corrupted data from backups.
  - Restoring affected systems to their pre-breach state.
  - Offering credit monitoring or other protective services to affected individuals, where appropriate.
  - Conducting a thorough review of the company's security posture.
  - Implementing new security technologies.
  - Improving incident response procedures.
  - Increasing security awareness training for employees.
  - Taking disciplinary action against any employees who were responsible for the breach, if applicable.
  - The remediation plan will be documented, and its implementation will be tracked and monitored.
- **6.7 Documentation and Reporting:**
  - The IRT will maintain a detailed and accurate record of the data breach, including:
    - The date and time of the breach.
    - The date of discovery
    - The source or cause of the

- breach.
- A description of the vulnerability exploited
  - The extent of the data compromise, including the types and amount of data affected.
  - The systems and individuals affected.
  - The actions taken to contain, investigate, and remediate the breach.
  - Copies of all notifications sent to regulatory bodies and affected individuals.
  - The costs associated with the breach, including investigation costs, notification costs, legal fees, and any other expenses.
  - Lessons learned from the breach.
  - Recommendations for preventing future breaches.
- A post-incident report will be prepared and submitted to senior management and the Board of Directors, outlining the findings of the investigation, the actions taken, and recommendations for preventing future breaches. The report will be comprehensive and will include:
- An executive summary
- A detailed description of the incident
  - The results of the risk assessment
  - A summary of the notifications made
  - A description of the remediation efforts
  - A cost analysis
  - A timeline of the incident and the response
  - A list of any policy or procedural changes that are recommended
  - The report will be reviewed by the Board of Directors and senior management, and will be used to improve the company's data security practices.
- ## 7. Notification Procedures
- **7.1 Legal Requirements:**  
Inazuma.co shall comply with all applicable data breach notification laws, including the Digital Personal Data Protection Act, 2023. The company will stay up-to-date on any changes to these laws and regulations.
  - **7.2 Internal Notification:**
    - The Company Secretary shall be responsible for notifying the Board of Directors and senior management of any significant data breach. Notification will be made as soon as practicable after the discovery

- of the breach.
- Internal notification will include:
    - A summary of the incident
    - The potential impact on the company
    - The steps being taken to respond to the breach
    - The need for any additional resources
- **7.3 External Notification:**
    - The decision to notify external parties, including regulatory bodies and affected individuals, shall be made by the IRT in consultation with legal counsel, considering the severity of the breach and the applicable legal requirements. The company will follow a risk-based approach to notification, prioritizing notification in cases where there is a high risk of harm to affected individuals.
    - All external notifications shall be approved by the Team Leader and senior management.
    - Notifications to affected individuals shall be made in a clear and conspicuous manner, using appropriate communication channels (e.g., email, mail, telephone, public notice). The method of notification will be determined based on the circumstances of the breach and the contact information available for affected individuals.
  - **7.4 Content of Notification:**
    - Notifications shall include the information required by law and any additional information that may be helpful to the recipients. This may include:
      - A description of the data breach, including the date, time, and location of the breach.
      - The type of information involved, including the specific types of personal data that were compromised.
      - The date of the breach (if known).
      - The steps the company has taken to address the breach, including containment, investigation, and remediation efforts.
      - The potential risks to affected individuals, including the likelihood and severity of potential harm.
      - Advice on what affected individuals can do to protect themselves, such as changing passwords, monitoring their accounts, and reporting any suspicious activity.
      - Contact information for further information,

- including a telephone number and email address.
- Any other information required by law, including any specific requirements under the Digital Personal Data Protection Act, 2023.
- If the breach involves identity theft, the notification will include information on how to obtain a credit report and how to place a fraud alert on their credit file.
- If the breach involves financial information, the notification will advise individuals to monitor their bank and credit card accounts for unauthorized transactions.

## 8. Data Security Measures

Inazuma.co shall implement and maintain appropriate technical and organizational measures to protect data and prevent data breaches. These measures will be designed to address the specific risks faced by the company, and will be regularly reviewed and updated to ensure their effectiveness. These measures may include:

- **8.1 Data Minimization:** Collecting only the data that is necessary for the specified purpose. The company will review its data

collection practices to ensure that it is not collecting more data than is needed.

- **8.2 Storage Limitation:** Retaining data only for as long as necessary to fulfill the purpose for which it was collected, and in accordance with the company's data retention policy and applicable laws.
- **8.3 Encryption:** Encrypting sensitive data both in transit and at rest, using strong encryption algorithms. This includes encrypting data stored on servers, databases, laptops, and mobile devices, as well as data transmitted over networks and the internet.
- **8.4 Access Controls:** Implementing strict access controls to restrict access to data to authorized personnel only. This includes:

- Strong passwords that meet industry best practices (e.g., length, complexity, regular changes).
- Multi-factor authentication (MFA) for all systems that contain sensitive data.
- The principle of least privilege, which means that users are only granted the minimum level of access necessary to perform their job duties.
- Role-based access control (RBAC) to manage user

- permissions.
- Regular review and revocation of access rights.
  - Secure log-in procedures.
  - Automatic logoff for inactive sessions.
- **8.5 Security Awareness Training:**  
Providing regular security awareness training to all employees and contractors. The training will cover:
    - The importance of data security
    - The company's data security policies and procedures
    - How to identify and report potential data breaches
    - Common threats, such as phishing, malware, and social engineering
    - Best practices for protecting data, such as using strong passwords and avoiding suspicious emails
    - The consequences of violating data security policies
    - Specific requirements of the Digital Personal Data Protection Act, 2023
    - The training will be ongoing and will be updated regularly to address new threats and vulnerabilities.
- **8.6 Vulnerability Management:**  
Regularly assessing and addressing vulnerabilities in systems and software through:
    - Regular security scans
    - Penetration testing
    - Patch management
    - Vulnerability tracking
    - Prompt remediation of identified vulnerabilities
- **8.7 Intrusion Detection and Prevention Systems:**  
Implementing systems to detect and prevent unauthorized access to data and systems, including:
    - Intrusion detection systems (IDS)
    - Intrusion prevention systems (IPS)
    - Firewalls
    - Security information and event management (SIEM) systems
- **8.8 Regular Backups:** Performing regular backups of data and ensuring their secure storage and recovery. Backups will be:
    - Performed regularly
    - Stored securely, both on-site and off-site
    - Tested regularly to ensure that they can be restored successfully
- **8.9 Data Loss Prevention (DLP) Tools:** Utilizing tools to prevent sensitive data from leaving the organization's control, whether intentionally or unintentionally.
- **8.10 Physical Security:**  
Implementing measures to protect physical access to data and systems, including:

- Secure facilities
  - Access controls
  - Surveillance cameras
  - Security guards
  - Secure storage for physical records
- **8.11 Vendor Risk Management:** Ensuring that third-party vendors that process data on behalf of Inazuma.co have adequate security measures in place to protect the data. This includes:
    - Conducting due diligence on vendors
    - Including data security requirements in contracts
    - Monitoring vendor compliance
    - Regularly assessing vendor security practices
  - **8.12 Data Privacy Impact Assessments (DPIAs):** Conducting DPIAs for any new projects or initiatives that involve the processing of personal data, particularly sensitive data, to identify and mitigate potential privacy risks.

## 9. Policy Review and Updates

This Policy shall be reviewed and updated at least annually, or more frequently as needed, to reflect changes in legal requirements, technological advancements, and the company's evolving data protection needs. The review will ensure that the policy remains relevant, effective, and

compliant with all applicable laws and regulations. Any updates to this Policy shall be approved by the Board of Directors. The company will also seek input from relevant stakeholders, such as the Information Security team, the Legal department, and the Compliance department, during the review process.

## 10. Employee Acknowledgement

All employees and contractors shall be required to acknowledge that they have read, understood, and agree to comply with this Policy. This acknowledgement will be obtained in writing, either electronically or in hard copy, and will be retained by the company. New employees and contractors will be required to acknowledge the policy as part of their onboarding process. Employees will also be required to acknowledge any updates to the policy. Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment or contract.