Inazuma.co

Information Security Policy

1. Introduction

Inazuma.co recognizes the importance of protecting its information assets from unauthorized access, use, disclosure, disruption, modification, or destruction. This Information Security Policy establishes a framework for managing and safeguarding information to ensure its confidentiality, integrity, and availability. We are committed to maintaining the trust of our customers, employees, partners, and stakeholders by implementing and adhering to robust security practices.

2. Purpose and Objectives

The purpose of this Information Security Policy is to:

- Provide a comprehensive framework for protecting Inazuma.co's information assets.
- Ensure compliance with applicable legal, regulatory, and contractual obligations related to information security.
- Establish clear roles and responsibilities for maintaining information security.
- Define acceptable use of information assets and technologies.
- Prevent security incidents and minimize their impact if they occur.
- Promote a culture of security awareness and responsibility throughout the organization.
- Provide guidance for the implementation of specific security controls and procedures.
- Ensure business continuity and minimize disruptions.

3. Scope

This policy applies to all information assets owned, controlled, or processed by Inazuma.co, including but not limited to:

- **Physical assets:** Facilities, equipment, hardware (e.g., computers, servers, mobile devices), and storage media.
- **Electronic information:** Data, software, applications, databases, and systems.
- **Networks:** Local area networks (LANs), wide area networks (WANs), wireless networks, and internet connections.
- **Communications:** Email, messaging, voice communications, and video conferencing.
- **Documents:** Paper documents, electronic documents, and records.
- **Personnel:** Employees, contractors, temporary staff, and any third parties accessing Inazuma.co's information assets.

This policy covers all activities involving information, including but not limited to:

- Collection
- Storage
- Processing
- Transmission
- Access
- Usage
- Sharing
- Disposal

4. Definitions

To ensure clarity and consistent understanding, the following definitions apply to this policy:

Term	**Definition**
Information Asset	Any data, system, device, or resource that has value to Inazuma.co.
Confidentiality	Ensuring that information is accessible only to authorized individuals.
Integrity	Ensuring the accuracy and completeness of information and preventing its unauthorized modification.
Availability	Ensuring that authorized users can access information and related assets when needed.
Threat	A potential cause of an unwanted incident that may result in harm to Inazuma.co.
Vulnerability	A weakness of an asset or control that can be exploited by a threat.
Risk	The potential for harm or loss when a threat exploits a vulnerability.
Security Incident	An event that compromises the confidentiality, integrity, or availability of information.
Access Control	The process of granting or denying specific requests to obtain and use information and related information processing systems.
Encryption	The process of converting information into an unreadable format to protect its confidentiality.

Authentication	The process of verifying the identity of a user, process, or device.
Authorization	The process of granting specific access rights to a user, process, or device.
Data Breach	A security incident that results in the unauthorized access, use, disclosure, disruption, modification, or destruction of personal information.
Personally Identifiable Information (PII)	Any information that can be used to identify an individual, directly or indirectly.
Third Party	Any individual or organization that is not part of Inazuma.co.

5. Information Security Principles

Inazuma.co adheres to the following principles to ensure the effective protection of its information assets:

Principle	**Description**
Risk Management	Identify, assess, and respond to information security risks in a systematic and ongoing manner.
Least Privilege	Grant users only the minimum necessary access rights required to perform their job duties.
Defense in Depth	Implement multiple layers of security controls to protect against a variety of threats.
Separation of Duties	Divide critical tasks among different individuals to prevent a single point of failure or malicious activity.
Need-to-Know	Access to information is granted only to those who require it to fulfill their job responsibilities.
Security Awareness	Provide regular training and promote awareness of information security responsibilities among all personnel.

Incident Response	Establish and maintain a plan for responding to and recovering from security incidents.
Continuous Improvement	Regularly review and update security policies, procedures, and controls to address evolving threats and vulnerabilities.
Compliance	Adhere to all applicable laws, regulations, and contractual obligations related to information security.
Accountability	Ensure that all individuals are held accountable for their actions related to information security.
Integrity	Maintain the accuracy and reliability of information assets.
Availability	Ensure that information assets are accessible to authorized users when needed.