Inazuma.co Acceptable Use Policy (AUP)

Version: 1.0
Effective Date: [Insert Date]
Reviewed By: Information Security and Compliance Team
Next Review Date: [Insert Date]

1. Purpose

This Acceptable Use Policy (AUP) outlines the acceptable and unacceptable uses of Inazuma.co’s information systems, computing devices, networks, and digital resources. The objective is to protect the integrity, confidentiality, and availability of Inazuma.co's digital infrastructure and to ensure a secure and productive environment for all employees, contractors, interns, and third-party vendors. This policy also seeks to:

- Promote responsible digital behavior;
- Prevent data loss and cyber threats;
- Ensure legal and regulatory compliance;
- Protect the reputation and operations of the organization.

2. Scope

This policy applies to all users of Inazuma.co's technology systems, including:

- Full-time and part-time employees
- Contractors and consultants
- Interns and apprentices
- Vendors and third-party partners
- Temporary or remote workers

The policy is applicable regardless of location, including on-site offices, remote work environments, co-working spaces, or any place where Inazuma.co systems or data are accessed.

3. Acceptable Use

3.1 General Guidelines

All users must:

- Access systems only through their authorized credentials.
- Use corporate assets (devices, data, networks) only for Inazuma.co-related activities.
- Adhere to organizational cybersecurity practices.
- Respect the intellectual property of the company and third parties.

- Avoid any conduct that disrupts, damages, or impairs company systems or business operations.

3.2 Permitted Uses

Permitted Use	Examples
Business communications	Email, chat, and video calls for work-related matters
Data analysis and software development	Use of authorized tools to perform job duties
Research	Market, product, or technical research as needed
Collaboration	Accessing shared drives, project management tools
Training and learning	Attending internal or external training sessions
Process documentation	Writing SOPs, process guides, and product documentation

4. Prohibited Use

Users must not engage in any of the following activities:

4.1 Unauthorized Activities

- Accessing internal systems not required for one's job function.
- Tampering with or bypassing security systems, firewalls, or access controls.
- Sharing login credentials or using another person's credentials.

4.2 Inappropriate Use of Resources

- Viewing, downloading, or distributing offensive or explicit material.
- Streaming non-work-related media during work hours.
- Running unauthorized software or scripts.

4.3 Personal Use Restrictions

- Excessive personal use of email, internet, or chat systems during work hours.
- Conducting personal business ventures on company time or infrastructure.

4.4 External Threats

- Clicking suspicious links or attachments in emails.

- Uploading company data to unauthorized cloud storage platforms.
- Using USB drives or external hardware without prior approval.

5. Email and Internet Usage

Emails and internet services provided by Inazuma.co are intended for business purposes. Users should:

- Use official email addresses for all company-related communication.
- Be mindful of tone, clarity, and professionalism in written correspondence.
- Avoid subscribing to unnecessary mailing lists or third-party newsletters.
- Report any suspicious or phishing email to the IT security team.
- Avoid using unauthorized internet-based communication platforms.

5.1 Web Browsing Guidelines

Permitted	Not Permitted
Business research	Gambling sites, pornographic content
Accessing industry news	Torrenting or illegal downloads
Learning platforms (e.g., Coursera)	Streaming Netflix/YouTube during work unless approved
Product analytics dashboards	Posting on forums without anonymity or approvals

6. Data Protection and Privacy

All users are expected to treat company and customer data with the utmost confidentiality. Specific practices include:

- Encrypting sensitive files and communication.
- Storing all data on designated, approved storage platforms.
- Avoiding transmission of confidential data via unencrypted emails or public platforms.
- Locking screens when stepping away from devices.
- Complying with the company’s Data Protection Policy and Privacy Notice.

7. Mobile and Remote Access

7.1 Access Conditions

- Remote access is allowed only through authorized Virtual Private Networks (VPNs).
- Only company-provided or approved devices should be used for remote work.

7.2 Device Security

- Use biometric or strong password authentication.
- Keep devices updated with the latest patches and antivirus definitions.
- Enable auto-lock and screen timeout features.
- Do not leave devices unattended in public spaces.

8. Monitoring and Auditing

Inazuma.co reserves the right to monitor digital activities to:

- Ensure compliance with internal policies and external regulations;
- Detect and respond to security threats;
- Conduct performance and productivity evaluations.

Monitoring may include:

- Email logs and content
- Internet browsing history
- Application usage statistics
- Access control logs

Users consent to such monitoring by accessing company systems.

9. Enforcement

Violations of this AUP will result in disciplinary actions such as:

Violation Severity	**Examples**	**Potential Action**
Minor	Excessive personal browsing	Verbal or written warning
Moderate	Installing unauthorized software	Access restrictions or

		performance review
Severe	Data breach, unauthorized access, harassment	Suspension, termination, or legal action

All incidents will be documented, and repeat offenders may face progressive disciplinary measures.

10. Responsibilities

Role	**Responsibility**
Employees	Adhere to this policy and report suspicious activities
IT Department	Ensure proper controls, monitoring, and user access provisioning
Compliance Officer	Investigate violations and ensure ongoing policy relevance
Managers	Enforce policy within their teams and guide users
Security Team	Conduct audits and manage security incidents

11. Training and Awareness

All new employees must complete an Acceptable Use Policy training module during onboarding. Annual refresher sessions will be held to:

- Reiterate the importance of compliance.
- Demonstrate policy updates or changes.
- Share best practices and common violations.

12. Policy Review and Updates

This policy is reviewed at least once per year or when significant technological or regulatory changes occur. Employees will be notified of updates through email and internal communications platforms.

13. Related Policies and Documents

- Information Security Policy
- Data Protection and Privacy Policy
- Password Policy
- Remote Work Policy

- Incident Response Plan

Acknowledgment Form

I have read and understood the Acceptable Use Policy. I agree to follow the principles and guidelines stated herein.

Name: _____________________
Signature: __________________
Date: ______________________