Inazuma.co Password Policy Document

Version: 1.0

Reviewed By: IT Security Department

1. Purpose

The purpose of this Password Policy is to establish a comprehensive standard for the creation, protection, and management of passwords at Inazuma.co. As a data-driven D2C enterprise with expansive digital infrastructure, protecting user identities and maintaining secure access is vital to business continuity and trust. Weak or compromised passwords significantly heighten the risk of cyber-attacks, data breaches, identity theft, and system corruption. This policy serves to mitigate such risks and strengthen the company’s overall security posture.

2. Scope

This policy applies to all individuals who access Inazuma.co information systems, including full-time and part-time employees, contractors, interns, consultants, temporary staff, and third-party vendors. It encompasses:

- Local machine accounts (workstations, servers)
- Web applications
- Cloud services
- VPN and remote access systems
- Network infrastructure (firewalls, routers, switches)
- Databases, code repositories, and other platforms requiring authentication

3. Password Creation Requirements

To ensure consistency and reduce vulnerability, all passwords must adhere to the following standards:

Requirement	Minimum Standard
Length	At least 12 characters
Character Variety	Must include uppercase, lowercase, number, and special character
Dictionary Words	Must not contain dictionary words or usernames
Repeat Passwords	Cannot reuse the last 5 passwords
Password Expiry	Must be changed every 90 days
Common Passwords	Use of any password on the global blacklist is prohibited

3.1 Examples of Strong Passwords:

- G7r@2#uLpXq9
- Z!3vMk@20rPf
- B!u3Rain&Tx#17

3.2 Prohibited Passwords:

- password123
- Welcome@2023
- admin01
- qwerty!@#

3.3 Password Suggestions:

Use a passphrase technique by stringing unrelated words and symbols together. Example:

- **Correct@Horse1Staple!**
- **Tree#Lamp$Cloud9&Moon**

---

4. Password Management

4.1 Storage and Transmission

- Passwords must never be written down or stored in plain text.
- Use of sticky notes, notebooks, or email drafts to store credentials is strictly forbidden.
- Passwords must be stored only in company-approved encrypted password management solutions.
- Passwords must not be transmitted via unsecured platforms (e.g., chat apps, personal email).

4.2 Change Protocol

- Mandatory password changes every 90 days for standard accounts.
- High-privilege accounts must change passwords every 30 days.
- Immediate password reset is required after suspected compromise or termination of employment.

4.3 Multi-Factor Authentication (MFA)

- MFA is mandatory for all critical systems including HRMS, CRM, codebase, financial, and admin dashboards.

- Second-factor options include biometrics, authenticator apps, and hardware tokens.
- SMS-based MFA is discouraged due to known vulnerabilities.

5. Responsibilities

Role	Responsibility
IT Security Team	Enforce password policy, monitor violations, approve tools
HR Department	Communicate password policies during onboarding and induction training
Compliance Team	Ensure adherence to regulations like ISO 27001 and GDPR
All Users	Create and maintain secure passwords, report incidents, complete training

6. Technical Controls

- Mandatory complexity enforcement at OS and application levels.
- Account lockout for 15 minutes after 5 consecutive failed attempts.
- Forced password change after first-time login.
- Audit trails and access logs must be enabled and reviewed quarterly.
- Integration with SIEM tools to monitor anomalies in login patterns.

7. Password Sharing and Privileged Accounts

7.1 Prohibition on Sharing

- No employee may share passwords with anyone, including team members.
- Shared credentials for team accounts (e.g., project tools) must be avoided.

7.2 Emergency Access

- Emergency access passwords must be stored in encrypted vaults with access logged.
- Temporary emergency access accounts must be disabled immediately after use.

7.3 Privileged Accounts

- Must use passwords of at least 16 characters.
- Subject to monthly audit and password rotation.
- Access must be logged with user activity and timestamp.
- Use of just-in-time privileged access management tools is strongly recommended.

---

8. Incident Management

8.1 Reporting

- Suspected credential compromise must be reported via the IT Helpdesk or security hotline within one hour.

- Immediate revocation of credentials if an account is involved in phishing or unauthorized access attempts.

8.2 Response

- Forensic analysis of login history, location, and device logs.
- Communication to affected stakeholders.
- Reset of all related access keys, API tokens, and secondary credentials.

---

9. Enforcement

9.1 Disciplinary Actions

- Non-compliance will be handled as per the Employee Disciplinary Policy.
- First offenses may result in formal warnings; repeat violations may lead to termination.
- Vendors failing to follow password standards may be barred from future contracts.

9.2 Monitoring and Audit

- Quarterly access reviews to detect excessive privilege or orphan accounts.
- Monthly scans for weak passwords using credential auditing tools.
- Penetration testing will assess password strength periodically.

---

10. Policy Review and Updates

- This policy is subject to annual review or earlier if prompted by security incidents or regulatory updates.
- All policy changes will be communicated via internal announcements and training portals.
- Employees must sign acknowledgment forms upon major policy revision.

Appendix A: Password Best Practices

- Avoid keyboard patterns (e.g., 123456, qwerty)
- Use different passwords for work, personal, and social platforms
- Always log out from shared or public devices
- Clear browser-saved passwords on shared machines
- Do not use company credentials for third-party or personal sites
- Change passwords immediately after returning from extended leave

---

Appendix B: Password Lifecycle Timeline

Event	Timeframe
Password Creation	Upon onboarding / new access
First Change	Within 24 hours of account issuance
Routine Change	Every 90 days (30 days for privileged accounts)
Emergency Change	Within 1 hour of suspected compromise

Post-Termination Deactivation	Within 2 hours of offboarding

Acknowledgment Form

I acknowledge that I have read, understood, and agree to comply with the Inazuma.co Password Policy.