Meme Bull: Information Security Policy

Policy Version: 1.0
Effective Date: January 2026
Applicability: All employees, contractors, and systems handling Meme Bull data.

1. Purpose & Scope

This document defines the framework for protecting Meme Bull's information assets (data, systems, networks) against internal and external threats. It applies to all company operations.

2. Information Security Principles

Confidentiality: Protecting information from unauthorized access.
Integrity: Safeguarding the accuracy and completeness of information.
Availability: Ensuring authorized users have reliable access to information when needed.

3. Governance & Responsibilities

Leadership: The CEO and Board are ultimately responsible for security governance.

CISO: The Chief Information Security Officer oversees policy implementation and the security program.

All Personnel: Responsible for adhering to all security policies and procedures.

4. Asset Management

All information assets shall be classified (e.g., Public, Internal, Confidential, Restricted) and inventoried. Handling requirements are defined per classification level.

5. Human Resources Security

Security roles are defined in job descriptions.
Background checks are conducted for relevant roles.
Mandatory security awareness training is provided annually and upon hiring.

6. Physical & Environmental Security

Secure access controls to company premises and data centers.
Protection against environmental threats (fire, flood).

7. Operational Security

Secure Development: Security-by-design principles integrated into the Software Development Lifecycle (SDLC).

Cryptography: Industry-standard encryption (AES-256, TLS 1.2+) for data at rest and in transit. Private keys are managed in Hardware Security Modules (HSMs) or secure vaults.

Vulnerability Management: Regular automated and manual security testing (penetration testing, code reviews). Critical vulnerabilities are patched based on a defined SLA.

Logging & Monitoring: Centralized logging of security events (access attempts, transactions). 24/7 Security Operations Center (SOC) monitoring and alerting.

Backup: Regular encrypted backups of critical data with tested restoration procedures.

8. Access Control Policy

Principle of Least Privilege: Users are granted minimum access necessary.

Strong Authentication: Multi-Factor Authentication (MFA) is mandatory for all administrative access and user accounts where feasible.

Identity & Access Management (IAM): Centralized control of user lifecycle (provisioning, de-provisioning, periodic access reviews).

9. Incident Response Plan

A formal plan is maintained to:

Prepare: Designated Incident Response Team (IRT) with clear communication channels.
Identify & Contain: Detect, analyze, and isolate security incidents.
Eradicate & Recover: Remove threat artifacts and restore systems.
Lessons Learned: Post-incident review and process improvement.

10. Business Continuity & Disaster Recovery (BC/DR)

BC/DR plans are documented and tested annually to ensure rapid recovery of critical services following a disruption.

11. Compliance

The security program is designed to align with relevant regulatory and industry standards (e.g., GDPR, SOC 2 Type II framework, essential financial regulations).

12. Policy Review

This policy is reviewed and updated at least annually or in response to significant changes in the threat landscape or business operations.