Comprehensive Security Policy

Purpose

This document outlines key security rules, an incident response plan, and explains how these policies uphold the principles of the **CIA Triad** (Confidentiality, Integrity, Availability).

1. Key Security Rules/Guidelines

Rule 1: Strong Password Policy

- **Employees must create passwords with at least 12 characters**, including upper/lowercase letters, numbers, and symbols.
- **Passwords must be changed every 90 days** and must not be reused within the last 5 cycles.
- **Multi-Factor Authentication (MFA)** is required for all remote access and sensitive system logins.

Rule 2: Acceptable Use of Technology

- Company-owned devices and networks must be used **only for authorized business purposes**.
- **No unauthorized software installations** or external storage device usage without IT approval.
- **Employees must report any suspicious emails or system behavior immediately** to the IT department.

Rule 3: Data Protection and Encryption

- **All sensitive data must be encrypted** at rest and in transit.
- **Confidential information must not be shared** outside the organization without appropriate authorization and security measures.
- **Employees must use VPNs** when accessing corporate resources from public or unsecured networks.

2. Incident Response Plan

Detection

- Utilize intrusion detection systems (IDS) and endpoint protection to monitor and alert on suspicious activity.
- Encourage employees to report any anomalies (e.g., phishing emails, system slowdowns) immediately.

Containment

- **Isolate** affected systems from the network to prevent spread.
- **Block access** to compromised accounts or services.
- **Inform relevant stakeholders** (management, legal, communication teams) about the incident.

Eradication

- Identify the cause of the incident (e.g., malware, unauthorized access).
- Remove malware, patch vulnerabilities, and disable any malicious accounts.
- Update all affected systems with the latest security fixes.

Recovery

- Restore data from verified, clean backups.
- Gradually reconnect systems to the network under enhanced monitoring.
- Conduct post-incident audits and security assessments.

Lessons Learned

- Document the incident, response actions, and outcomes.
- Update policies and procedures based on lessons learned to prevent future incidents.
- Conduct a follow-up training session with employees if necessary.

3. Maintaining the CIA Triad

Confidentiality

- **Strong password policies**, encryption standards, and restricted access controls ensure that sensitive information is only accessible to authorized users.
- Security training and acceptable use policies prevent unintentional disclosure of confidential data.

Integrity

- Regular system updates, incident response procedures, and endpoint security tools help maintain the **accuracy and trustworthiness** of information.
- Post-incident audits ensure that any compromised data is restored to its correct state.

Availability

- Incident response measures, system redundancy, and frequent backups ensure that data and systems remain **available even during and after a security breach**.
- Quick detection and recovery steps minimize downtime, keeping critical business operations running smoothly.

Conclusion

By following this comprehensive security policy—including strict security rules, a robust incident response plan, and adherence to the CIA Triad principles—the organization strengthens its cybersecurity posture, protects its assets, and maintains trust with clients and partners.