Security Policy Document

1. Security Rules and Guidelines

- **Access Control Policy**:
    - **Guideline**: Only authorized personnel should have access to sensitive systems and data. Multi-factor authentication (MFA) is required for accessing critical infrastructure, and access rights must be granted on a need-to-know basis.
    - **Purpose**: Limiting access to verified individuals enhances confidentiality and protects sensitive data from unauthorized access or leakage.
- **Data Encryption Policy**:
    - **Guideline**: All sensitive data, whether at rest or in transit, must be encrypted using industry-standard protocols such as AES-256 for stored data and TLS 1.2 or higher for data in transit.
    - **Purpose**: Encryption safeguards the integrity of the data, preventing unauthorized alterations, ensuring confidentiality, and maintaining compliance with regulatory standards.
- **Patch Management Policy**:
    - **Guideline**: Systems and software must be updated regularly, and critical security patches should be applied within 24 hours of release. Automated tools are recommended to streamline patch deployment.
    - **Purpose**: Timely updates reduce vulnerabilities that attackers may exploit, ensuring that systems remain secure and minimizing risks to data integrity and availability.

---

2. Incident Response Plan

Objective: In the event of a security breach, this plan outlines clear steps to detect, contain, eradicate, and recover from incidents to minimize damage and prevent recurrence.

- **Step 1: Detection and Identification**
    - Use a Security Information and Event Management (SIEM) system to monitor network traffic and alert the security team to unusual activities.
    - Perform a thorough investigation to identify the nature and scope of the breach.
- **Step 2: Containment**
    - **Short-term**: Immediately isolate affected systems from the network to prevent further spread.
    - **Long-term**: Implement segmented network zones and limit access to only essential users and systems until the root cause of the breach is identified and addressed.
- **Step 3: Eradication**

    - Conduct a malware scan on all affected systems to remove malicious software.
    - Apply any missing security patches and harden system configurations as necessary.
- **Step 4: Recovery**
    - Restore systems from secure, malware-free backups, ensuring they are fully operational.
    - Monitor the network and systems closely for any signs of lingering threats.
- **Step 5: Post-Incident Review and Improvements**
    - Conduct a post-mortem review to analyze the incident response and identify areas for improvement.
    - Update policies, training programs, and response plans as necessary to prevent similar breaches in the future.

---

3. Maintaining the CIA Triad

- **Confidentiality**: Access Control and Data Encryption policies ensure that sensitive information is only accessible to authorized personnel and is unreadable if intercepted. This reduces the likelihood of data leaks and maintains confidentiality.
- **Integrity**: By mandating encryption and timely patch management, these policies protect data from unauthorized modifications or tampering. Any alterations can be detected and rectified, upholding data accuracy and trustworthiness.
- **Availability**: Patch Management policies protect against disruptions by reducing vulnerabilities that could lead to service outages. The incident response plan includes recovery procedures to restore data and systems quickly after a breach, ensuring business continuity and data availability.