**Name: Kabeer Ahmad**

**Incident Response Plan (IRP)**

**1. Purpose:**

The purpose of this Incident Response Plan is to provide a structured approach for detecting, responding to, and recovering from security incidents. This plan aims to minimize the impact of security breaches, mitigate risks, and recover systems in a timely and controlled manner.

**2. Incident Response Team (IRT):**

The Incident Response Team is responsible for handling all aspects of the incident response lifecycle. The team consists of the following roles:

**Incident Commander**:

* Responsible for leading and coordinating the entire incident response process.
* Ensures all phases of the IRP are followed.
* Liaises with senior management and external parties.

**Security Analyst(s)**:

* Investigates and analyzes the technical aspects of the incident.
* Responsible for identifying, containing, and eradicating threats.
* Documents findings and reports to the Incident Commander.

**System Administrator(s)**:

* Ensures the affected systems are contained and recovered.
* Responsible for applying patches, restoring backups, and monitoring recovery efforts.

**Legal Counsel**:

* Advises on legal implications of the incident.
* Provides guidance on regulatory reporting requirements.

**Communications Lead**:

* Handles internal and external communications regarding the incident.
* Coordinates with PR teams to manage public statements and updates.

**3. Incident Classification:**

Incidents are classified based on severity and impact on business operations. This helps prioritize the response:

* **Low**: Minor incidents with little to no impact on business continuity (e.g., isolated malware).
* **Medium**: Incident affecting non-critical systems or data (e.g., compromised employee account).
* **High**: Incident impacting critical systems, customer data, or causing a data breach (e.g., SQL Injection leading to data leakage).
* **Critical**: Major breaches that could cause severe operational or financial damage, or widespread data theft.

**4. Incident Response Phases:**

**Phase 1: Preparation**

* Set up logging and monitoring tools to detect unusual behavior in real-time (e.g., using SIEM systems).
* Regularly train staff on incident response procedures.
* Ensure that backups of all critical systems and data are up to date.
* Prepare communication templates for internal and external stakeholders.

**Phase 2: Detection & Identification**

* **Objective**: Detect and accurately identify the occurrence of an incident.
  + Review security alerts from IDS/IPS, monitoring tools, or user reports.
  + Identify the type of incident (e.g., malware, data breach, DoS attack).
  + Gather necessary evidence such as log files, screenshots, or forensic data.

**Tools**: SIEM (Security Information and Event Management), IDS/IPS, Firewall Logs.

**Phase 3: Containment**

* **Objective**: Prevent the spread of the incident and minimize damage.
  + **Short-term containment**:
    - Disconnect affected systems from the network or isolate them.
    - Restrict access to the affected systems.
  + **Long-term containment**:
    - Patch affected systems and mitigate vulnerabilities.
    - Establish new firewall rules, and deploy security controls to prevent further exploitation.

**Phase 4: Eradication**

* **Objective**: Eliminate the root cause of the incident.
  + Remove malware, compromised accounts, or affected files.
  + Patch vulnerabilities that were exploited.
  + Harden systems against future attacks (e.g., implement multi-factor authentication, patch systems).
  + Review logs to ensure all traces of the attacker have been removed.

**Phase 5: Recovery**

* **Objective**: Restore systems and services to their normal state.
  + Restore affected systems from clean backups.
  + Closely monitor systems after restoration for any unusual activity.
  + Validate the effectiveness of fixes and patches.
  + Perform tests to ensure that the application and services are functioning as expected.

**5. Post-Incident Analysis and Documentation**

* Conduct a **Post-Incident Review** to evaluate the handling of the incident:
  + What went well?
  + What could have been improved?
  + What were the root causes of the incident?
  + Were there any gaps in detection or containment?
* **Document the entire incident response**:
  + Incident timeline.
  + Actions taken during each phase.
  + Decisions made and rationale for them.
  + Lessons learned and recommendations for future improvement.

**6. Communication Plan:**

* **Internal Communication**:
  + Notify stakeholders, such as senior management, about the status of the incident response.
  + Provide regular updates on the progress of detection, containment, and recovery.
* **External Communication**:
  + If required, notify customers or affected parties about data breaches or service disruptions.
  + Report the incident to regulators or law enforcement agencies if necessary (e.g., GDPR or local regulatory requirements).
  + Prepare official statements to be released publicly.

**7. Incident Reporting:**

* All incidents should be reported to the Incident Commander immediately after detection.
* Incident reports should include:
  + The nature and scope of the incident.
  + Systems and data affected.
  + Response actions taken.
  + Estimated impact (financial or reputational damage).

**8. Conclusion:**

* After the incident response is complete, review and update this plan based on lessons learned.
* Ensure that all identified vulnerabilities have been addressed.
* Schedule regular **Incident Response Plan tests** (e.g., tabletop exercises, simulated breaches) to assess the readiness of the IRT.