Security Incident Response Policy

Our organization has a defined process for detecting, triaging, and resolving security-impacting incidents. The process includes:

1. Detection & Identification
   - Continuous monitoring tools and intrusion detection systems are used to detect potential security incidents in real-time.
   - Employees are trained to report suspected incidents immediately.

2. Triage & Classification
   - Incidents are triaged based on severity, scope, and potential impact.
   - High-severity incidents are escalated to the incident response team (IRT).

3. Containment & Mitigation
   - Affected systems are isolated to prevent further damage.
   - Temporary controls are applied to contain threats while permanent fixes are implemented.

4. Investigation & Resolution
   - Root cause analysis is performed to identify vulnerabilities exploited.
   - Permanent remediation steps are deployed, including security patches, configuration updates, or process changes.

5. Communication
   - Relevant stakeholders, including management and impacted parties, are notified in accordance with the severity of the incident.
   - External communication follows regulatory and contractual obligations.

6. Post-Incident Review
   - Lessons learned sessions are conducted to improve response processes.
   - Incident documentation is stored securely for compliance and auditing.

This structured process ensures that all incidents are promptly detected, properly assessed, effectively mitigated, and thoroughly reviewed to improve future security posture.