IT Security Incident Response SLA Template

1. Purpose

This Service Level Agreement (SLA) defines the scope, objectives, and processes for IT security incident response between the IT Security Team and stakeholders.

2. Scope

This SLA applies to all reported IT security incidents affecting the organizationâ€™s information systems, infrastructure, and data.

3. Definitions

- **Incident:** Any event that compromises the confidentiality, integrity, or availability of information assets.
- **Severity Level:** Classification based on the impact and urgency of the incident.

4. Incident Severity Levels & Response Times

Severity	Description	Initial Response Time	Resolution Time
Critical	System-wide impact, major data breach, or critical business function compromised.	Within 30 minutes	Within 4 hours
High	Significant user group affected, sensitive data potentially compromised.	Within 1 hour	Within 8 hours
Medium	Limited impact, non-sensitive data, individual users affected.	Within 4 hours	Within 3 business days
Low	Minimal impact, informational, or request for information.	Within 1 business day	Within 5 business days

5. Roles and Responsibilities

- **IT Security Team:** Incident identification, classification, analysis, containment, eradication, recovery, and reporting.
- **Stakeholders:** Timely notification of incidents, cooperation during resolution.
- **Management:** Providing resources and support for incident response.

6. Incident Response Process

1. Identify and report the incident.
2. Classify the severity based on impact.
3. Assign response team.
4. Analyze and contain the incident.
5. Eradicate the root cause.
6. Recover affected systems.
7. Communicate status and updates.
8. Close incident and document lessons learned.

7. Communication

The IT Security Team will provide updates to stakeholders as follows:

- Initial notification after incident is identified.

- Regular progress updates during resolution.
- Final report upon closure.

8. Review and Revisions

This SLA will be reviewed annually or upon significant changes in policy, technology, or threat landscape.

9. Approval

Approved by: _____

Date: _____