Incident Response Policy

---

1. Purpose

The purpose of this Incident Response Policy is to establish a structured approach for detecting, responding to, and recovering from security incidents.

---

2. Scope

This policy applies to all employees, contractors, and third parties who handle or access [Organization Name]'s systems and data.

---

3. Incident Response Team

- **Incident Manager**: Oversees the response process.
- **IT Team**: Handles technical containment and recovery.
- **Legal Team**: Advises on compliance and legal implications.
- **PR Team**: Manages communication with stakeholders.

---

4. Incident Response Phases

1. **Preparation**: Train the team and maintain tools.
2. **Detection & Analysis**: Identify and analyze incidents.
3. **Containment**: Isolate affected systems.
4. **Eradication**: Remove the root cause.
5. **Recovery**: Restore systems and data.
6. **Post-Incident Activity**: Review and improve the response process.

---

5. Reporting

- **Internal**: Report incidents to the IT department immediately.
- **External**: Notify law enforcement or regulatory bodies as required.

---

6. Enforcement

- **Monitoring**: The IT department will monitor incident response activities.
- **Violations**: Violations of this policy may result in disciplinary action.

---

7. Acknowledgment

All users must acknowledge that they have read, understood, and agree to comply with this Incident Response Policy.

---

8. Review and Updates

This policy will be reviewed annually or as needed.

Acknowledgment Form

I, [Full Name], acknowledge that I have read, understood, and agree to comply with [Organization Name]'s Incident Response Policy. I understand that violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.

Signature: _____

Date: _____