Incident Response Plan for Network Breach

1. Purpose

This document outlines the response plan for a network breach incident. Its objective is to describe the actions required to minimize the impact of a breach, contain the threats, and recover normal operations.

2. Scope

This plan applies to all employees, systems, and networks of [Organization Name]. All stakeholders must be familiar with the procedures described herein.

3. Definitions

Term	Definition
Incident	Any event that threatens the security, integrity, or availability of network systems.
Network Breach	Unauthorized access to the internal network and its resources.

4. Roles and Responsibilities

Role	Responsibility
Incident Response Team (IRT)	Coordinate and lead the incident response process.
IT Support	Assist in containment, eradication, and recovery actions.
Management	Decision-making, communication, and stakeholder notification.

5. Incident Response Steps

1. **Preparation**
    - Maintain up-to-date contact lists.
    - Train staff and test the incident response plan regularly.
2. **Identification**
    - Detect and confirm the network breach.
    - Document initial facts and affected systems.
3. **Containment**
    - Isolate affected systems from the network.
    - Change access credentials if needed.
4. **Eradication**
    - Remove malicious files and unauthorized users.
    - Patch vulnerabilities exploited in the breach.
5. **Recovery**
    - Restore systems from clean backups.
    - Monitor network for reinfection signs.
6. **Lessons Learned**

    - Conduct post-incident review.
    - Update policies and response plan as needed.

6. Communication Plan

- Inform leadership and affected stakeholders as soon as possible.
- Use predefined templates for internal and external communications.
- Report incidents to regulatory authorities if required.

7. Contact List

Name/Role	Email	Phone
IRT Leader	irt.leader@example.com	+1 555-1234
IT Support	it.support@example.com	+1 555-5678
Management	management@example.com	+1 555-9012

8. Review and Maintenance

This Incident Response Plan must be reviewed annually and updated according to new threats, changes in technology, or lessons learned from incidents.

Document Version: 1.0

Last Reviewed: [Date]