Cybersecurity Breach Response Plan Example

1. Purpose

This document provides a structured plan for the response to cybersecurity breaches to minimize damage, ensure timely notification, and support recovery.

2. Scope

This plan applies to all information systems, employees, contractors, and stakeholders involved in the organization.

3. Incident Response Team Contacts

Role	Name	Email	Phone
Incident Response Lead	Jane Doe	jane.doe@example.com	+1 555 111 2222
IT Security Analyst	John Smith	john.smith@example.com	+1 555 333 4444
Legal Counsel	Maria Lopez	maria.lopez@example.com	+1 555 555 6666

4. Breach Response Steps

1. **Identification**
    - Detect potential incidents via alerts, reports, or unusual activities.
    - Document initial findings (date, type of breach, affected systems).
2. **Containment**
    - Immediately isolate affected systems to prevent further damage.
    - Preserve evidence for forensics.
3. **Eradication**
    - Remove malicious elements (malware, unauthorized accounts).
    - Update system credentials and patch vulnerabilities.
4. **Recovery**
    - Restore affected systems from clean backups.
    - Monitor systems for re-infection or unusual behavior.
5. **Notification**
    - Report breach to legal, regulatory authorities, and affected parties as required.
    - Communicate with employees, customers, and stakeholders.
6. **Post-Incident Review**
    - Conduct a lessons-learned meeting.
    - Update policies, procedures, and security controls.

5. Communication Plan

Internal and external communications must be coordinated by the Incident Response Lead. All information released

must be accurate and approved by legal counsel.

- Do not discuss the breach with media without authorization.
- Follow the pre-defined communication templates for notifications.

6. Documentation and Reporting

All actions taken during the breach response must be documented thoroughly, including:

- Timeline of incident events
- Analysis of cause and impact
- Actions taken and decisions made
- Notified parties and timing

7. Review and Update

This response plan must be reviewed annually and after every major incident to ensure its effectiveness and relevance.