CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

[NAME OR ORGANIZATION OR ADD LOGO]

[DOCUMENT TITLE]

[DOCUMENT SUBTITLE]

ORGANIZATION, DEPARTMENT OR AUTHOR NAME

DATE

CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

DRAFT FOR REVIEW

Table of Contents

I. INTRODUCTION

A. PURPOSE

General statement of what the response plan is meant to accomplish. The statement should be supported by a brief synopsis of the plan's contents.

B. SCOPE

States specifically the facilities, groups, departments, units, or personnel to which the plan applies.

C. SITUATION OVERVIEW

1. Describes, in very general terms, the current planning environment and the types of cybersecurity threats the planning organization must be prepared to manage.

2. Types of cybersecurity threats

   a) Adverse Impact to Organization. These events have significant impact on the normal operations but do not fall into any of the following categories.

   b) Alteration/Compromise of Information. These events involve the unauthorized altering of information or incidents that involve the compromise of information.

   c) Denial of Service Attacks. These events are attacks that affect the availability of critical resources such as email servers, web servers, routers, gateways, or communication infrastructure.

   d) Loss or Theft. These events involve the potential compromise of sensitive material. This includes the compromise of user accounts and passwords that could allow unauthorized persons to access IT resources.

   e) Probes and Scans. These events include probing or scanning networks for critical services or security weaknesses. It also includes nuisance scans.

   f) Unauthorized Access and Unsuccessful Attempts. These events include all successful unauthorized accesses and suspicious unsuccessful attempts.

   g) Virus/Worms/Malicious Code. These events are performed by hackers in an attempt to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity. The attempts include the use of mobile code such as viruses, Trojan horses, worms,

and scripts. This category includes any virus or code that is intended to disrupt or annoy users.

3. Relative probability and potential impact of threats.

4. Vulnerability of critical systems.

5. Dependency of external organizations, vendors, or government agencies.

6. Current asset identification, hazard prevention, protection, and mitigation measures that are in place.

D. PLANNING ASSUMPTIONS

1. Describes what the planning team assumes to be facts for planning purposes in order to execute the plan.

2. During response operations, the assumptions indicate areas where adjustments to the plan have to be made as the facts of the incident become known.

II. CONCEPT OF OPERATIONS

A. DETECT

1. Procedures, processes, and systems in place for monitoring and detecting threats and anomalies.

2. Description of how continuous threat monitoring and detection is maintained.

3. Processes in place for evaluating effectiveness of monitoring, detection, and protective measures.

B. RESPOND

1. Threat Notification:

   a) Upon detection of an event or threat, describes the process for preliminary alert messaging which communicates the existence of an

emergency situation and provides basic incident information necessary to initiate an effective response.

b) Where will initial notifications originate?

c) Who will receive initial notifications? Establishes initial point of contact for initial incident alerts by position or job title

d) What information is provided in the initial notification?

2. Situation Assessment:

a) Process of gathering initial incident information, establishing situational awareness, determining severity of impacts, assessing needs, and determining whether to activate the incident response operations.

b) Incident triage and analysis process to determine nature, complexity, and severity of incident.

c) Incident response priorities based on existing or anticipated impacts to normal operations. Examples:

(1) Protect human life and safety. Protection of human life always takes precedence over all other considerations.

(2) If applicable, protect classified data as regulated by government statutes and regulations.

(3) Protect sensitive data, including proprietary, financial, law enforcement, scientific, and managerial data.

(4) Prevent system damage (e.g., loss or alteration of system files, damage to hard drives).

(5) Minimize disruption of computing resources. In many cases, it is better to shut down a system or disconnect from a network than to risk damage to data or systems.

d) Thresholds and trigger points for escalating and mobilizing response activity if an incident becomes more critical.

e) Identify and describe the actions that will be taken to monitor the movement and future effects that may result from the emergency.

f) Describe how the initial assessment is disseminated/shared in order to make protective action decisions and establish response priorities.

3. Response Plan Activation

a) Establishes which individuals by position/job title who have the authority to activate the response plan and initiate response operations.

b) Describes response process flow.

c) Details decision-making process for plan activation and initiation of coordinated response activity.

d) Procedures for assembling, and deploying personnel, supplies, and equipment to support the response to an incident.

4. Alert and Warning

a) Processes for reporting threats, events, and anomalies to elected and appointed officials, community leadership, management, personnel, law enforcement, and external stakeholders.

b) Establishes minimum reporting information requirements. (i.e. date, time, name and title of reporting person, location, systems/applications affected, etc.)

c) Identify and describe the actions that will be taken to coordinate, manage, and disseminate notifications effectively to alert/dispatch response and support agencies.

d) Identify and describe the actions that will be taken to notify and coordinate with adjacent jurisdictions.

5. Response Operations

   a) Describes deployment and management of response tasks, personnel, and resources to ensure life safety, stabilize the incident, isolate threat, limit impact, and protect property.

   b) Details how command and control is established (i.e. Incident Command, EOC, etc.)

   c) Development of incident response goals and objectives (i.e. incident action plan)

6. Demobilization

   a) Organized deactivation and release from duty of emergency response resources and personnel.

   b) Describe process of developing demobilization plan.

   c) Identify the individual by role, position, or job title that has the authority to release personnel and resources from duty.

   d) Outline decision-making process for determining when demobilization will take place

   e) Establish criteria for releasing personnel and resources.

7. Incident Close Out and Response Deactivation

   a) Identify processes for collection of required documentation.

   b) Identify processes to manage the accounting of supplies, equipment, and other materials.

   c) Describe formal transition process/change of command from response to recovery operations.

   d) Notification process to internal and external stakeholders of formal end to response operations, transition to recovery operations, and /or return to normal activity.

C. RECOVER

1. Describe process of preserving and restoring critical applications, systems and services in order to resume normal operations.

2. Disaster Recovery

    a) Identify individuals by position/job title that would have operational authority over recovery activity, if different from response phase.

    b) Establish process for implementing the organization's information technology (IT) disaster recovery plan.

3. Business Continuity

    a) Discuss implementation of existing plans to ensure continuity of critical government services and business activity, and expedite resumption of normal operations.

4. System/Application Restoration

    a) Describe procedures to restore systems to the original state and validate the system has been cleared of any detected threats.

    b) Describe how affected and restored systems are tested and validated before being brought back online.

5. After Action Review (AAR) and Improvement Planning

    a) Detail process used by the jurisdiction to review and discuss the response in order to identify strengths and weaknesses in the emergency management and response program.

    b) Describe how the jurisdiction ensures that the deficiencies and recommendations identified in the AAR are corrected/completed.

III. ASSIGNMENT OF RESPONSIBILITIES

A. General list of tasks to be performed, by position and/or department, without the procedural details included in standard operating procedures.

B. Organizational charts can also be inserted here (i.e. Incident Command, Emergency Operations Center, Security Operations Center, Crisis Management Team, etc.)

IV. DIRECTION, CONTROL, AND COORDINATION

A. Identifies the individuals by position/job title that have operational and management authority over response operations.

B. Outlines how response activity and resource management is coordinated internally as well as with external stakeholders, vendors, agencies, and organizations.

V. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION

A. Identifies the type of information needed, the source of the information, who uses the information, how the information is shared, the format for providing the information, and any specific times the information is needed.

VI. COMMUNICATIONS

A. Describes the communication protocols and coordination procedures used between response organizations during emergencies and disasters.

VII. ADMINISTRATION, FINANCE, AND LOGISTICS

A. Outlines general support requirements and the availability of services and support for incident response, as well as general policies for managing resources.

B. Describes pre-incident, operational, and post-incident documentation requirements

C. Existing contracts and contracting requirements for material resources, staffing, and vendor-managed services.

D. Purchasing and procurement requirements.

E. Cost tracking and funding requirements.

F. Inventory, supply, and resource tracking.

G. Processes for addressing legal issues and regulatory requirements.

VIII. PLAN DEVELOPMENT AND MAINTENANCE

A. Discusses the overall approach to planning and the assignment of plan development and maintenance responsibilities.

B. Assigns responsibility for the overall planning and coordination to a specific individual by job title within the organization.

C. Establishes process and schedule for plan development, review, training, exercise, evaluation, and improvement.

IX. POLICIES, AUTHORITIES, AND REFERENCES

A. Lists of laws, statutes, ordinances, executive orders, regulations, and formal agreements relevant to emergencies.

B. Specifies the extent and limits of the emergency authorities granted to the senior official, including the conditions under which these authorities become effective and when they would be terminated

C. Identifies state, national, international, and professional standards that apply to the plan.

D. Establishes any pre-delegation of emergency authorities that may not be described in other planning documents.