**Incident response is a process, not an isolated event.** In order to be successful, organizations must take a coordinated and organized approach to any incident. There are several important phases that every response plan should cover in order to effectively address the range of security incidents that could occur.

This Incident Response Plan Template covers the basics of Incident Response. You can reorder the Phases listed here, rename headings and modify table contents to meet your specific needs.

You can find more details on incident response here:

[**NIST Cybersecurity**](https://www.nist.gov/topics/cybersecurity) **|** [**NIST Cybersecurity Framework**](https://www.nist.gov/cyberframework)

[**Default Security Policies and Standards for Commonwealth Employees**](https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards)

## **Phase 1. Preparation**

Have on hand:

* Up-to-date inventory of data and systems
  + Refer to **[Four Steps to prepare for a Cybersecurity Risk Assessment](https://www.macomptroller.org/wp-content/uploads/four-steps-to-prepare-for-a-cybersecurity-risk-assessment.pdf)**
* Your third party cyber partner’s contact information
* Malware, anti-virus, network update plan
* A list of response team members and backups

And, know ahead of time if you are going to pay a ransom.

## **Phase 2. Detection**

What is it? How? Response?

|  |  |  |
| --- | --- | --- |
| **Incident Type** | **Incident Threat** | **Response Playbook #\*** |
| Unauthorized network/email access | Phishing or targeted |  |
| Virus | Advanced persistent threat (Emotet, Ryuk) |  |
| Ransomware | Hacking/unauthorized third-party access to system |  |
| Denial of Service (type) | Malicious/Non-Malicious |  |
| Employee payment | Insider or outsider threat |  |
| Vendor payment | Insider or outsider threat |  |
| Data breach | Insider or outsider threat |  |
| Unsuccessful access attempt | Worthy to note why |  |

**\* Different incidents require different responses and possibly different personnel – see Phase 5**

## **Phase 3. Initial Assessment**

Incident Suspected or Confirmed?

Was the incident contained?

|  |  |
| --- | --- |
| **Rating** | **Description** |
| Low | Unsuccessful breach attempt |
| Medium | No evidence of impact on network; agency network scan is needed |
| High | Potential impact on enterprise systems and/or loss of Commonwealth funds or data |
| Critical | Confirmed data breach or ransomware/malware infection |

## **Phase 4. Protection, Mitigation and Recovery**

Select Incident Response Team – based on Incident Type and Playbook (**Phase 2**).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Team Role** | **Name** | **Contact\*** | **Alternate** | **Contact\*** |
| Incident Manager |  |  |  |  |
| Technology |  |  |  |  |
| Security |  |  |  |  |
| Business Team reps  Accounting, Payroll, Procurement, etc. |  |  |  |  |
| Legal Counsel |  |  |  |  |
| Scribe |  |  |  |  |
| Communication |  |  |  |  |

**\*Use mobile phones for texting in case phone/email systems are down. Texts should be preserved for post-incident documentation and review. Personal phones may be subject to EOTSS policies.**

* **Protection**

Do other systems, applications, servers, etc. need to be shut down?

Who has access to the impacted systems, applications or servers? Is changing passwords enough or should access be deactivated?

* **Mitigation**

Different playbooks for Incident Categories – these are your detailed steps to contain, protect, eradicate and recover.

Enable your Continuity of Operations Plan if necessary.

* **Recovery**

Full system scan usually required; restore from data backups.

## **Phase 5. Communication/Notification**

Who needs to know?

|  |  |  |  |
| --- | --- | --- | --- |
| **Interested Party** | **Contact** | **When Contacted** | **By Whom** |
| Senior staff |  |  |  |
| IT staff only |  |  |  |
| All employees |  |  |  |
| Business owners (A/P, Payroll, Procurement) |  |  |  |
| Comptroller |  |  |  |
| Customers/clients |  |  |  |
| Cyber Legal Counsel (internal/external) |  |  |  |
| Office of the State Treasurer |  |  |  |
| Third Party cyber partner |  |  |  |
| Local law enforcement/FBI |  |  |  |
| State Auditor |  |  |  |
| Attorney General/Consumer Affairs |  |  |  |

## **Phase 6. Reporting by Scribe**

1. Agency detailed report of the incident that includes all phases - dates, facts or circumstances of the incident, steps taken to date, all parties involved, along with additional steps necessary for remediation and recovery.

Also for Consideration:

* 1. Executive Summary
  2. Appendices and location of back up files
  3. Lessons learned
     1. What worked
     2. What needs to be added to the plan to improve cyber readiness

## **Phase 7. Follow Up**

Once you have a written plan, use tabletop exercises to test the various scenarios you have identified.

Other Resources:

* [5 Key Criteria for Creating an Incident Response Plan Practical for Your Organization](https://digitalguardian.com/blog/5-key-criteria-creating-incident-response-plan-practical-your-organization)
* [Incident Response Team Roles Responsibilities](https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities)
* [Using Existing Tools Facilitate Incident Response](https://digitalguardian.com/blog/using-existing-tools-facilitate-incident-response)