****Text, logo

Description automatically generated

# Incident Response Plan

**Responding Effectively to Cyber Issues**

**Establishing cyber readiness practices and policies helps to reduce risk, but it’s important to assume that our company is likely to have to deal with a security incident at some point that could impact business operations. Trying to determine how to respond during an incident is not a good idea. Response time is critical to minimize the damage. Having a clear plan in place can be the difference between an incident and a catastrophe.**

### Overview

A comprehensive, step-by-step Incident Response Plan equips us to quickly respond, resolve, and learn from every incident. This Incident Response Plan serves as a roadmap for what to do when responding to a security incident, to ensure we have a strategic response rather than a reactive one.

**There are three main elements to our incident response:**

1. **Prepare** for a possible future incident
2. **Respond** during the incident
3. **Recover** from the incident

### 

### How to Prepare

**Organizational Guidelines:**

As with so many things, a little preparation goes a long way. There are a few response essentials that should be done as soon as possible to properly prepare for and reduce the damage of an attack.

1. **Back up data and make sure you can re-install from the backups.** Recovering from an attack will go a lot faster and impact operations much less if you have current back ups of your system software, applications and especially your important data. You also want to make sure that each person in your organization has back ups if you do not do this centrally. It is important to regularly test your backups.

* Date completed: [DATE]

1. **Make sure everyone knows how to report a possible incident.** Early detection is really important. Every team member should know how to spot suspicious activity and who to contact about it.

* Designated Internal Incident Contact: [CONTACT DETAILS]
* Date completed: [DATE]

1. **Find good technical external incident response support.** Know who to go to and how to contact them in an emergency. A fire that’s beyond your ability to control means calling the fire department. You need to know who to call if a cyber incident is beyond your ability to control. At the very minimum, this should be an IT support expert you know and trust. Depending on the size and nature of your business, identifying additional communications and legal support is wise.

* Designated External Incident Contact: [CONTACT DETAILS]
* Date completed: [DATE]

**How to Respond**

Something crazy is happening on an employee’s computer and they don’t know what to do. This is the equivalent of smelling smoke or seeing a small flame in the coffee room.

**Here’s what you do:**

1. **Isolate the problem** – immediately get the device off the network
2. **Identify the type of incident** and take the following action:

* Malware - get the device off the network immediately
* Credential theft – disable, but do not delete the account, and reset the password
* Data breach – call IT Emergency Contact
* Ransomware – get the device off the network immediately
* Denial of Service – contact your manager/IT/Internet Service Provider

1. **Determine the scope** of the incident by asking these questions:

* When did the incident occur?
* Who is affected?
* What is the technical nature of the incident? How did it occur?
* Who knows about the incident?
* Is it still ongoing?

1. **Determine if it can be properly controlled internally** or if you need to call external IT support to ensure the breach is handled appropriately.
2. **Keep checking for the problem to return.** If it’s unclear whether the issue has been resolved, err on the side of caution and reach out to an expert about the issue.

**How to Recover**

The crisis is over and now it’s time to get things back to normal. The scope of the incident and the severity of the impact will determine how much time and effort will be needed to recover. However, the basic steps are the same.

**Here’s what you do.**

1. Notify all affected parties
2. Re-set the user ID and password of the compromised device
3. Patch all devices
4. Reinstall software and data from back-ups as needed

**Incident Response Checklist**

This checklist is to help the IT manager or Cyber Leader

Prepare

1. Back-up daily

* Automatic Backup Setup/Confirmed: [DATE]

1. Test back-ups every three months

* Date last completed: [DATE]

1. IRP Protocol Communicate to workforce

* Date last completed: [DATE]

IT emergency contact is: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Internet Service Provider is: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Legal emergency contact is: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Communications emergency contact is: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Respond**

1. Isolate the problem – get the device off the network
2. Identify the type of incident

* Credential theft
* Ransomware
* Malware
* Denial of Service
* Loss of confidential data

1. Determine the scope of the incident
   * Who is impacted?
   * When did it start?

* Is it still happening?

**Recover**

1. Notify all parties
2. Re-set the user ID and password of the compromised device
3. Patch all of the devices
4. Reinstall software and data from back-ups as needed

### Additional Guidance for Incident Response This guidance is to help the IT manager or Cyber Leader

If you’d like to have an even more robust Incident Response Plan for your organization, below is a four-step approach to do so based on guidance from the National Institute of Standards and Technology (NIST). It may not be completely feasible for you to follow each step but do your best to act on each of the four steps in ways that make sense to you and your organization.

**Preparation**  
  
Preparation is the key to rapid response.   
In this step, you compile a list of all your assets - what makes your company run. This list will include but is not limited to servers, networks, applications, and critical endpoints (like laptops). After you’ve compiled your asset list, rank them by the level of importance. Then monitor their traffic patterns so you can create baselines to be used for comparisons later - or hire a vendor to monitor their traffic patterns if your resources allow. If you cannot afford a vendor, a list of assets and prioritized attention toward your assets is a good first step. Create a communications plan, with guidance on who to contact, how, and when based on each incident type. Don’t forget to connect with everyone on this list before a crisis occurs. A common refrain in crisis management is “You should never be exchanging business cards during a crisis.” Make sure everyone on your list knows what you are expecting from them during a crisis.

Determine which security events, and at what thresholds, would trigger your incident response plan. To help you identify thresholds, think about what will disrupt your business operations.

After identifying those thresholds, create an incident response plan for each type of incident. It can be improved through tabletop exercises, during which you identify holes in your process, but it will also be improved after actual events (more on that later). The point is, get a process in place.

**3**

**Containment, Eradication,   
& Recovery**   
  
**Containment** aims to stop the bleeding. Here is where you patch the threat’s entry point.  
  
**Eradication** aims to remove the threat. If the threat gained entry from one system and proliferated into other systems, you’ll have more work on your hands here.  
  
**Recovery** aims to get the system operational if it went down or simply back to business as usual if it didn’t.

**1**

**Lessons Learned**   
  
This step provides the opportunity to learn from your experience so you can better respond to future security events. Tempting as it may be to skip, especially with your never-ending to-do list, this step is strongly recommended.  
  
Take a look at the incident with a humble but critical eye to identify areas for improvement. Then add those improvements to your documentation.  
  
No process is perfect for every possible scenario. Some scenarios can’t even be fathomed until they’ve occurred. The threat landscape is also ever evolving so your incident response process will naturally need the occasional update. Remember, your future self will thank you. As the saying goes, “Don’t waste a good crisis.”

**Detection and Analysis**  
  
At this point in the process, a security incident has been identified. This is where you go into research mode. Gather everything you can on the incident. Then analyze the data. Determine the entry point   
and the breadth of the breach. This process is made substantially easier and faster if you’ve got all your security tools filtering into a single location. You may have hired a vendor that can perform these functions for you.

**4**

**2**