

[insert company name/logo here]  
Cyber Readiness Playbook

Policies and Procedures to Reduce our Cyber Risk



**CYBERREADINESSINSTITUTE.ORG**

# Introduction

This Playbook is a living document our organization updates to reflect changes in the data, software, and hardware we use to operate our business. It also gets updated when any of the following take place:

* A new Cyber Leader has been appointed
* Emergency contacts are changed
* Backups are completed
* Backups are tested
* Software updates are installed
* Training is completed

|  |  |
| --- | --- |
| **Fill in the dates below:** | |
| Date of Playbook completion: |  |
| Date of last update: |  |

|  |  |
| --- | --- |
| **If we chose to be CRI Certified Cyber Ready, CRI verified this Playbook met their requirement:** | |
| Date(s) of CRI verification call(s): |  |
| Date of CRI Certification: |  |

# Cyber Readiness Checklist

|  |
| --- |
| **Our organization completed the following activities on our journey to become cyber ready:** |

|  |  |
| --- | --- |
| Current Cyber Leader name: |  |
| Cyber Leader position in organization: |  |
| Appointed by (name and title): |  |
| Date appointed: |  |
| If applicable, former Cyber Leader(s) (name and start/end dates): |  |

|  |  |  |
| --- | --- | --- |
|  | **DATE COMPLETED** | **NOTES** |
| Baseline Metrics Recorded in the online Cyber Readiness Program |  |  |
| Core Four Policies Established |  |  |
| Prioritization Worksheet Complete |  |  |
| Incident Response Plan Complete |  |  |
| Software Update Management Tool Complete |  |  |
| Workforce training on Core 4 and Business Continuity Complete |  |  |
| Training Attestation Signed |  |  |
| Cyber Readiness Online Program Complete |  |  |
| Playbook Reviewed for Verification (if seeking certification) |  |  |

# Core Four Policies

Our organization adopted the following policies to become cyber ready and help prevent cyber-attacks. If we have additional cyber readiness policies, they are included on the following page(s).

|  |  |
| --- | --- |
|  | Passwords+ Multifactor Authentication  * Multifactor Authentication (MFA) must be enabled on all hardware and software that supports it. * Passwords should be at least 15 characters in length. If an application or device does not allow for 15 characters, passwords must be the maximum length allowed. * Passwords are not required to be changed periodically, however, if there is evidence of a cybersecurity breach, all passwords should be changed immediately. |
|  | Software Updates  * Develop a software update process using CRI’s Software Update Management Tool. |
|  | Phishing  * Phishing awareness communications are delivered to all employees monthly. * All employees are required to successfully complete phishing training on a quarterly basis to include at a minimum: awareness, examples, and response methods. * New employees are required to successfully complete phishing training as part of their onboarding process or within 30 days of their start date. |
|  | Secure File Storage and Sharing  * Prohibit the use of USBs and removable media devices except in predetermined business-critical cases. (See Tips, Tricks, and Guidance for examples) * Prioritize cloud storage for the transfer and storage of files on all applications where available. * Turn on auto-encryption for the transfer and storage of files on all applications where available. * All critical business data should be regularly backed up using secure and trusted removable media and/or secure and trusted cloud storage. |

# Additional Cyber Readiness Policies

Our additional cyber readiness policies are provided on these pages.

# Business Continuity Plan

Our Business Continuity Plan consists of the following:

 Prioritization Worksheet: On the following worksheet our organization lists the data, software, and hardware used to run our operations. Our management and Cyber Leader identified what is most important to protect us from data loss and to keep our organization running.

 Incident Response Plan: This document outlines what our organization does to prepare for a possible cyber incident, and what to do and who to contact in the event of a suspected or actual cyber incident.



Our organization relies on the following data, software, and hardware to operate. After the comprehensive lists, we prioritized what data is most important to protect and what software and hardware is most important to our business continuity.

# Comprehensive Data Listing

**THIS IS THE DATA WE NEED TO RUN OUR ORGANIZATION**



|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

# Comprehensive Software Listing

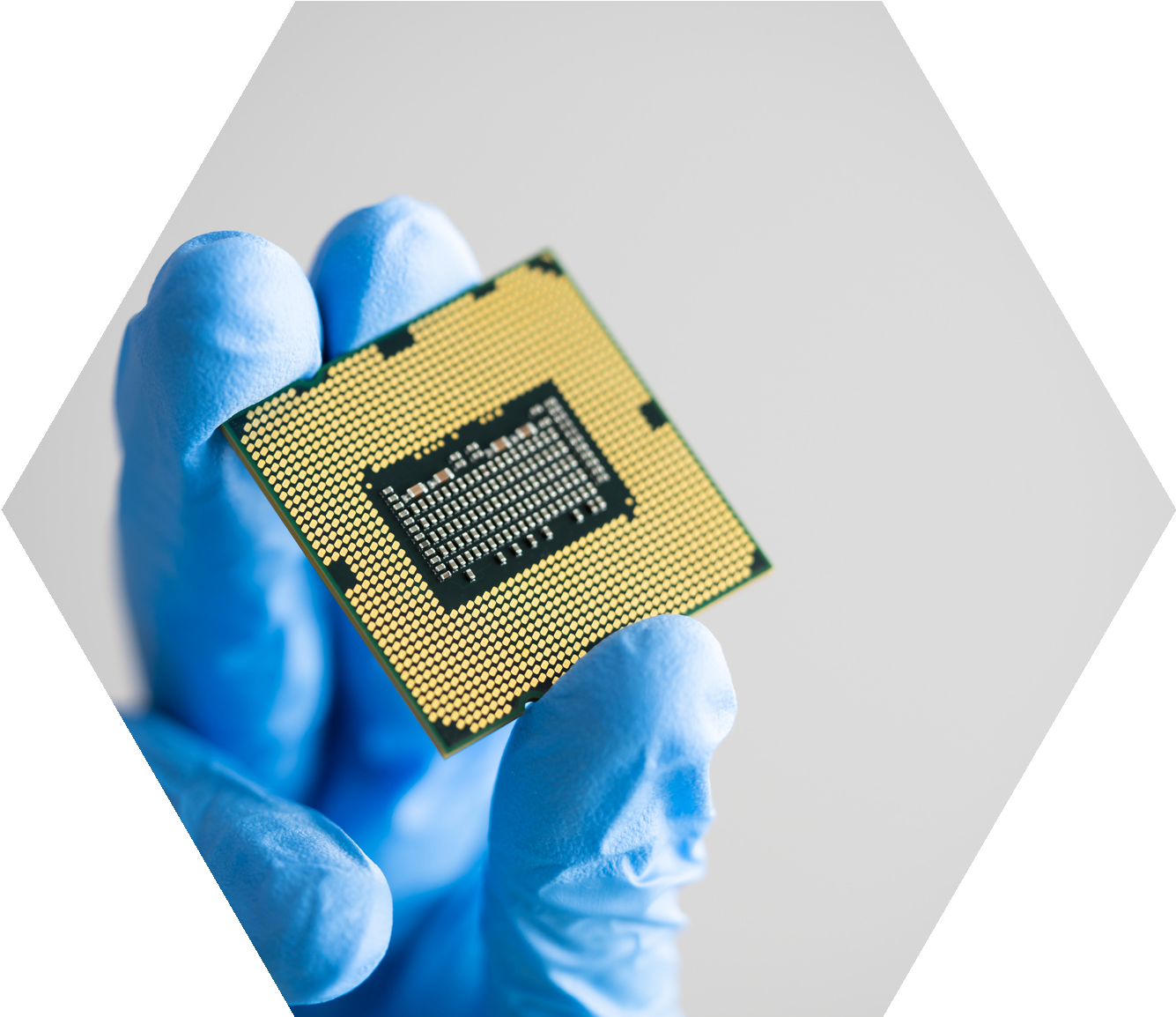
**THIS IS THE SOFTWARE WE USE TO RUN OUR ORGANIZATION**



|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

# Comprehensive Hardware Listing

**THIS IS THE HARDWARE WE USE TO RUN OUR ORGANIZATION**



|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

# Prioritization Worksheet

Our organization has met to review the Comprehensive Listings and identified the items below as the most important for us to protect.

**PRIORITY DATA**

THIS IS THE DATA THAT IS MOST IMPORTANT TO PROTECT BECAUSE IT WOULD CAUSE THE MOST DAMAGE TO OUR ORGANIZATION IF IT WAS LOST OR UNUSABLE.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**PRIORITY SOFTWARE**

THIS IS THE SOFTWARE THAT IS MOST IMPORTANT TO OUR DAILY OPERATIONS.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**PRIORITY HARDWARE**

THIS IS THE HARDWARE THAT IS MOST IMPORTANT TO OUR DAILY OPERATIONS.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

## Incident Response Plan (IRP)

Our organization took steps to prevent cyber-attacks by adopting the Core Four policies and training our workforce. However, everyone still needs to prepare for a cyber incident.

Our Incident Response Plan has three main elements:

|  |  |
| --- | --- |
|  | **Prepare for a possible future incident** |
|  | **Respond during the incident** |
|  | **Recover after the incident** |

# Prepare

EMERGENCY CONTACTS

These are the critical people to contact in case of an incident or a suspected incident. The first person to notify is our Cyber Leader. The Cyber Leader will contact the other Emergency Contacts. If for some reason you cannot reach the Cyber Leader, contact the IT Emergency Contact. In some incidents you may not be able to use email, so you will need to contact by phone.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ROLE** | **NAME** | **TITLE** | **ORGANIZATION** | **EMAIL** | **PHONE NUMBER** |
| Cyber Leader |  |  |  |  |  |
| IT Emergency Contact |  |  |  |  |  |
| Internet Service Provider |  |  |  |  |  |
| Legal Emergency Contact |  |  |  |  |  |
| Communications Emergency Contact |  |  |  |  |  |
| Law Enforcement Agency (cyber-crime agency, police, etc.) |  |  |  |  |  |

# Data Backups

Our organization routinely conducts backups of our data and systems to minimize the disruption to our operations and protect our assets. We also test the backups on a set schedule. This is the record of when our backup was done, who performed it, and where the backup is located.

|  |  |  |  |
| --- | --- | --- | --- |
| **BACKUP DATE** | **RESPONSIBLE PERSON OR PARTY** | **BACKUP LOCATION** | **NOTES** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Respond

If you suspect that your computer, tablet or smartphone is infected, or if you clicked on an email or attachment that caused your computer to behave strangely, immediately do the following:

|  |  |
| --- | --- |
|  | **Shutdown or turn off your computer, tablet or smartphone** |
|  | **Disconnect from the network**  Wi-Fi will disconnect when you shut down the device. If you are physically connected to the network with a cable, unplug the cable. |
|  | **Call your Cyber Leader** |

The Cyber Leader will notify everyone in the organization and contact the Emergency Contacts.

# Recover

Our Cyber Leader is responsible for managing the recovery process. They will coordinate with the appropriate people to restore system operations as quickly as possible. Here are the steps we will take:

1. Notify all affected parties, including relevant suppliers and customers
2. Reset the User ID and Password of the compromised device
3. Patch all the devices
4. Reinstall software and data from backups as needed
5. Below are additional recovery steps in our Incident Response Plan:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

# Software Update Management Tool

This table lists the software we use in our organization. The list is aligned with the software listed in the Prioritization Worksheet. Our Cyber Leader is responsible for keeping this tool current.

**Our policy is to turn auto-update on for all software that has this capability.**

This applies to any company-issued devices (desktop computers, laptops, tablets, smartphones), any personal devices used to access our organization’s systems, and any software used to operate machinery and equipment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SOFTWARE** | **WHO IS RESPONSIBLE FOR UPDATING THE SOFTWARE** | **WHO USES THE SOFTWARE** | **PRIORITY** | **AUTO-UPDATE ENABLED** | **DATE LAST UPDATE COMPLETED** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

SEE THE PLAYBOOK GUIDE FOR INSTRUCTIONS AND TIPS ON USING THIS TOOL

# Training Policy

* Our organization will provide training to all employees and contractors on an annual basis to assist in understanding and complying with the Core Four policies and Incident Response Plan in this Playbook.
* Training will be conducted on an annual basis.
* All new personnel will be trained within 30 days of joining our workforce.
* Training materials will be updated by the Cyber Leader or the person appointed by the Cyber Leader as needed to inform the workforce of any changes to policies and the Incident Response Plan.
* Employees and contractors must participate in and complete the required training.
* Our Cyber Leader, or a person designated by them, is responsible for managing the cyber readiness training program and will keep training attendance records.

# Cyber Readiness Training Attestation

The Cyber Readiness Institute (CRI) requires organizations to ensure that all employees and contractors are trained in order to be CRI Certified Cyber Ready. The training must specifically cover policies that meet or exceed CRI’s requirements in the areas of Passwords + Multifactor Authentication, Software Updates, Phishing, Secure Sharing and Storage, and Incident Response.

This Attestation must be signed by the Cyber Leader and the senior executive or manager of the organization and provided to your CRI Cyber Coach as part of the verification process.

By signing and returning this Attestation Form, we affirm our commitment to training all employees and contractors in CRI’s Policies and their role in our Incident Response plan and confirm to the best of our knowledge and reasonable assurance that this training has been completed across our organization.

|  |  |
| --- | --- |
| Company Name: |  |
| Number of Employees Trained: |  |
| Number of Contractors Trained: |  |

|  |  |
| --- | --- |
| Print name & title of Senior Executive |  |
| Signature |  |
| Date Signed |  |

|  |  |
| --- | --- |
| Print name of Cyber Leader |  |
| Signature |  |
| Date Signed |  |