

\*replace with your company logo

# CYBER SECURITY

**INCIDENT RESPONSE**

# POLICY

## Purpose

The purpose of this policy is to provide general guidance for the actions that we take in the event of a Cyber Security Incident being reported. It is general guidance, and is not intended to be specific to any particular system, but is intended to provide a structure and process to the steps that our team take.

## Scope

This plan is applicable to, and will be communicated to, all \*COMPANY NAME HERE\* users, with particular focus on those who provide IT support and first line response to our users.

## Plan

This plan is made up of two sets of actions, those which should happen immediately, and those which can be considered secondary. The order for the immediate actions should be followed and completed as soon as possible. The secondary actions are discretionary, based on the output of the immediate actions but each must be considered. Any incident must be reviewed by senior management before it is closed.

## *Immediate Actions*

1. Reset the user’s password.
2. If applicable, forcibly log out any existing sessions, for example on a Remote Desktop or Citrix Server, Mobile Devices or Laptops.
3. Check Sign-In Logs for the user in questions for suspicious activity, particularly failed logins, or logins from IP Addresses not native to the customer.
4. Escalate and share with the Cyber Security Incident Response Group at

\*COMPANY NAME HERE\*, so that senior team members are aware of a potential incident.

## *Secondary Actions*

Review sign-in logs for all users to check for suspicious activity. Review firewall logs for any suspicious activity.

Check the user’s mailbox for Suspicious Email Forwarding, Rules and Sweep Rules – remove/disable any suspicious logs.

Inspect Sent Items for any suspicious email that may have been sent.

If the attack was a phishing email or similar, block the email address in question, and check the logs to see if any other users received the email.

Send a warning to all users, of the attack that has happened and what sort of email they need to watch out for.

Run a full Anti-Malware scan on the user’s system or Remote Desktop. Block all suspicious IP Addresses.

## Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Note |
| 1.0 | 12/01/2021 | \*Your Name\* |  |
|  |  |  |  |

## 