**Cyber Security Incident Containment**

**Last Update Status:** *Updated October 2022*

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to* [*policy-resources@sans.org*](mailto:policy-resources@sans.org)*.*

# Incident Name:

## Isolate affected systems:

## Command Decision Team approved isolation from network? YES NO

If YES: date, time, method, and systems isolated:

If NO, reason:

# Backup or forensic image of affected systems:

## System backup or forensic image successful for all systems? YES NO

Method and name of persons who obtained backup or forensic image:

Date and time backup / forensic image started:

Date and time backup / forensic image complete:

Backup / forensic image turned over to:

Signature: Date:

Backup / forensic image Storage Location:

Incident Containment Form by: Date and Time of Form:

Title: Signature: