SANS

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.*

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:________

CONSENSUS POLICY RESOURCE COMMUNITY