

INCIDENT RESPONSE WORKFLOW



NON-TECHNICAL

PREPARE

What is the issue?

What system is affected?

DETECT/ACTIONS

What did I do (step-by-step actions)?

Any error messages or notable errors?

Is there a demand for any payment?



Leave machine on but unplug the network cable from the back



If a suspicious email is identified, keep hold of it

Inform Internal IT Support

IT Support to refer to 'Monitor Detection Channels' on technical guide

Take a photo