

Incident Response Guide Make and Take Workshop



Introduction and Preparation

Introduction:

Incident Response Planning is an important part of successful security planning. Incident Response Plans establish and test clear measures that your school district will practice and follow to reduce the impact of a security breach. An Incident Response Plan is a concrete plan, with identified roles and responsibilities, lines of communication and established procedures of response.

Having an Incident Response Plan and using it during Tabletop or Sandtable exercises to proactively practice in your district are important elements identified throughout the NIST framework. School districts may also have local Board policy identifying the need for incident response plans, disaster recovery, or business continuity planning.

Preparation:

In order to leave the Incident Response Guide, Make and Take Workshop with a completed Incident Response Guide, you should bring the following information.

1. Your school district or organization Incident Response Team members names, roles, and contact information.
2. Your school district or organization's Vendor list and contact information
3. Your school district or organization's Board policies that pertain to incident response, data classification, data encryption, securing sensitive data, incident response reporting, or business continuity.
4. **Links to your school district or organization's incident preparation lists:
 1. Inventory of System Interconnections (data flows)
 2. Data Sharing Agreement Inventory
 3. Hardware Inventory, including asset specifics and owner (assigned to) information for mobile, endpoint, server, and virtual devices.
 4. Software Inventory
 5. System Inventory, including system and business owner and contact information; operating, database, and application software; and physical and network location.
 6. Network Topology, including subnet information for endpoint, server, wireless and voice networks.
 7. Vendor Managed System Inventory, including system, vendor and business owner and contact information; operating, database, and application software; physical and network location; and contact information for the vendor security team.
5. Your school district or organization's incident analysis resources
6. Your District level Incident Response Team members names, roles, and contact information
7. Your school district or organization's key contacts

You can make a copy of the [BEFORE Incident Response Guide Planning](#) spreadsheet to help you gather your information.

***If you do not bring the listed items, you can gather them after the workshop to complete your district Incident Response Guide. You will not leave with a completed document, but rather with a template that you will still need to complete later.**

****Do not let the collection of #4 information put an end to your preparation for the Make and Take Workshop! You can work on collecting this information over time and enlist the help of others. Incident Response is a team sport. Not having all this information does not prohibit you from getting your plan in place.**