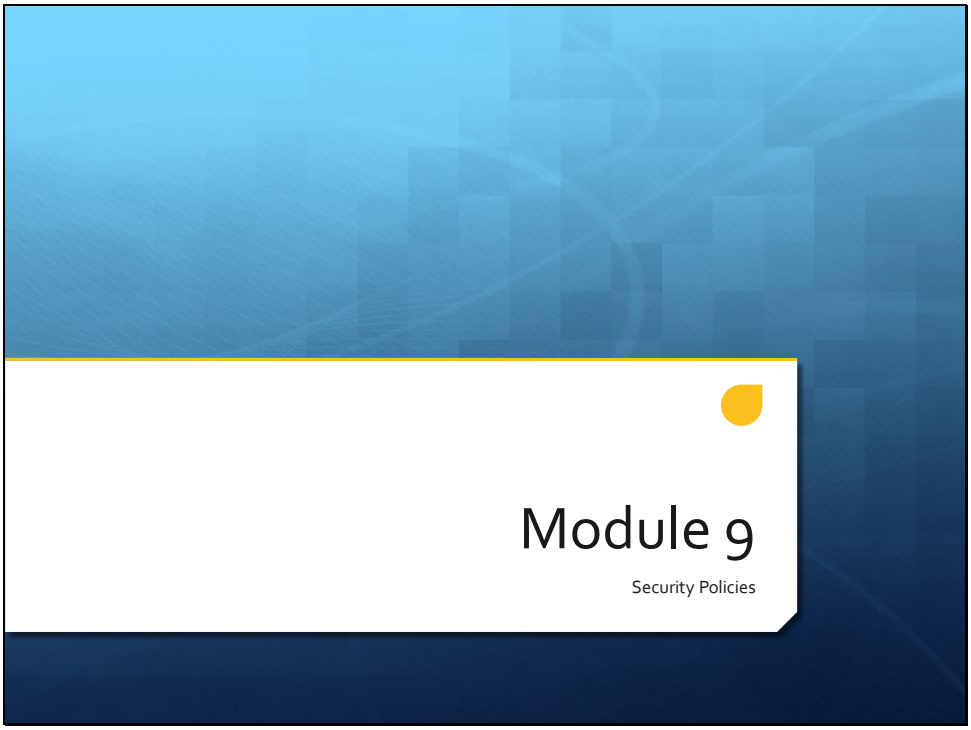
Security Awareness

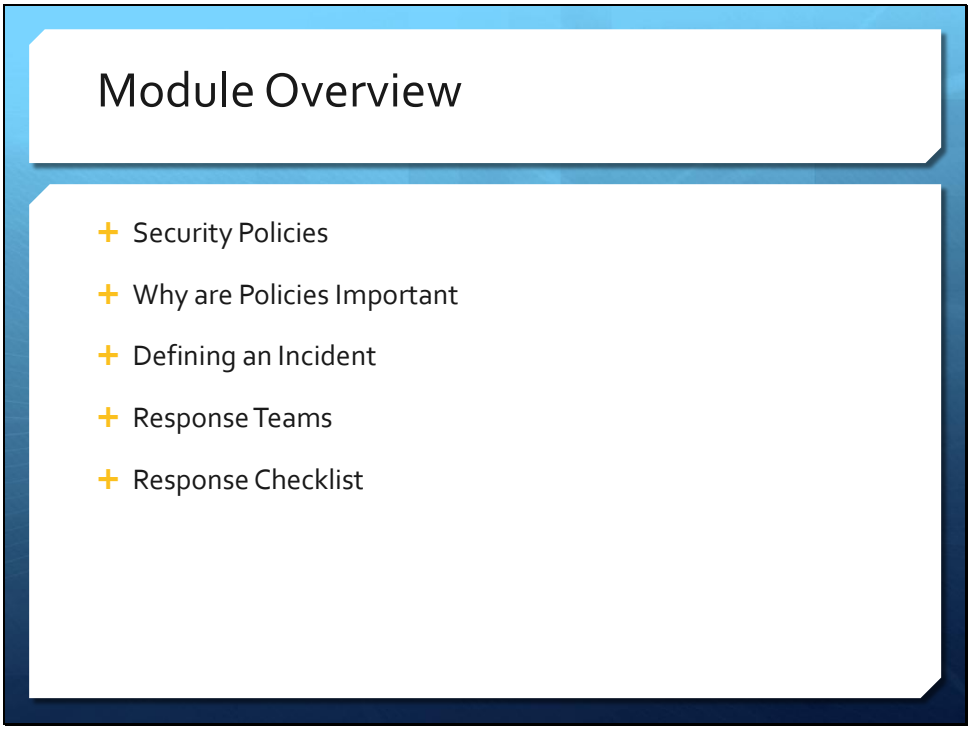
Module 09 – Security Policies

WORKBOOK

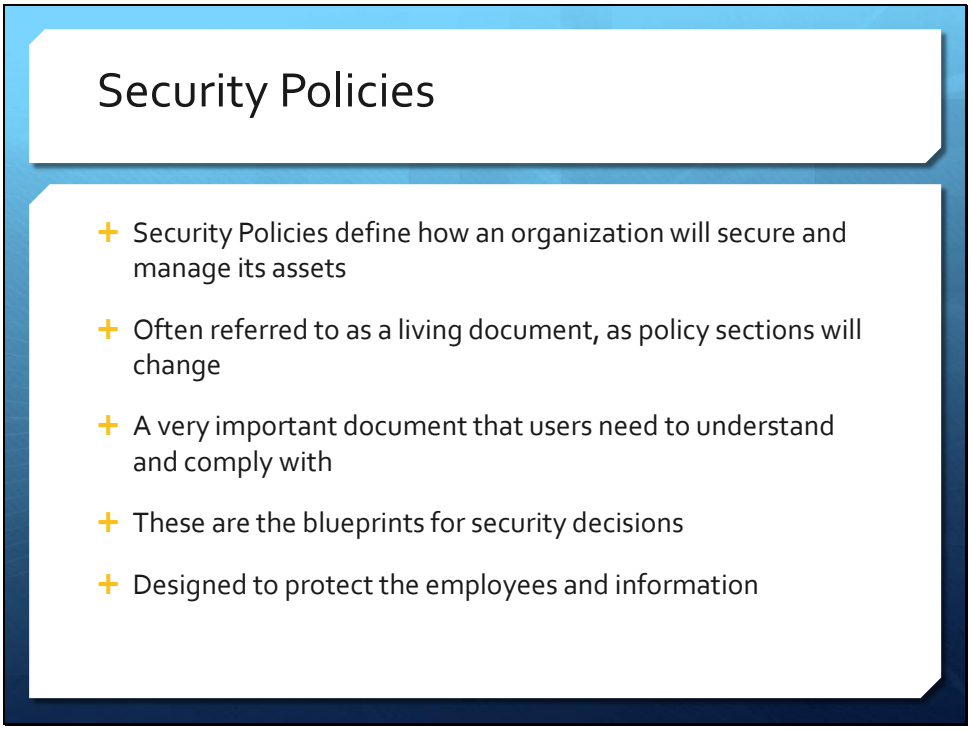
Slide 1



Slide 2


Module Overview
Security Policies
Why are Policies Important
Defining an Incident
Response Teams
Response Checklist

Slide 3


Security Policies
Security Policies define how an organization will secure and manage its assets
Often referred to as a living document, as policy sections will change
A very important document that users need to understand and comply with
These are the blueprints for security decisions
Designed to protect the employees and information

Slide 4

Security Policies (Cont.)

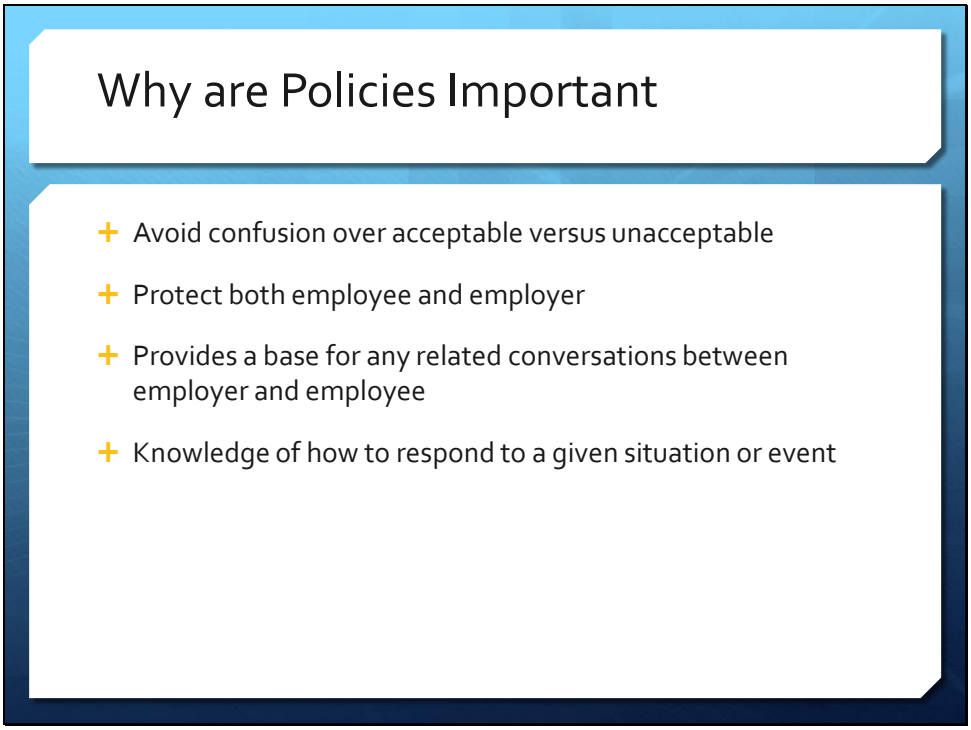
- Generally not very technical
- Considered the basis for Standard Operation Procedures (SOP)
  - User Account Statements
  - Internet Access Statements
  - Email Use Statements
  - Equipment Acceptable Use
  - Expectation of Privacy

Slide 5

Security Policies (Cont.)

- Remember these are blue prints:
  - Like building a house, it is not very technical
  - They are the plans around which real security is built
- Examples may include:
  - Users may not install software without written authorization
  - Users are required to protect their user account
  - Users may not share their user account
  - Users may not create multiple user accounts

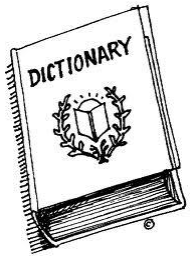
Slide 6


Why are Policies Important
Avoid confusion over acceptable versus unacceptable
Protect both employee and employer
Provides a base for any related conversations between employer and employee
Knowledge of how to respond to a given situation or event

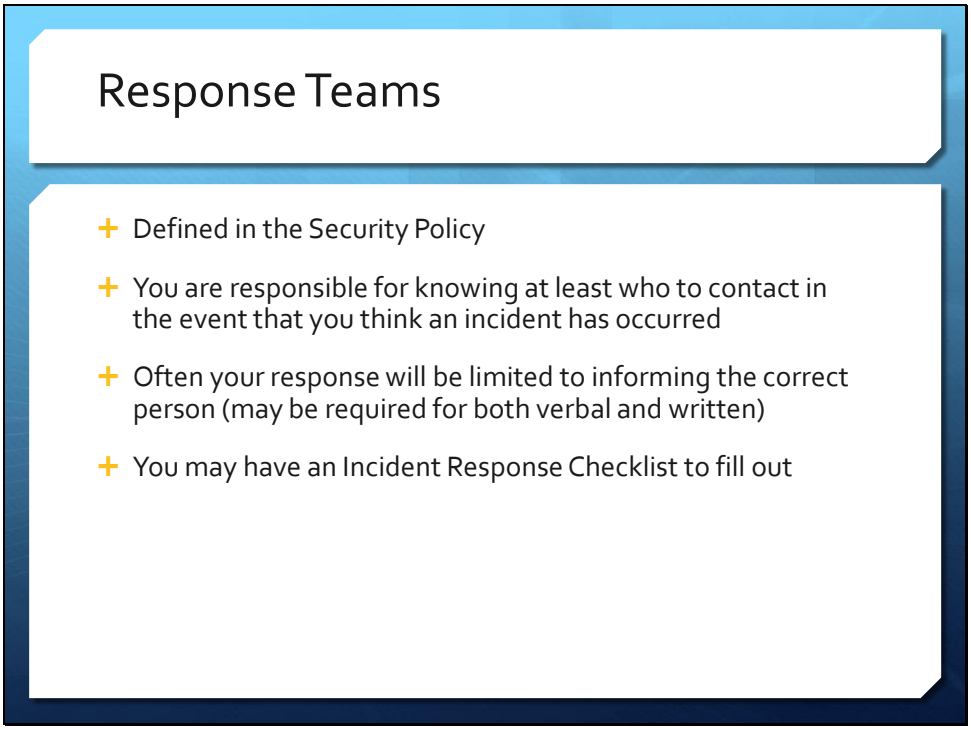
Slide 7

Defining an Incident

- Your computer is infected by a virus
- You cannot connect to the Internet
- Your files are disappearing
- Your computer will not start or shut down
- Your computer screen is covered in pop-up ads
- You lost your laptop
- You lost backup data



Slide 8

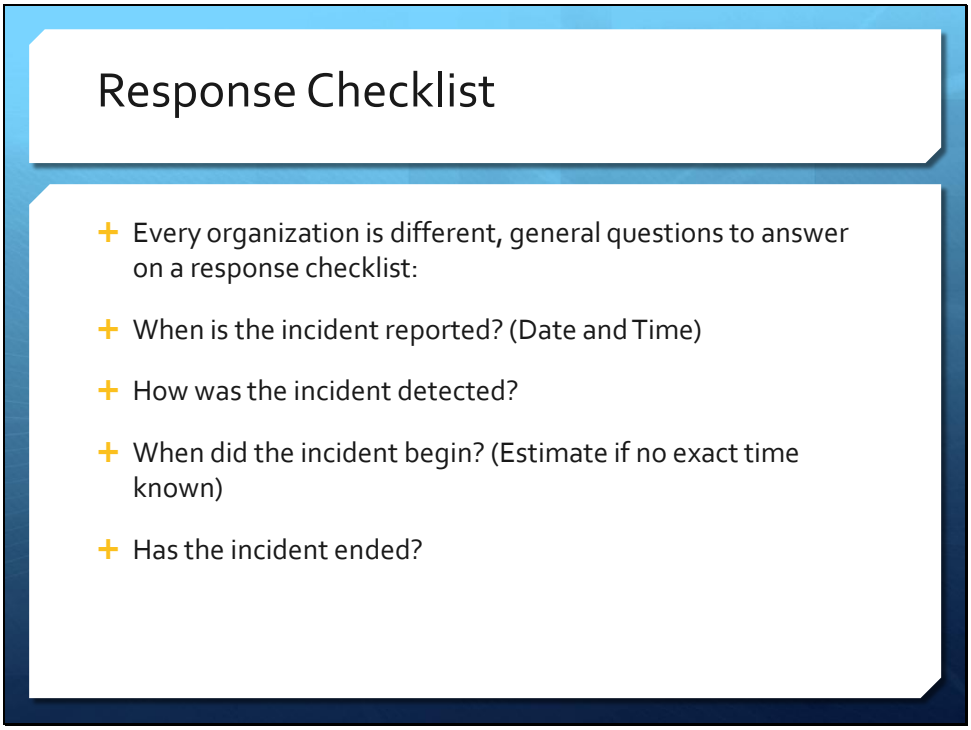

Response Teams
Defined in the Security Policy
You are responsible for knowing at least who to contact in the event that you think an incident has occurred
Often your response will be limited to informing the correct person (may be required for both verbal and written)
You may have an Incident Response Checklist to fill out

Slide 9

Response Teams (Cont.)

- A team should include:
  - OS Expert
  - Security Expert
  - Forensics Trained Expert
  - Legal Counsel
  - Decision Maker

Slide 10


Response Checklist
Every organization is different, general questions to answer on a response checklist:
When is the incident reported? (Date and Time)
How was the incident detected?
When did the incident begin? (Estimate if no exact time known)
Has the incident ended?

Slide 11

Response Checklist (Cont.)

- What type of incident is being reported?
- Has the incident affected critical resources?
- Have any backups been compromised?
- Does the affected system have network connectivity?

Questions and Answers

Review Questions:

1. How should an organization set up the guidelines for how to secure its data and other assets?
    A. Memorandums
    B. Word of mouth
    C. Blueprints
    D. Security policies

2. True or False: Security policies rarely ever have to be changed if created correctly.
    A. True
    B. False

3. A security policy should address which of the following areas of technology?
    A. Use of user accounts
    B. Use of Internet access
    C. Use of e-mail
    D. Use of equipment

4. True or False: A security policy needs to be supported from the highest levels of management.
    A. True
    B. False

5. You just discovered that your web server has been infected by a virus. What action should you take first?
    A. Shut down the server
    B. Contact the incident response team immediately
    C. Run the server's AV software
    D. Re-image the server

Answer Key:

1. D
   Security policies are designed to be the blueprint for outlining how an organization should enact security.

2. B
   False. We think of a security policy as a "living" document that will need to always go through a review process, especially as technology changes.

3. D
   All of the above should be addressed within the security policy.

4. A
   True. This is called the "top-down" approach, but in order for a policy to be effective (followed by members of the organization) there needs to be enforcement from the highest levels of management.

5. B
   Any incident should be immediately reported so that the response team can make decisions on how to proceed with containing the problem.