



**Episode What are Network Operations?** 

title:

Objective: **4.1 Explain common security concepts** 



- Security risks
- Business risks
- Documentation
- Nondisclosure agreement (NDA), memorandum of understanding (MOU), bring your own device (BYOD), statement of work (SOW)
- Change management

- Disaster planning
- Forensics
- Incident response
- High availability



- Network operations is a broad term that describes the actions needed to be taken to protect the network and organization
- Two main risks are security and business
- High availability ensures that your network doesn't go down



Episode Security Policies

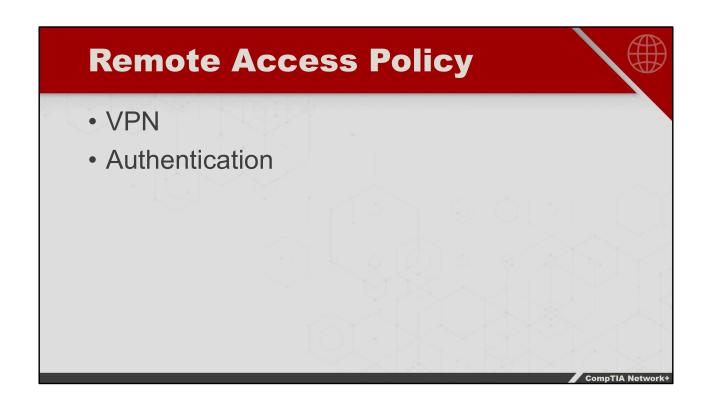
title:

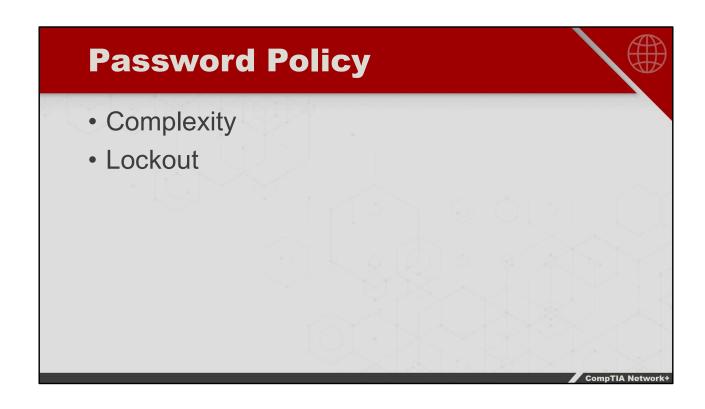
Objective: 3.2 Explain the purpose of organizational

documents and policies

# **Acceptable Use Policy**

- Define ownership
- Web site access
- Access time





## **IT Safety Policy**

- Lifting equipment
- Equipment handling
- Spills
- Procedures



## **International Export Control**

- Military information
- Nuclear information
- License keys





- Security policies document to users how to access system resources and what is allowable and acceptable
- Safety policies apply to the IT department too!
- NDAs, software licensing, and data restrictions need to be considered to protect an organization



**Episode Change Management** 

title:

Objective: 3.2 Explain the purpose of organizational

documents and policies



- Change management... here we go!
- Change management team... action figures!
- Some are even human
- Strategic change vs. infrastructure change
- Documentation is the last step in change management process



- The change management team handles infrastructure-level changes
- The change process includes requests, types of changes, configuration procedures, rollback and more
- The end game is documentation of all the changes made



**Episode** Patching and Updating

title:

Objective: 4.3 Given a scenario, apply network hardening

techniques

- Patching
- Operating system updates
- Driver updates
- Firmware updates
- Research
- Test
- Configuration backups



- Operating system updates are the most common type of update
- Firmware updates are necessary, but they depend on the device
- Before patching, be sure to research, test, and configure backups



**Episode Security Risk Management** 

title:

Objective: 4.1 Explain common security concepts

- Asset
- Threat assessment
- External threats
- Internal threats
- Natural events
- Natural disasters
- Vulnerability assessment
- Penetration (pen) testing

- Posture assessment
- Business risk assessment
- Vendor assessment
- Process assessment



- A vulnerability assessment can point out potential weaknesses in your organization
- Pen testing is used to examine the strength of your network security
- A risk posture is an overall look at security in the organization



Episode **Points of Failure** 

title:

Objective:

3.3 Explain high availability and disaster recovery concepts and summarize which is the

best solution

- Critical assets
- High availability (HA)
- Virtual IP
- Redundancy
- Fault tolerance
- Clustering
- Load balancing



- A single point of failure is one system that, if it fails, will bring down an entire process, workflow, or the whole organization
- Critical assets are the systems needed to maintain production
- Critical nodes are the devices needed to maintain the network
- The key to maintaining production on the network is to avoid a single point of failure



**Episode Standard Business Documentation** 

title:

Objective: 3.2 Explain the purpose of organizational

documents and policies

- Service Level Agreement (SLA)
- Memorandum of Understanding (MOU)
- Multi-Source Agreement (MSA)
- Statement of Work (SOW)

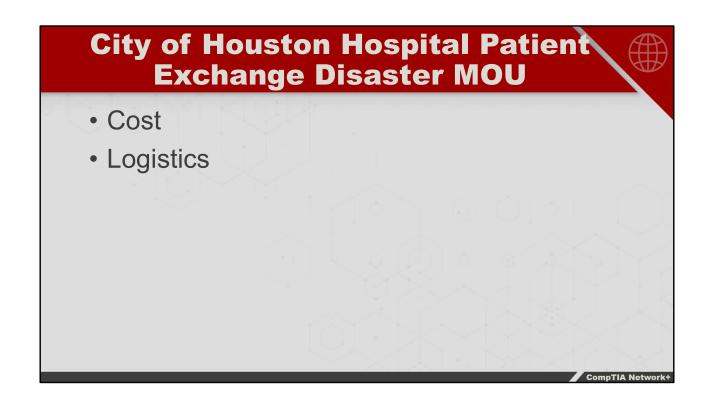
## Service Level Agreement (SLA)

- Between a customer and service provider
- Scope, quality, and terms of service to be provided
  - Definition of service provided
  - Equipment
  - Technical support

#### **Memorandum of Understanding (MOU)**



- Defines an agreement between two parties
- Used where a legally binding contract is inappropriate
  - Definition of agreed duties
  - Time frame
  - . ?????????



## **Statement of Work (SOW)**

- Legal contract between two parties (vendor and customer)
  - Defines services to be performed/supplied
  - Defines time frame/deliverables
  - Defines milestones/defines progress



- Standard business documentation is common in networking
- Standards on the exam include SLA, MOU, MSA, and SOW
- These are real-world standards



**Episode Incident Response and Forensics** 

title:

Objective: **4.1 Explain common security concepts** 

- Forensics
- First responder
- Secure the area
- · Document the scene
- Collect evidence
- Chain of custody
- Forensics report
- Legal hold
- Electronic discovery (e-discovery)



- The first responder is the person who must report an incident as soon as it happens
- If the first responder faces a serious threat, they must escalate it to the proper people
- The four-step process of forensics is secure the area, document the scene, collect evidence, and interface with authorities (submit forensics report)



# Episode 18.09

**Episode Disaster Recovery and Backups** 

title:

Objective: 3.3 Explain high availability and disaster

recovery concepts and summarize which is the

best solution

- Backup plan assessment
- Recovery point objective (RPO)
- Recovery time objective (RTO)
- Configuration data
- State data
- Mean time to repair (MTTR)
- Mean time to failure (MTTF)
- Mean time between failures (MTBF)

- Snapshots
- Local backups
- Offsite backups
- Cloud backups



- A single point of failure is one system that, if it fails, will bring down an entire process, workflow, or the whole organization
- Critical assets are the systems needed to maintain production
- Critical nodes are the devices needed to maintain the network
- The key to maintaining production on the network is to avoid a single point of failure



# Episode 18.10

Episode **Business Continuity** 

title:

3.2 Explain the purpose of organizational documents and policies Objective:

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution



- Business continuity plan (BCP)
- Disaster recovery
- Business continuity
- Distance and location
- Internet requirements
- Housing and entertainment

- Legal issues
- Annual exercises
- Failover
- Alternative processing sites
- Alternative business practices
- After action reports



- Contingency planning (business continuity planning) attempts to mitigate incidents to preserve business functionality
- Understand the pros and cons of the offsite options available: cold site, warm site, hot site, cloud site
- Thorough planning and practice is what makes recovery plans successful when disasters occur



# Episode 18.11

Episode **Deployment Models** 

title:

3.2 Explain the purpose of organizational documents and policies Objective:

5.5 Given a scenario, troubleshoot general networking issues



- Bring your own device (BYOD)
- BYOD policy
- Acceptable use policy (AUP)
- Onboarding policy
- Offboarding policy
- Mobile Device Manager (MDM)
- BYOD challenges



- Corporate-owned, business only (COBO)
- Corporate-owned, personally enabled (COPE)
- Choose your own device (CYOD)



- A bring your own device (BYOD) policy enables employees to use their own device on the network
- The Mobile Device Manager (MDM) can manage mobile devices brought by employees
- The organization should establish which data is controlled by the user and which is controlled by the organization