aci LEARNING
AUDIT-CYBER-IT

Module 4
Operational Procedures

 Updated: July 2023 CD Team

A+ 1102

Module 4
Operational Procedures

A+ 1102

Module 4 Learning Objectives

- Compare and contrast organizational documentation and procedures.
- Summarize change management best practices.
- Summarize and identify basic workstation backup and recovery techniques.
- Explain the significance of equipment and personal safety procedures.

A+ 1102

Module 4 Learning Objectives

- Identify and explain environmental variables and controls.
- Explain privacy and licensing concepts.
- Define incident response policies and procedures.
- Explain proper communication techniques and professionalism.

A+ 1102

Module 4 Learning Objectives

Identify the basics of scripting.

Compare and contrast remote access technologies.

A+ 1102

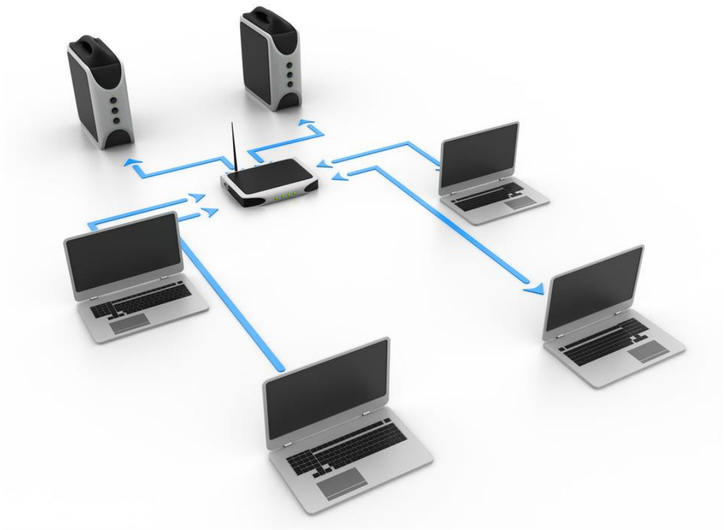
Table of Contents

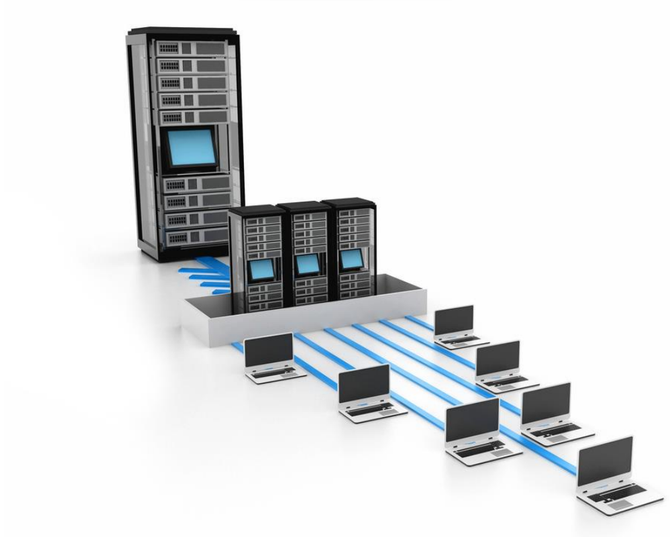
1. Documentation and Support Systems IS
2. Change Management
3. Backup and Recovery Methods
4. Common Safety Procedures
5. Environmental Factors
6. IR, Privacy, Policies, and Licensing
7. Proper Communication and Professionalism
8. Basics of Scripting
9. Remote Access Technologies

Topic: Documentation and Support Systems IS

In this section, we will cover:

- Network Topology
- Acceptable Use Policies
- Password Policies
- Compliance & SOPs
- Ticketing Systems

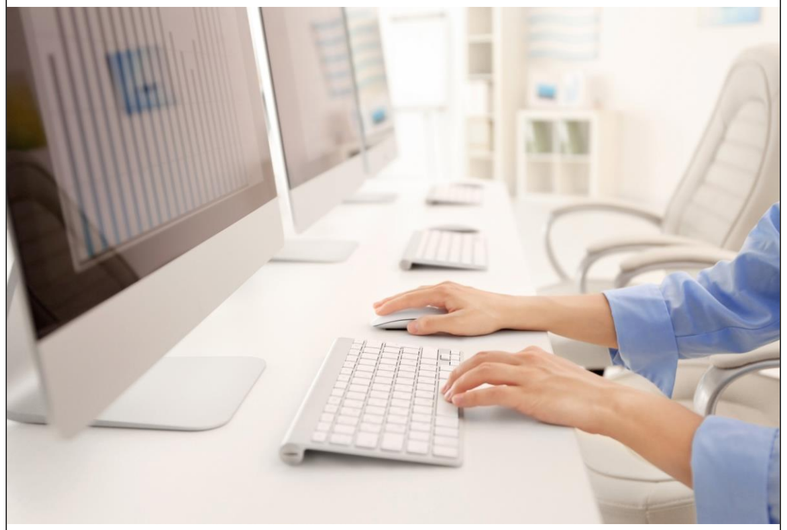




network topology

A network topology is a layout of a network structure; in essence, it is a blueprint of the network design and configurations.

A topology illustrates how devices are connected to the network. Topology examples include bus, star, mesh type setups or LAN, WAN, and CAN type setups.



acceptable use policies

Acceptable use policies are agreements users sign when using a company's devices and network.

Acceptable use policies help users understand how to access and use a company network. Some constraints may be placed on what users are allowed to do when using the network resources.

password policies

Password policies control how passwords are to be set up and maintained.

Some things to consider for password policies include password length, the use of special characters, and password lockouts on failed attempts.

compliance and SOPs

Regulatory compliance documentation is a set of documents specifying an organization's adherence to laws and regulations. You should also have Standard Operating Procedures (SOPs), which are written instructions for employees on how to perform routine tasks.

SOPs are created for actions, for example, the procedures for custom installation of software packages, new user setup checklists, and end-user termination checklists. These not only support the company's compliance but, more importantly, ensure that all employees are familiar with the correct procedures.

ticketing systems

Ticketing systems are key for organizing and documenting all incidents and any changes, including who and often why changes were made.

Some things to consider and track for ticketing systems include user and device information, description of problems, categories, severity, escalation levels (and process), clear/concise written communication of the problem description, progress notes, and problem resolution.

Topic: Change Management

In this section, we will cover:

- Risk Analysis
- Backup Plan
- Documenting Changes

risk analysis

A risk analysis is a way of addressing the negative impacts that malware and other security incidents may cause on the availability of the network.

A risk assessment matrix can be used to determine the impact of a particular attack on the network and the consequences that will derive from that attack.

Vulnerability assessments need to be done regularly, based on your network setup and the resources to determine and remediate potential vulnerabilities.

backup plan

A backup plan is a written plan to restore a system or network after a failure.

A backup plan is a contingency plan for how you will restore a system or network to operational status. They normally include a rollback plan, sandboxing for testing, and who the responsible employee.

Common types of backups include Full Backups, Incremental Backups, and Differential Backups. They can then be set up in a backup plan like the 3-2-1 Backup Rule and Grandfather, Father, and Son.

document changes

Document changes are a way to keep track of system or network changes and are core to basic change management best practices.

You want to ensure you keep up-to-date information for changes made to a system or network. A company should have request forms that gather the purpose and scope of the change, the date and time of the change, affected systems/impact, risk level, and end-user acceptance.

Topic:
Backup and Recovery Methods

In this section, we will cover:

- 3-2-1 Backup Rule
- Grandfather-Father-Son (GFS)
- Full Backup
- Differential Backup
- Incremental Backup
- Imaging
- Cloning
- On-site vs. Off-site backup
- Cloud Storage vs. Local Storage
- Account Recovery

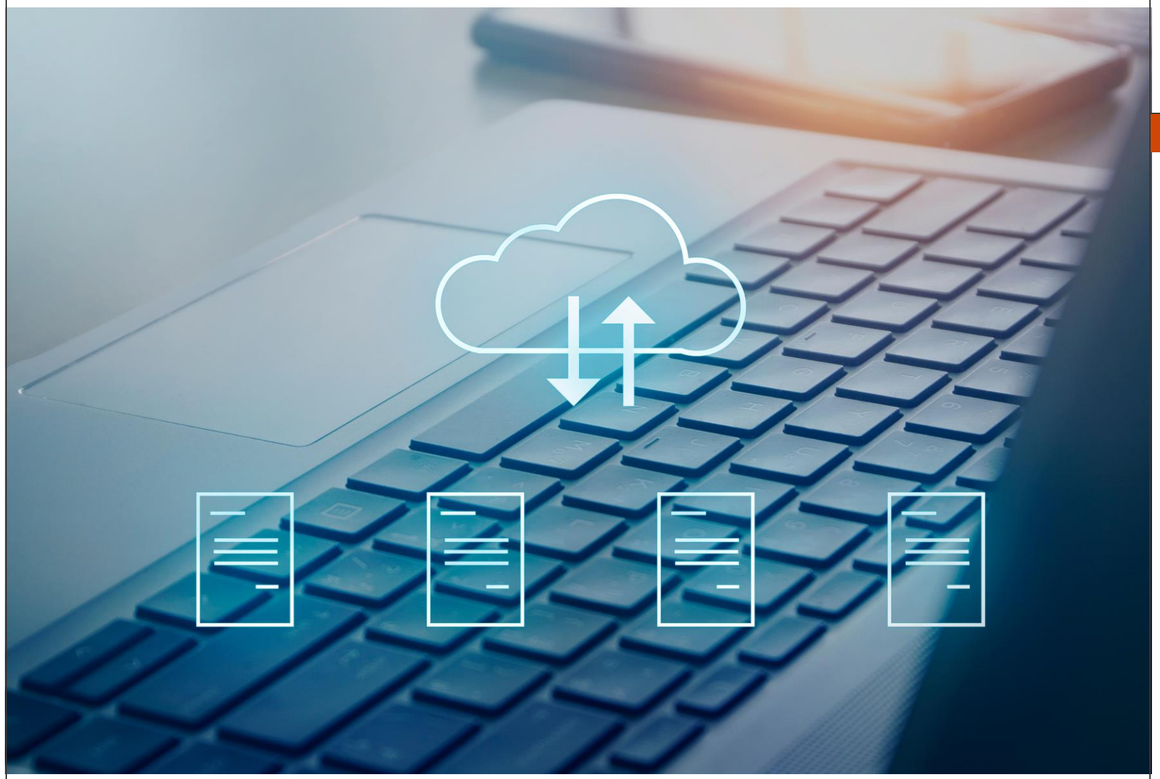
3-2-1 backup rule

The 3-2-1 rule is a good rule to follow. You should have: 3 copies of your data, store 2 copies of data on different media types and store at least 1 copy at an off-site location.

3 copies – Have one as a primary and two others.
2 different media types – You should back up the data to two different media types. For instance, tape drives and HDDs.
1 off-site location – This will help to aid in the instance of fire and other natural disasters.

While the cloud is off-site, you should also have a copy offline so that it is not connected in case of ransomware.

Grandfather – Father – Son (GFS)



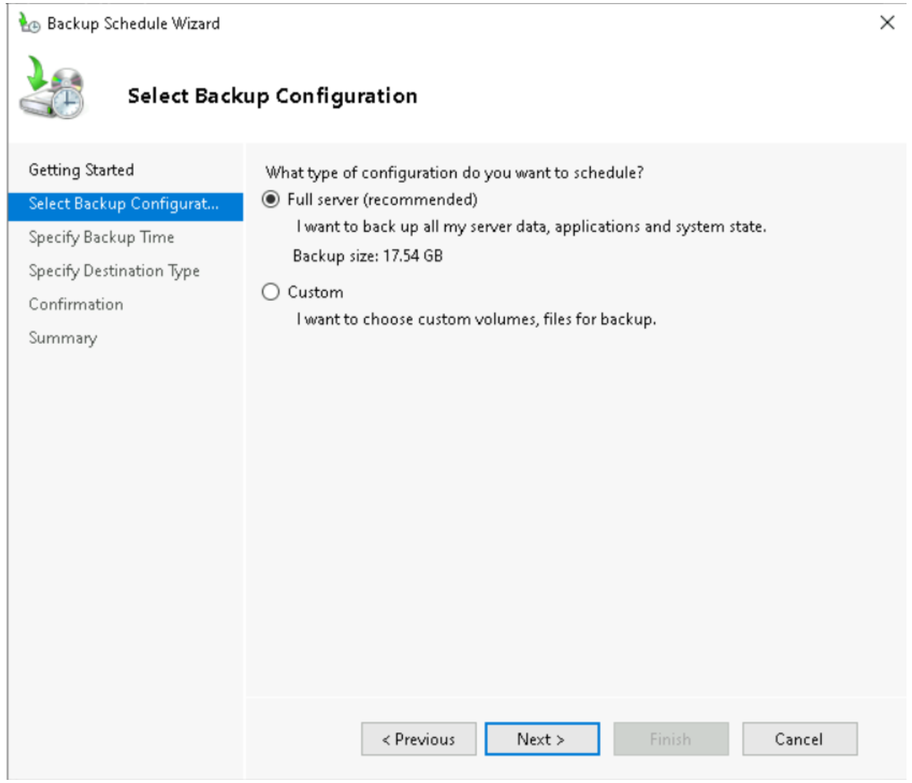
Grandfather is the 1 monthly full backup that is stored offsite in case of disaster.

Father is the 1 weekly full backup that is kept onsite for quick backup restoration.

Son is the daily incremental backup.

This backup method was created to maintain a comprehensive backup of the computer while using the least amount of storage space possible.

full backup

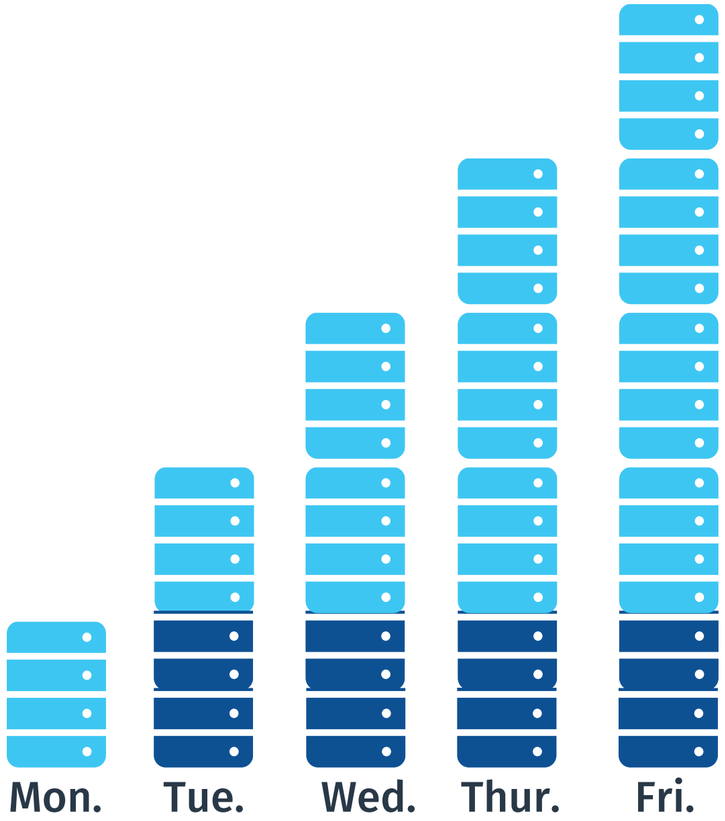


A full backup is a backup of all your targeted data. Full backups may be an entire volume, specific directories, or file groups/types. Backups are stored on a separate physical drive from the source location of the data.

Full backups are different from copies because it interacts with the archive bit in the file attributes. A full backup clears the archive bit (sets it to 0).

A full backup can be stored on an internal or externally attached storage drive, data storage servers, or using cloud storage.

differential backup



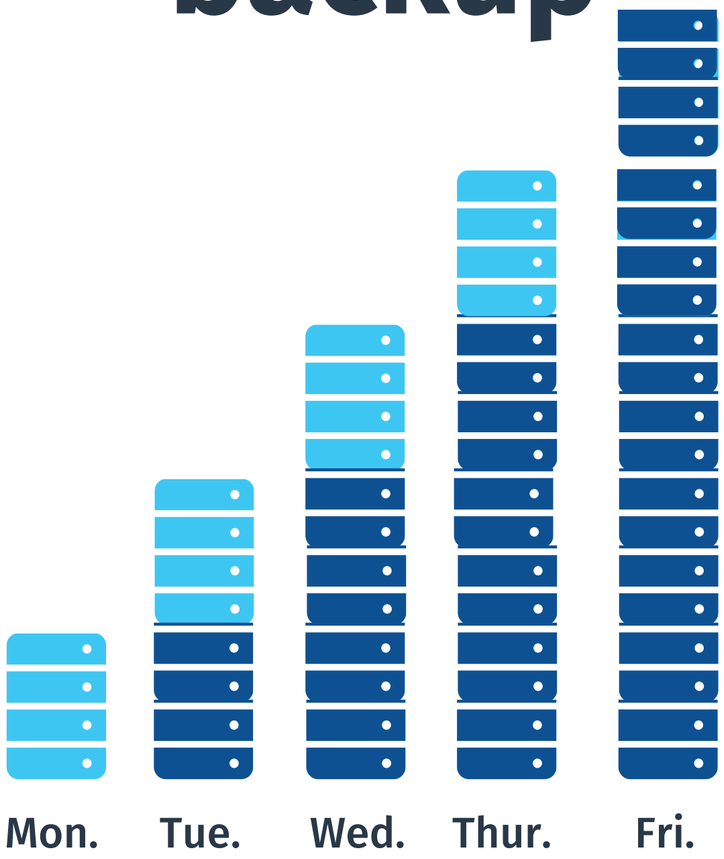
A differential backup is a backup of what has changed since the last full backup. A change is a modification of an existing file or the creation of a new file.

This type of partial backup **does not** clear the archive bit.

There are two types of partial backups that will be discussed, differential and incremental. The differential is used to simplify the partial backup process since only one file is used for each iteration of the process.

If a full backup is done weekly, a differential would likely be done daily. If a full backup is done daily, the differential would be done every few hours.

incremental backup



Full Backup on Fridays

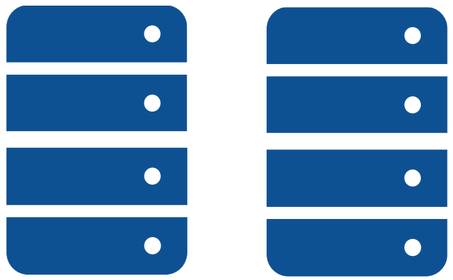
An incremental backup is a partial backup of what has occurred since the last backup, whether it was a full or previous incremental.

This type of partial backup **does** clear the archive bit.

Due to the clearing of the archive bit, only the data that has changed since the last backup will be captured. Less space will be used to store the data, and quicker backups will happen. However, recovery of the data will take longer due to using multiple backups to restore.

You perform incremental backups at the same frequency that a differential would be done. Partial backups are done with only one of the techniques, never both.

imaging

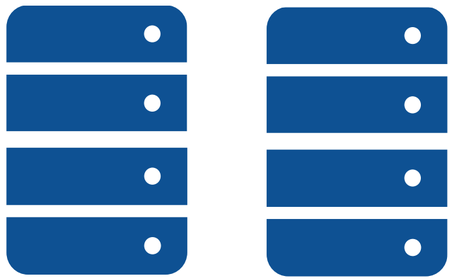


VM

Imaging backs up all of the data and the boot and partition data on the storage drive, where it is compressed and saved as an image file; this is commonly used for virtual machines.

Both imaging and cloning are done bit by bit. Images are stored in various file types based on the software used to create them. “.iso” is a very common file type used for general-purpose imaging.

cloning

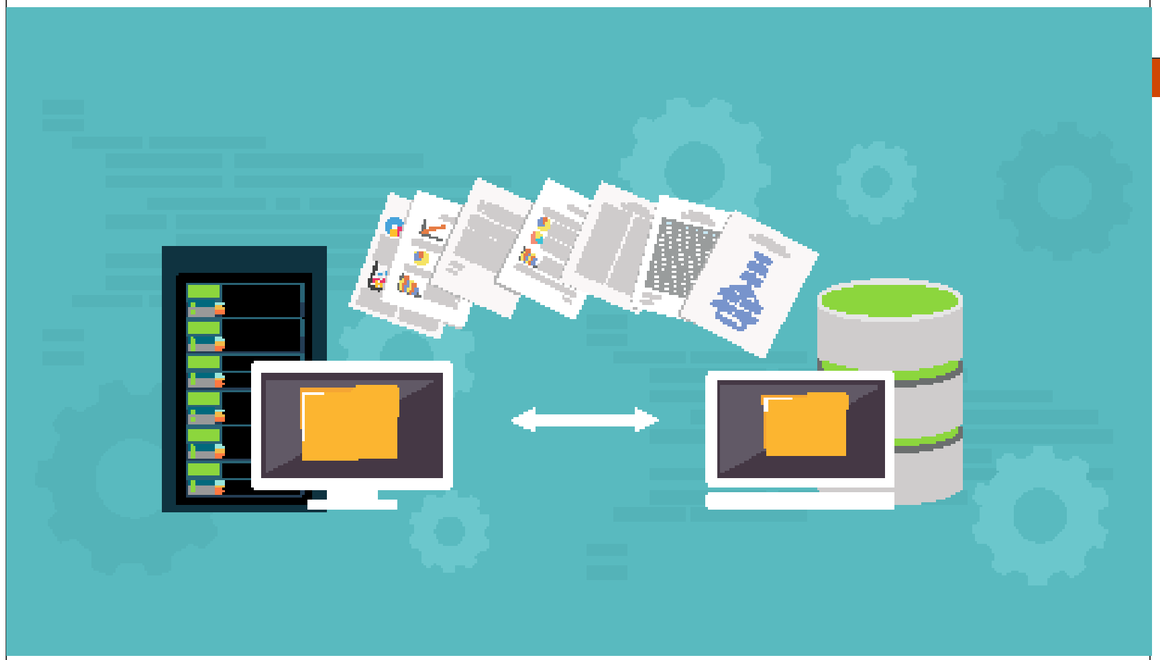


Clone

Cloning involves making an exact duplicate of the entire storage drive.

With cloning, you create a backup of the entire storage drive, so if your drive fails, you can swap out the failed drive for the cloned drive.

on-site vs. off-site backup



On-site is the term for items being stored or operated within the same physical structure where the live data resides. Off-site refers to a location physically separated from the live data; typically, this means off of the surrounding grounds as well as across town. Ideally, it would be regionally or geographically separated.

The benefit of off-site storage is that if there is a disaster like a flood or fire, then the backup that is “off-site” could be used and would be the only viable option. Some companies use cloud services for this, while others use physical storage devices that are taken to another secure facility.

cloud storage vs. local storage

When creating backups and storing data in general, there are several methods available — locally, internal drives, external drives, and tape drives are all common ways to store data.

Cloud storage gives the ability to store a copy of data in a data center that can be accessed via the internet anywhere in the world. This allows for fast recovery.

Cloud storage has the added benefit of increasing storage space beyond your system without the need to purchase additional physical storage.

account recovery

Account recovery is a way to gain access to an account if you are locked out of it.

Account recovery allows a way to get back into your account if you lock yourself out or if a hacker gains access to your account and changes the password.

There are third-party apps to help get you back into your account.

Topic: Common Safety Procedures

In this section, we will cover:

- Electrostatic Discharge (ESD) Strap
- Antistatic Bags
- Personal Safety

electrostatic discharge (ESD) strap

1

Electrostatic discharge (ESD) is like dragging your feet on the floor and touching a metal object. It merely annoys humans; however, the effects when this happens when touching electronics are detrimental.

2

An electrostatic discharge (ESD) wrist strap is a bracelet used to help prevent static electricity. An electrostatic discharge (ESD) wrist strap is used to safely ground yourself to a computer device to prevent the build-up of static electricity. ESD mats can also be used to minimize static electricity while working on sensitive components like memory.

antistatic bags

1

An antistatic bag is a special bag used to house electrical components when they're not in use.

2

When an item is placed inside an antistatic bag, make sure to close it to offer the most protection from static electric build-up.

personal safety

1

Personal safety can be achieved by using proper handling and grounding procedures, which include:

- Disconnecting the power before repairing a PC
- Using safe lifting techniques
- Knowing electrical fire safety measures
- Using safety goggles
- Using an air filtration mask when needed

2

Make sure you comply with all government regulations.

Topic: Environmental Factors

In this section, we will cover:

- Safety Data Sheet (SDS)
- Heating, Ventilation, and Air Conditioning (HVAC)
- Ventilation
- Temperature
- Humidity
- Brownout
- Power Surges
- Surge Protector
- Uninterruptable Power Supply (UPS)

safety data sheet (SDS)

An SDS, previously Material Safety Data Sheet (MSDS), is a document explaining the specific data needed to safely handle hazardous material.

Manufacturers must provide an SDS for products containing hazardous materials. It explains what to do in case of spills or emergencies.

This is important for the proper disposal of items, for example, batteries, toner, and other devices which may contain chemicals or materials.

heating, ventilation, and air conditioning (HVAC)

HVAC systems are used to control interior climate, such as temperature and humidity.

AC units are usually central units distributed throughout the building. In buildings with rooms or areas that need to be independently managed, a central unit may be distributed to zones rather than the whole building, or smaller area/room-sized units can be incorporated into that space.

ventilation

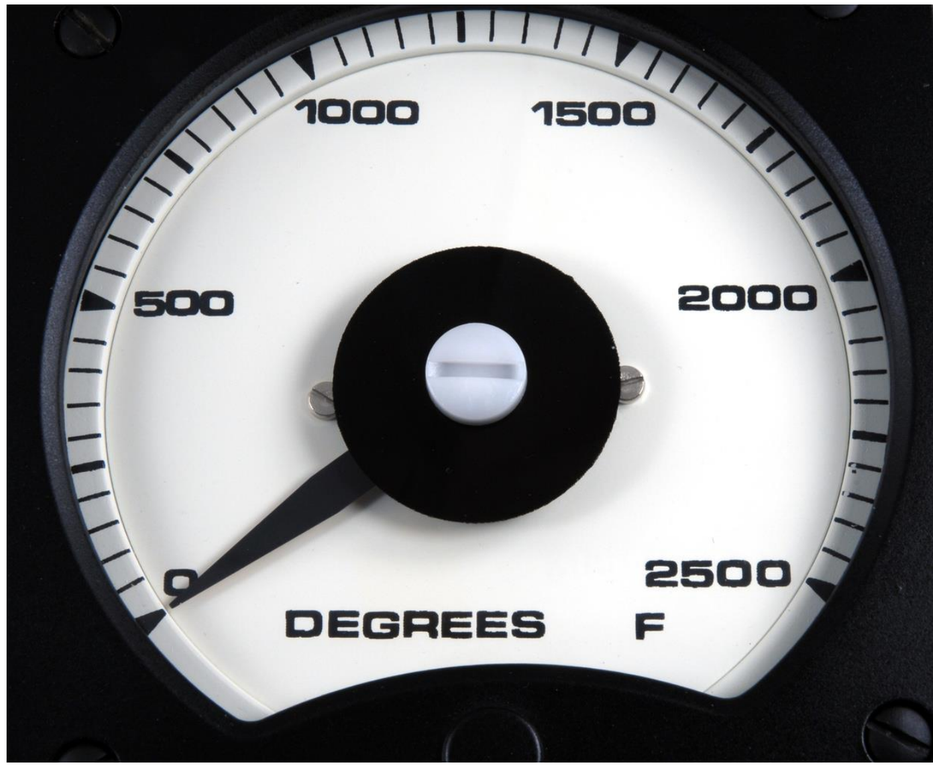
Ventilation is moving air from one area to another. Throughout a building, room, or inside a computer.

Ventilation is used to distribute cooled or heated air. It may be used to force air through a filtering process. Make sure that the intended capacity and path are not restricted.

temperature

Equipment needs to operate at a certain temperature. The recommended temperature range is between 68°F and 76 °F.

Equipment can generate heat, so you want to keep the equipment well-spaced and ensure that the equipment will not overheat.



humidity

Humidity is the amount of water vapor or moisture in the air.

When air cools, the water vapor condenses, becoming water droplets. When that happens within computer equipment, the water droplets can cause damage, short circuits, or other water-based damage to components. When the opposite happens, and there is not enough moisture in the air, these conditions produce electrostatic discharge (ESD).

The recommended range is between 45% and 55%

power surges

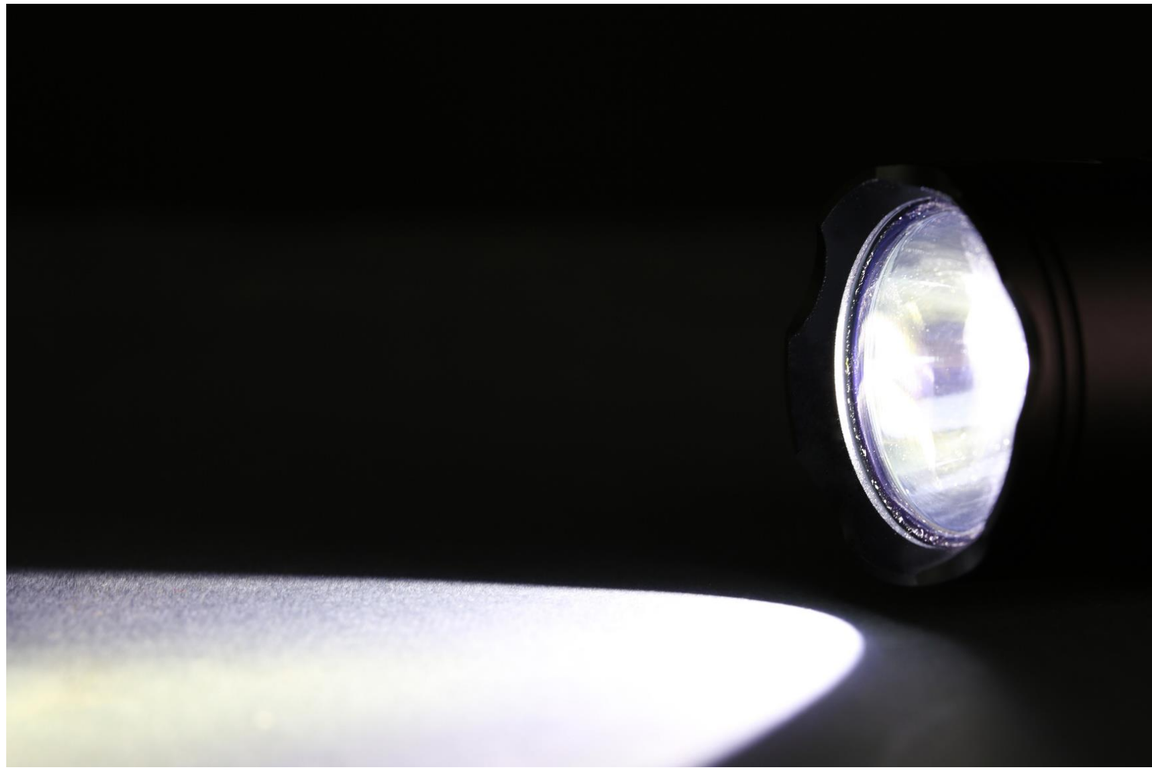
A power surge is when electricity flowing through an electrical cable produces more electricity than it should and causes a major electrical spike.

Power surges can damage equipment, so make sure that you use a surge protector for your electrical equipment.

brownout

A brownout is an intentional or unintentional drop in electricity.

When electricity utilization is close to or exceeds a certain standard, you will begin to experience fluctuations or outages.



surge protector

A surge protector or surge suppressor is a device frequently integrated into a power strip used to protect against surges and sudden, large increases in power.

Power surges can damage equipment, so make sure you use a surge protector for electrical equipment.

Surge protectors need to be monitored or tested. Some use a green and red light or steady and blinking light to indicate working versus not working properly, respectively.

uninterruptable power supply (UPS)

An uninterruptable power supply (UPS) is an enclosure with a battery and an inverter (change battery DC power to AC power), and many with outlets to perform as a backup power supply used if power is lost.

An uninterruptable power supply will take over in the event of a power outage but is limited to the time it can support the systems drawing power from it. Many last from 30 minutes to several hours. It is meant to give you time to shut down devices properly or get generators going.

Topic:
IR, Privacy, Policies, and Licensing

In this section, we will cover:

- Incident Response (IR)
- Personally Identifiable Information (PII)
- Privacy Issues and Solutions
- Payment Card Industry Data Security Standard (PCI-DSS)
- General Data Protection Regulation (GDPR)
- Licensing/Digital Rights
- Open-Source Software
- Proprietary (Closed-Source) Software
- Cloud License
- Personal License
- Enterprise License

Incident response (IR) is a critical component of security and best business practices to protect private and sensitive data.

Incident response is a core principle that includes a team of people trained to respond to an incident and ensure the proper chain of custody for evidence while ensuring data integrity and preservation and the proper documentation of any incidents. They are also tasked with informing management & law enforcement as necessary.

Your company should have an Incident Response Plan (IRP), and it should inform who should be contacted on the Incident Response Team should an incident occur.

incident response (IR)

Personally identifiable information (PII) is information that defines you as an individual.

Personally identifiable information (PII) can be a social security number (SSN), date of birth (DOB), phone number, or address.

This information can be used in identity theft, where a person impersonates you.

personally identifiable information (PII)

Privacy issues and solutions involve stopping your sensitive information from being stolen or compromised.

The goal of privacy solutions is to process and securely store personal information in your custody, including your business data and that of employees and clients.

Encryption is used to help secure data at rest and data in motion. Be sure to use the highest recommended standards. The Advanced Encryption Standard (AES) is today's Department of Defense-approved encryption standard and is used in many protocols and services.

privacy issues and solutions

Payment card industry data involves regulations for how debit or credit card transactions are secured, as well as storage of the data, how long it must be stored, and incident reporting.

Encryption must be used when dealing with debit or credit card transactions and data storage; this regulation ensures that a user's data will be protected and sets strict reporting measures.

Be mindful of things called skimmers, as your data can be stolen from legitimate transaction devices. Smart chips help reduce this risk.

payment card industry data

The security standard, called the Payment Card Industry – Data Security Standard (PCI-DSS), is the actual regulation for securing debit or credit card payments/transactions.

Security Standard (PCI-DSS) applies to all entities that accept, store, process or transmit a cardholder's information.

Businesses/companies who use/accept/process/store credit cards must be PCI-DSS-compliant.

security standard (PCI-DSS)

The General Data Protection Regulation (GDPR) is a new compliance standard in the European Union (EU).

The General Data Protection Regulation (GDPR) addresses how data collected and stored by an individual can be used by the company.

general data protection regulation (GDPR)

Licensing ensures that you have the right to use the software. This may or may not include a fee but will generally include an agreement (End User License Agreement or EULA) that outlines the restrictions and limits of use.

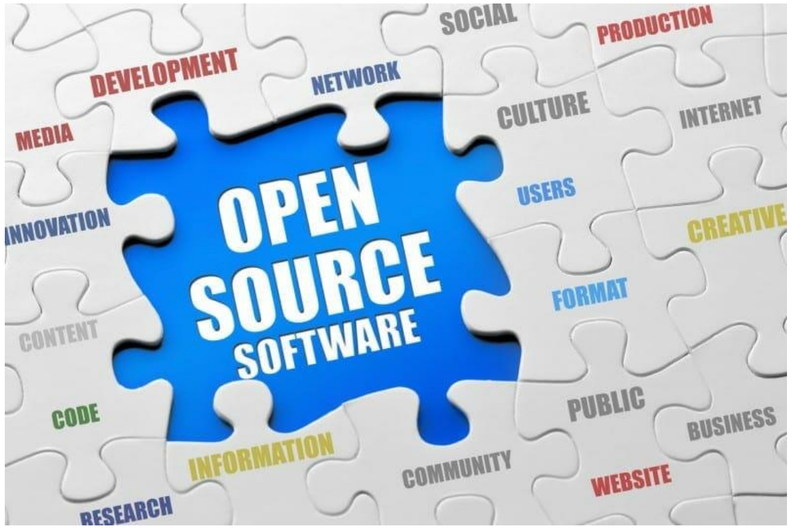
Digital Rights Management (DRM) refers to the protection of digital media, for example, software, music and videos being shared across computer networks.

Licensing and digital rights may apply to several things, for example, logos, pictures, videos, music, and written materials.

licensing/digital rights

Open-source software has its code accessible, normally without any fees. This allows users to modify the source code and create new customized versions of an operating system.

Creators of open-source software have made it accessible the source code and distribute it freely if you follow the basic rules/restrictions of use and attribution. Also called copyleft, a spin-off of copyright.



open-source software

Proprietary (closed-source) software, the code is not freely accessible by users.

Creators of proprietary software have made it so that the code used can't be shown freely.

You can get permission from the vendor to use or share a proprietary software's source code but be mindful to follow their rules when doing so.

proprietary (closed-source) software

A cloud license (OS, per VM, per CPU, per user) is issued to you from a cloud provider like AWS or Microsoft Azure.

A cloud license normally allows you to use cloud products for a certain premium or fee.

Renew a cloud license monthly or yearly as needed; a yearly license or longer can save you some money over time.

cloud license (OS, per VM, per CPU, per user)

A personal use license is issued to you by a company to use their product for personal use for a certain amount of time.

A personal use license allows you to use a company's products for a certain premium or fee unless there is a free version with reduced functionality or a time limit.

Personal use license can be renewed monthly or yearly as needed; a yearly license or longer may save you some money over time.

Personal use license

A corporate use license is issued to you by a company to use their product for business use for a certain amount of time.

A corporate use license allows you to use a company's products for a certain premium or fee.

A corporate use license can be renewed monthly or yearly as needed; a yearly license or longer may save you some money over time.

Corporate use license

Topic: Proper Communication and Professionalism

In this section, we will cover:

- Proper Communication (Basics)
- Proper Communication (Dealing with Difficult Situations)
- Professionalism

- Use proper language and avoid jargon, acronyms, and slang when applicable.
- Maintain a positive attitude/project confidence.
- Actively listen, take notes, and avoid interrupting the customer.
- Be culturally sensitive.
- Use appropriate professional titles when applicable.
- Be on time (if late, contact the customer).

Avoid distractions:

- Personal calls
- Texting/social media sites
- Personal interruption

proper communication (basics)

- Do not argue with customers or be defensive.
- Avoid dismissing customer problems.
- Avoid being judgmental.
- Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding).
- Do not disclose experience via social media outlets.

- Set and meet expectations/timelines and communicate status with the customer.
- Offer repair/replacement options as needed.
- Provide proper documentation on the services provided.
- Follow up with customer/user later to verify satisfaction.

proper communication (dealing with difficult situations)

Ensure you have a professional appearance and attire — match the required attire of the given environment:

- Formal
- Business
- Business casual

Ensure you deal appropriately with customers' confidential and private materials — these may be on a computer, a desktop, a printer, in a file, or elsewhere in the office.

professionalism

Topic:
Basics of Scripting

In this section, we will cover:

- Script File Types
- Use cases for Scripting
- Other Considerations when using Scripts
- Environment Variables
- Data Types
- Integers
- Floating Point Numbers
- Character & Strings
- Loops

script file types

Script files come in many types. Here are some of the more common ones:

- .bat
- .ps1
- .vbs
- .sh
- .js
- .py

It is important to be aware of these file types as these can be used for good or bad (think malware or malicious code execution).

Scripting has many use cases:

- Basic automation
- Restarting machines
- Remapping network drives
- Installation of applications
- Automated backups
- Gathering of information/data
- Initiating updates

Scripting can be very helpful for automating the basic or repetitive actions that need to be completed.

use cases for scripting

other considerations when using scripts

Scripts are great; they are also very powerful, which can lead to some issues, such as:

- Unintentionally introducing malware.
- Inadvertently changing system settings.
- Browser or system crashes due to mishandling of resources.

Be sure to double-check and proofread scripts to ensure accuracy and stability. Always test them thoroughly before using them for large groups of users.

Topic: Remote Access Technologies

In this section, we will cover:

- Telnet
- Secure Shell (SSH)
- Remote Assistance
- Remote Desktop Protocol (RDP)
- Virtual Network Computing (VNC)
- Virtual Private Network (VPN)
- Third-Party Tools

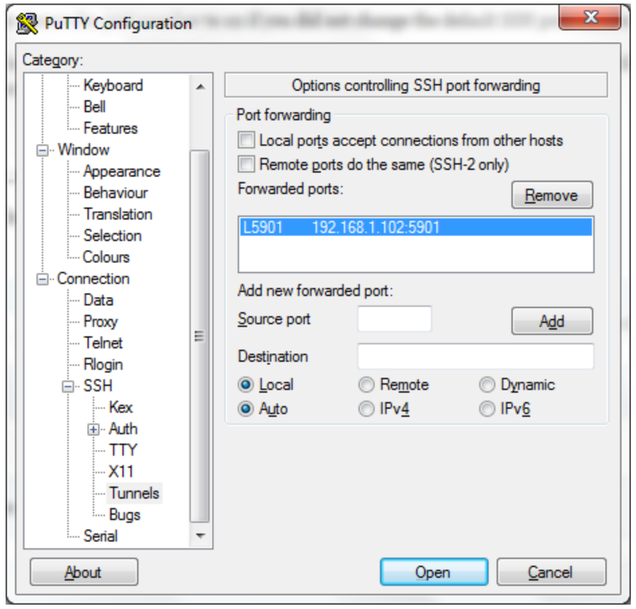
Telnet

Telnet is a protocol that creates an unsecure remote connection between two devices for remote command line administration.

Telnet operates on port 23. With Telnet, an unsecure remote connection is established between two devices; if you use a network sniffer, for example, Wireshark, unencrypted network traffic can be captured.

Telnet was replaced by SSH mostly but can still be used. By nature, it is not enabled in Windows and would need to be enabled. It needs to be verified that the firewall is blocking Telnet communications. This type of connection is not recommended due to the lack of encryption.

Secure Shell (SSH)

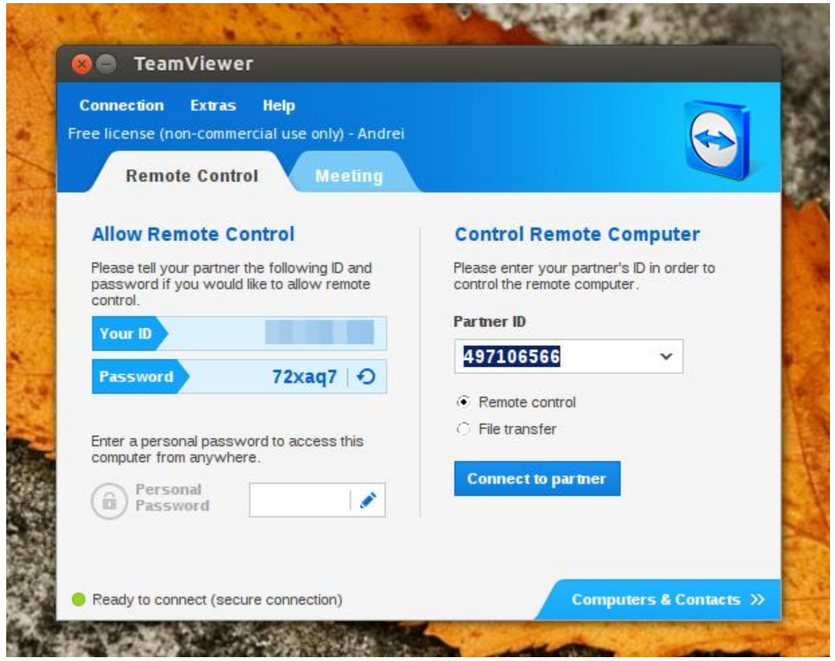


Secure Shell (SSH) is a protocol that creates a secure remote connection between two devices.

Secure Shell (SSH) operates on port 22. A secure connection uses encryption like RSA to help encrypt data packets, which protects information going across the wire.

If you connect to a router or switch, you can protect the usernames and passwords used to access the device. Putty is a free application that can be used for this type of connection: https://www.putty.org/.

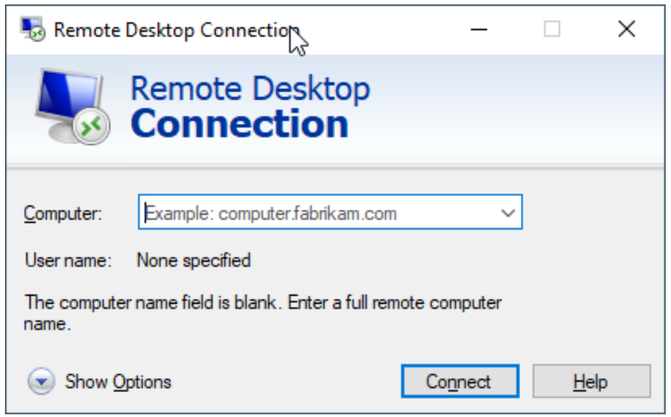
Remote Assistance



Remote Assistance is a remote connection that allows a user to connect to another logged-in user's session through an offer or invitation. This type of connection requires a per-session authorization or a stored persistent authorization.

Once connected, both parties will view the same desktop interface on their respective screens; it will be presented on the client-side connection (invited user) in a program window. Many of these connections offer view-only and/or full-control access options.

Remote Desktop Protocol (RDP)



Remote Desktop Protocol (RDP) is a remote connection protocol that allows users to remotely connect from one device to another device. TCP port 3389 is used by Microsoft's Remote Desktop utility. Using this function, you will log in to a user account and gain full access, per that account, to the computer you are connected to.

This is a client-server connection. The device being used to view the connection is the client, and the device where the host OS is running is the server.

There are many other software options for using remote desktops, such as TeamViewer, AnyDesk, and RealVNC, to name a few.

Virtual Network Computing (VNC)

VNC is the generic term that covers both Remote Desktop and Remote Assistance.

Most software in this space is VNC, meaning they provide both types of connections, sharing a live desktop session or logging into a remote system.

virtual private network (VPN)

A virtual private network (VPN) is used to create a virtual network tunnel between two locations, mostly used across an unprotected WAN, especially the internet.

A VPN uses various encryptions and protocols so that all data is secured from site-to-site, point-to-point, or a combination of those.

In Windows, access the VPN settings in the Control Panel → Internet options → Connections.

third-party tools

A wide variety of Third-party tools are available with special features and functionalities.

Third-party tools include:

- Screen-sharing software
- Video conferencing software
- File transfer software
- Desktop management software

You should always consider the security aspects of different third-party tools you plan to use and/or are using.

summary

In this module, we covered:

- Documentation and Support Systems IS
- Change Management
- Backup and Recovery Methods
- Common Safety Procedures
- Environmental Factors
- IR, Privacy, Policies, and Licensing
- Proper Communication and Professionalism
- Basics of Scripting
- Remote Access Technologies