ICDL

IT Security

Quick Reference

This quick reference is for Microsoft Internet Explorer 10 and Windows 7.

Certification Test Goals

This module sets out concepts relating to the secure use of ICT in daily life and skills used to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately.

Successful candidates will be able to:

- Understand the importance of keeping information and data secure, and identify common data/privacy protection, retention and control principles.
- Recognise threats to personal security from identity theft and potential threats to data from using cloud computing.
- Be able to use passwords and encryption to secure files and data.
- Understand the threat of malware and be able to protect a computer, device or network from malware and address malware attacks.
- Recognise common network and wireless security types and be able to use personal firewalls and personal hotspots.
- Protect a computer or device from unauthorised access and be able to safely manage and update passwords.
- Use appropriate web browser settings and understand how to authenticate websites and browse the web securely.
- Understand communication security issues that can arise from using e-mail, social networks, voice over Internet protocol, instant messaging and mobile devices.
- Back up and restore data to local and cloud storage locations and delete and dispose of data and devices securely.

1 Security Concepts

1.1 Data Threats

1.1.1 Distinguish between data and information.

- Data is unprocessed information for data processing. Data may be a collection of unprocessed numbers, text, or images.
- Information is the processed output of data making it meaningful to the person who receives it.

1.1.2 Understand the terms cybercrime, hacking.

- Cybercrime involves using the Internet or a computer to carry out illegal activities, often for financial or personal gain. Examples include identity theft and social engineering.
- Hacking involves using computer expertise to gain access to a computer system without authorisation. The hacker may wish to tamper with programs and data on the computer, use the computer's resources, or just prove they can access the computer.

1.1.3 Recognise malicious, accidental threats to data from:

- Individuals - Could steal or accidentally delete data such as new product information or important reports
- Service providers - Could lose, destroy, or steal valuable company or personal data
- External organisations - Could gain access to a computer system and steal or delete data

1.1.4 Recognise threats to data from extraordinary circumstances.

- Extraordinary circumstances are natural disasters or unforeseen events that can threaten data like:
  - Fire
  - Floods
  - War
  - Earthquake

1.1.5 Recognise threats to data from using cloud computing like:

- Data control - Access to data could be restricted or unauthorised access allowed leading to malware issues
- Potential loss of privacy - More people could have access to data and could compromise personal (images, videos) or financial (credit card information) data

1.2 Value of Information

1.2.1 Understand basic characteristics of information security like:

- Confidentiality - Ensures information is protected against unauthorised access or disclosure
- Integrity - Ensures the trustworthiness of information resources and that they cannot be modified without authorisation
- Availability - Ensures the availability of information resources

1.2.2 Understand the reasons for protecting personal information like:

- Avoiding identity theft - Personal information can be misused for identity theft
- Avoiding fraud - Personal information can be used fraudulently
- Maintaining privacy - Personal information can be disclosed without permission

1.2.3 Understand the reasons for protecting workplace information on computers and devices like:

- Preventing theft - Stopping client or sensitive company information being stolen
- Preventing fraudulent use - Stopping client or financial information being used fraudulently
- Preventing accidental loss of data - Stopping workplace information being lost by accident
- Preventing sabotage - Stopping workplace information being deliberately damaged or destroyed by employees or competitors

1.2.4 Identify common data/privacy protection, retention and control principles like:

- Transparency - Data subjects have the right to be informed if data controllers process their data.
- Legitimate purposes - Data controllers can only process data for specified and legitimate purposes.
- Proportionality - Data controllers should only process data for an intended purpose, avoiding excessive additional processing.

1.2.5 Understand the terms data subjects and data controllers.

- Data subjects are individuals who provide their personal data to a data controller.
- Data controllers are people or entities who control the content and use of personal data.

1.2.5 Understand how data/privacy protection, retention and control principles apply to data subjects and data controllers.

- Data subjects have rights such as
  - being informed of any data processing where they are the data subject
  - accessing data about themselves
- Data controllers are required to observe several principles such as
  - processing data fairly and lawfully
  - only collecting and using data for legitimate purposes
  - keeping data up to date
  - not keeping data longer than necessary
  - enabling data subjects to fix, erase or block incorrect data about them

1.2.6 Understand the importance of adhering to guidelines and policies for ICT use and how to access them.

- Guidelines and policies provide a standard for users on how ICT should be used to protect the organisation's data.
- Guidelines and policies are typically provided to staff on joining a company with current versions available from the IT department, human resources department or the company intranet or portal.

1.3 Personal Security

1.3.1 Understand the term social engineering.

- Social engineering involves manipulating people into performing actions or divulging confidential information, rather than obtaining the information by hacking.

1.3.1 Understand the implications of social engineering like:

- Unauthorised computer and device access - Potentially accessing confidential information without permission
- Unauthorised information gathering - Collecting information that may be confidential or valuable without permission
- Fraud - Using gathered information to commit an act of deception

1.3.2 Identify methods of social engineering like:

- Phone calls - Misleading someone about your identity in a phone call to gain valuable information
- Phishing - Misleading someone about your identity online to gain valuable information
- Shoulder surfing - Using direct observation such as looking over someone's shoulder to get information

1.3.3 Understand the term identity theft and its implications.

- Identity theft involves assuming another person's identity for personal gain.
- It can lead to the theft or misuse of personal, financial, business or legal information.

1.3.4 Identify methods of identity theft like:

- Information diving - Recovering information from discarded material
- Skimming - Using a scanner device to skim information, often from a credit/debit card
- Pretexting - Gaining personal information through deception

1.4 File Security

1.4.1 Understand the effect of enabling/disabling macro security settings.

- Enabling a macro will ensure that the macro will run but may harm the computer if the source of the file is unknown.
- Disabling a macro will ensure the macro will not run but may prevent you from using all the features of a file.

1.4.2 Understand the advantages and limitations of encryption.

- Advantages:
  - Encrypted data cannot be read without a key.

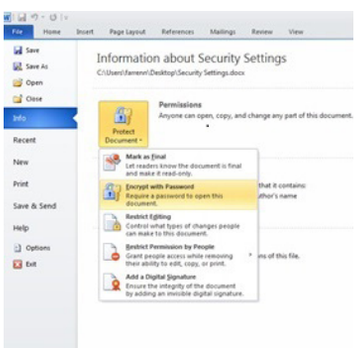
- Only an authorised receiver can read the message.
- Limitations:
  - If the encrypted key is lost, the data becomes unusable.

1.4.2 **Be aware of the importance of not disclosing or losing the encryption password, key, or certificate.**
- Disclosing - Could lead to data theft or misuse
- Losing - Could lead to the data becoming inaccessible

1.4.3 **Encrypt a file, folder.**
- Select the file, folder to encrypt.
- Click File and click Properties.
- On the General tab, click the Advanced button.
- Check the Encrypt contents to secure data check box.
- Click OK twice.

1.4.3 **Encrypt a drive.**
- Click the Start button.
- Click Control Panel.
- Click Security.
- Click BitLocker Drive Encryption.
- Click Turn On BitLocker.
- Follow the setup wizard to complete the encryption setup.

1.4.4 **Set a password for documents.**
- Click File.
- On the Info tab, click Protect Document.
- Click Encrypt with Password.



- Enter a password and click OK.
- Reenter the password and click OK.

1.4.4 **Set a password for spreadsheets.**
- Click File.
- On the Info tab, click Protect Workbook.
- Click Encrypt with Password.
- Enter a password and click OK.
- Reenter the password and click OK.

1.4.4 **Set a password for compressed files.**
- On the Home tab, select Encrypt.
- Select the files, folders to zip.
- Click Zip.
- Enter a password and reenter the password.
- Click OK.

2 Malware

2.1 Types and Methods

2.1.1 **Understand the term malware.**
- Malware is malicious software that is designed to install itself on a computer or device without the owner's consent.

2.1.1 **Recognise different ways that malware can be concealed on computers and devices like:**
- Trojans - Non self-replicating malware that pretend to be harmless applications
- Rootkits - Malware that enable continued access to computers or devices while hiding their presence
- Backdoors - Malware that bypass system security to gain unauthorised remote access to computers

2.1.2 **Recognise types of infectious malware and understand how they work like:**
- Viruses - Malware that can replicate when triggered by a human action and cause damage to a computer
- Worms - Self-replicating malware that uses a computer network to send copies of itself to other computers

2.1.3 **Recognise types of data theft, profit generating/extortion malware and understand how they work like:**
- Adware - Automatically plays, displays, or downloads advertisements to a computer
- Ransomware - Restricts access to files, computers or devices until the user pays a demanded ransom
- Spyware - Collects information on user browser habits without their consent
- Botnets - Infect and control a number of computers without consent for malicious purposes
- Keystroke logging - Captures information that is typed on a keyboard
- Diallers - Install onto computers and attempt to dial premium telephone lines at other locations

2.2 Protection

2.2.1 **Understand how anti-virus software works and its limitations.**
- Anti-virus software uses scans to detect and block viruses before they infect a system.
- Anti-virus software needs to be kept up to date with definition files. It cannot always stop attacks to system vulnerabilities or security flaws.

2.2.2 **Understand that anti-virus software should be installed on computers and devices.**
- Up-to-date anti-virus software should always be installed and enabled on all computers and devices to protect against virus threats.

2.2.3 **Understand the importance of regularly updating software like:**
- Anti-virus - Update regularly to detect new viruses
- Web browser, plug-in, application, operating system - Update regularly to receive the latest support to fix known problems and security risks

2.2.4 **Scan specific drives, folders, files using anti-virus software.**
- Open the anti-virus application.
- Select the Drives, Folders, Files to scan.
- Click Scan.

2.2.4 **Schedule scans using anti-virus software.**
- Open the anti-virus application.
- Click Settings.
- Set the frequency, approximate time and type of scan.
- Click Save.

2.2.5 **Understand the risks of using obsolete and unsupported software like:**
- Increased malware threats - Software that contains flaws and security vulnerabilities can be open to more malware threats.
- Incompatibility - Software that cannot communicate with newer software and hardware can have problems functioning.

2.3 Resolving and Removing

2.3.1 **Understand the term quarantine and the effect of quarantining infected/suspicious files.**
- Quarantining a file moves it to a safe location on a drive managed by the anti-virus software.
- The file can be restored or deleted from quarantine if required.

2.3.2 **Quarantine, delete infected/suspicious files.**
- Click the Start button.
- Click Control Panel.
- Click the Windows Defender button.
- Click Scan.
- Click Full Scan.
- Click Review detected items to view any potential threats detected by the scan.
- Click the Action drop-down and click Quarantine or Remove.
- Click Apply actions.

2.3.3 **Understand that a malware attack can be diagnosed and resolved using online resources like:**
- Websites of operating system software providers - Provide software patches and updates
- Websites of anti-virus software providers - Provide software updates
- Websites of web browser software providers - Provide browser updates
- Websites of relevant authorities - Provide help and guidance documentation

3 Network Security

3.1 Networks and Connections

3.1.1 **Understand the term network.**
- A network is a group of two or more computer systems linked together by communication channels to allow for sharing of resources and information.

3.1.1 **Recognise the common network types like:**
- Local area network (LAN) - A wired network that connects computers and devices in close proximity, usually in the same building
- Wireless local area network (WLAN) - A wireless network that connects computers and devices in close proximity, usually in the same building
- Wide area network (WAN) - A network that connects computers and devices over a long distance, using telephone lines and satellite communications
- Virtual private network (VPN) - A private network typically accessed using the Internet to allow users to privately share information between remote locations, or between a remote location and a business' home network

3.1.2 **Understand how connecting to a network has implications for security like:**
- Computers connected to a network may be infected with malware.
- Connecting to a network may result in unauthorised data access.
- Connecting to a network may increase the challenge of maintaining privacy.

3.1.3 **Understand the role of the network administrator.**
- They are involved in managing the authentication, authorisation and accounting within a network.
- They maintain staff access to required data on the network and ensure network usage is in line with ICT policy.
- Their tasks include monitoring and installing relevant security patches and updates, monitoring network traffic and dealing with malware found within a network.

3.1.4 **Understand the function of a firewall in a personal, work environment.**
- A firewall is used to protect a personal or work network from intrusions from outside sources.

3.1.4 **Understand the limitations of a firewall in a personal, work environment.**
- Does not always provide automatic notification if a network is hacked
- Cannot protect against an attack generated from within the network
- May restrict some legitimate traffic

3.1.5 **Turn a personal firewall on, off.**
- Click the Start button.
- Click Control Panel.
- Click the Windows Firewall button.
- In the left panel, click Turn Windows Firewall on or off.
- Click the appropriate option.
- Click OK.

3.1.5 **Allow an application, service/feature access through a personal firewall.**
- Click the Start button.
- Click Control Panel.
- Click the Windows Firewall button.
- In the left panel, click Allow a program or feature through Windows Firewall.
- Click Change settings.
- Check the check box next to the program or feature you want to allow.
- Check the check box of the network locations you want to allow communication on.
- Click OK.

3.1.5 **Block an application, service/feature access through a personal firewall.**
- Click the Start button.
- Click Control Panel.
- Click the Windows Firewall button.
- In the left panel, click Allow a program or feature through Windows Firewall.
- Click Change settings.
- Uncheck the check box next to the program or feature you want to block.
- Uncheck the check box of the network locations you want to block communication on.
- Click OK.

3.2 Wireless Security

3.2.1 **Recognise different options for wireless security and their limitations like:**
- Wired Equivalent Privacy (WEP) - Limitations include a small number of possible values available, some weak and easily cracked values, and keys remaining

static leading to repeat use.
- Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2) - Limitations include possibly needing to update older wireless access points and software, WPA being hacked with advanced tools, and WPA2, though more secure, can slow down computer or device performance.
- Media Access Control (MAC) filtering - Limitations include difficulty keeping track of addresses with many devices.
- Service Set Identifier (SSID) hiding - Limitations include software utilities finding the hidden SSID.

3.2.2 **Understand that using an unprotected wireless network can lead to attacks like:**
- Eavesdroppers - Other people accessing and reading your data to find sensitive or confidential information
- Network hijacking - Other people taking control of network communications
- Man in the middle - Other people observing communications and collecting data that is transmitted

3.2.3 **Understand the term personal hotspot.**
- A personal hotspot enables a mobile device to share its internet/data connection with other devices.

3.2.4 **Enable a secure personal hotspot.**
Example - iOS:
- Click Settings.
- Click Mobile.
- Click Personal Hotspot within Mobile Data Network.
- Enter an APN, Username and Password.
- Click Settings.
- Click Personal Hotspot.
- Click the slider to turn on.

3.2.4 **Disable a secure personal hotspot.**
- Click Settings.
- Click Personal Hotspot.
- Click the slider to turn off.

3.2.4 **Securely connect devices to a secure personal hotspot.**
- Click Settings.
- Click Wi-Fi.
- Click the name of the personal hotspot.
- Enter the Wi-Fi Password.
- Click Done.

3.2.4 **Securely disconnect devices from a secure personal hotspot.**
- Click Settings.
- Click Wi-Fi.
- Click Disconnect Wi-Fi Clients.

4 Access Control

4.1 Methods

4.1.1 **Identify measures for preventing unauthorised access to data like:**
- User name - A unique name given to authorised users
- Password - A string of characters used for authentication, to prove identity or gain access to a resource
- PIN - A personal identification number, used as a numeric password for authentication, to prove identity or gain access to a resource
- Encryption - The process of encoding data to make it unintelligible to any unauthorised person who tries to read the data
- Multi-factor authentication - Uses two or more independent authentication credentials from the following:
  - What the user knows (password or PIN)
  - What the user has (security token or smart card)
  - What the user is (biometrics)

4.1.2 **Understand the term one-time password and its typical use.**
- A one-time password is valid for only one login session or transaction, offering enhanced security.
- It is typically used when accessing important data, for example from a VPN or when carrying out financial transactions.

4.1.3 **Understand the purpose of a network account.**
- A network account provides network security by only allowing users with unique network accounts to access the network.

4.1.4 **Understand that a network account should be:**
- Accessed through a user name and password
- Locked or logged off when not in use

4.1.5 **Identify common biometric security techniques used in access control like:**
- Fingerprint scanning
- Eye scanning
- Face recognition
- Hand geometry

4.2 Password Management

4.2.1 **Recognise good password policies, like:**
- Adequate password length
- Adequate letter, number and special characters mix
- Not sharing passwords
- Changing them regularly
- Different passwords for different services

4.2.2 **Understand the function of password manager software.**
- Password manager software is used to store multiple usernames and passwords securely in one place. One master password is used to open the software and gain access to multiple usernames and passwords.

4.2.2 **Understand the limitations of password manager software.**
- Spyware or hackers only have to guess one password to gain access to multiple usernames and passwords.

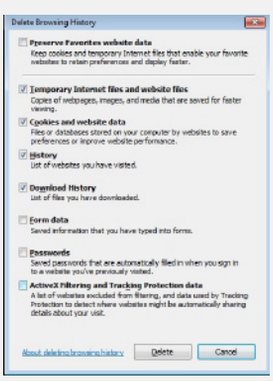
5 Secure Web Use

5.1 Browser Settings

5.1.1 **Select appropriate settings for enabling, disabling autocomplete when completing a form.**
- Click the Tools button on the Command bar.
- Click Internet Options.
- Click the Content tab.
- Click Settings beside AutoComplete.
- Check or uncheck the AutoComplete options as required.
- Click OK.

5.1.1 **Select appropriate settings for enabling, disabling autosave when completing a form.**
- Click the Tools button on the Command bar.
- Click Internet Options.
- Click the Content tab.
- Click Settings beside AutoComplete.
- Check or uncheck the AutoComplete options for saving user names and passwords as required.
- Click OK.

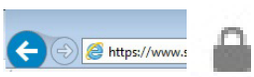
5.1.2 **Delete private data from a browser like: browsing history, download history, cached Internet files, passwords, cookies, autocomplete data.**
- Click the Tools button on the Command bar.
- Click Internet Options.
- On the General tab, in the Browsing history field, click the Delete button.
- Check or uncheck the Browsing history options as required.



5.2 Secure Browsing

5.2.1 **Be aware that certain online activity (purchasing, banking) should only be undertaken on secure web pages using a secure network connection.**
- Purchasing - For example online shopping
- Banking - For example online banking, fund transfers

5.2.2 **Identify ways to confirm the authenticity of a website like:**
- Content quality - Ensure the website is free from spelling and grammar mistakes.
- Currency - Ensure the website is regularly updated and shows a recent date.
- Valid URL - Ensure the URL matches the company name e.g. www.paypal.com and not www.ppaypal.com.
- Company or owner information - Ensure that detailed company or owner information is visible on the website.
- Contact information - Ensure the contact information e.g. address, telephone and e-mail are visible. Contact the company using these details to double check that they are authentic.
- Validating domain owner - Validate the domain owner using a website checking service such as whois.com.
- Security certificate - Make sure the website is secure (https://www.example.com) and has a valid security certificate (click on the padlock symbol to access the certificate).



5.2.3 **Understand the term pharming.**
- Pharming is an attack that redirects a website's traffic to a fake website without the user or website's knowledge or consent in order to steal the information they enter, such as their bank details.

5.2.4 **Understand the function and types of content-control software like:**
- Internet filtering software - Designed to filter and monitor access to websites to make undesirable content unavailable to the user
- Parental control software - Used to restrict the time spent on the Internet and the type of content accessed

6 Communications

6.1 E-Mail

6.1.1 **Understand the purpose of encrypting, decrypting an e-mail.**
- Encrypting and decrypting an e-mail ensure that only the intended recipient can read it.

6.1.2 **Understand the term digital signature.**
- A digital signature is a mathematical scheme used to validate the authenticity of a message.

6.1.3 **Identify possible fraudulent e-mail, unsolicited e-mail.**
- A fraudulent or unsolicited e-mail may contain a virus or malware, or be an attempt to gain information from the recipient and should not be opened.

6.1.4 **Identify common characteristics of phishing like:**
- Using names of legitimate organisations, people
- Using false web links, logos, branding
- Encouraging disclosure of personal information

6.1.5 **Be aware that you can report phishing attempts to the legitimate organisation, relevant authorities.**
- Phishing attempts can be reported to legitimate organisations (bank, online retailer) or relevant authorities (government security agency).

6.1.6 **Be aware of the danger of infecting a computer or device with malware:**
- By opening an e-mail attachment that contains a macro
- By opening an e-mail attachment that contains an executable file

6.2 Social Networking

6.2.1 **Understand the importance of not disclosing confidential or personal identifiable information on social networking sites.**

- Confidential information can include passwords, PIN numbers, certain company information, and client details.
- Personal identifiable information can include full name, home address, national identification number, and date of birth.
- Disclosing such information could lead to personal information, company information, client information or finances being stolen or misused.

6.2.2 **Be aware of the need to apply and regularly review appropriate social networking account settings like:**

- Account privacy - Privacy settings can be customized to show different personal details to different people or groups in order to protect the user's privacy.
- Location - Location settings can be adjusted to show or hide the user's location.
- Regularly review settings to ensure they are appropriate.

6.2.3 **Apply social networking account settings: account privacy**

Example - Facebook:

- Click ▼ in the upper-right corner of the social network site page.
- Click Settings from the drop-down menu.
- Click Privacy on the left.
- Click a setting to edit it.

6.2.3 **Apply social networking account settings: location**

- Go to a post on the Timeline.
- Click ∨ and select Change Location.
- Click x to remove it.
- Click OK.

6.2.4 **Understand potential dangers when using social networking sites like:**

- Cyber bullying - Harming other people, in a deliberate, repeated, and hostile manner through the site
- Grooming - Befriending a person through the site, in the negative context of preparing them to accept inappropriate behaviour
- Malicious disclosure of personal content - Maliciously circulating personal content, such as images and videos, of other users
- False identities - Assuming a false user identity to contact or trick other users
- Fraudulent or malicious links, content, messages - Sending links, content or messages to get information from other users

6.2.5 **Be aware that you can report inappropriate social network use or behaviour to the service provider, relevant authorities.**

- Inappropriate social network use or behaviour can be reported to the service provider (social network) or relevant authorities (police, government agency).

6.3 VoIP and Instant Messaging

6.3.1 **Understand the security vulnerabilities of instant messaging (IM) and Voice over IP (VoIP) like:**

- Malware access
- Backdoor access
- Access to files
- Eavesdropping

6.3.2 **Recognise methods of ensuring confidentiality while using IM and VoIP like:**

- Encryption
- Non-disclosure of important information
- Restricting file sharing

6.4 Mobile

6.4.1 **Understand the possible implications of using applications from unofficial application stores like:**

- Mobile malware - Can be created by individuals to rapidly spread malware, which is facilitated by a lack of technical support or application store quality controls.
- Unnecessary resource utilisation - May not be fully tested and quality approved and can slow down a mobile device and other applications.
- Access to personal data - May automatically give the application permission to access personal data such as contacts, images, and location without the user's knowledge.
- Poor quality - Insufficient testing and lack of quality control can lead to poor quality applications and device instability.
- Hidden costs - Users can unknowingly sign up to contracts or in-application purchases that charge large amounts of money.

6.4.2 **Understand the term application permissions.**

- Application permissions are requested by an application during installation to allow it to access data such as location, personal information, storage, and network communication. The user should consider if the application needs these permissions before authorising them.

6.4.3 **Be aware that mobile applications can extract private information from the mobile device like:**

- Contact details - Can be accessed by the application and used for their own purposes
- Location history - Can be recorded using the device GPS
- Images - Can be accessed and used without the user's knowledge

6.4.4 **Be aware of emergency and precautionary measures if a device is lost like:**

- Remote disable - Can be installed or enabled on the device so that the device can be disabled remotely. The data will remain on the local drive.
- Remote wipe - Can be installed or enabled on the device so that the device data can be wiped remotely so it is no longer accessible.
- Locate device - Can be installed or enabled on a device so that the device can be tracked and found using GPS to provide the coordinates of the device location.

7 Secure Data Management

7.1 Secure and Back up Data

7.1.1 **Recognise ways of ensuring physical security of computers and devices like:**

- Do not leave computers or devices unattended to avoid theft.
- Log equipment location and details to track them.
- Use cable locks to secure computers and devices safely.
- Implement access control measures such as swipe cards, biometric scans.

7.1.2 **Recognise the importance of having a backup procedure in case of loss of data from computers and devices.**

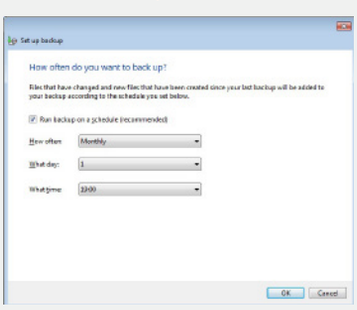
- Backup procedures will ensure that data can be recovered from a backup copy if it is lost from a computer or device.

7.1.3 **Identify the features of a backup procedure like:**

- Regularity/frequency - Set up how often you want a back-up to occur.
- Schedule - Set up a back-up schedule.
- Storage location - Set up a location to store your back-up to like an external hard drive.
- Data compression - Choose from any available compression options.

7.1.4 **Back up data to a location like: local drive, external drive/media, cloud service.**

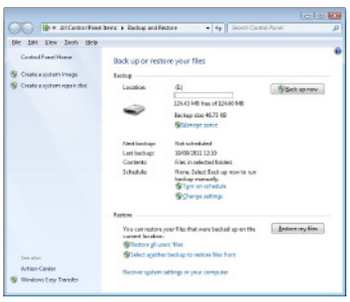
- Click the Start button.
- Click Control Panel.
- Click the Backup and Restore button.
- Click Set up Backup.
- Select a back-up location (drive/network) and click Next.
- Select the data to back up or accept the recommended default settings.
- Select the back-up schedule.



- Save Settings and Backup.

7.1.5 **Restore data from a backup location like: local drive, external drive/media, cloud service.**

- Click the Start button.
- Click Control Panel.
- Click the Backup and Restore button.
- Click Restore My Files.
- Select the files or folders (or items) to restore by using Search, Browse for Files or Browse for Folders.



- Click Next.
- Choose to restore In the original location or In the following location to choose a new location.
- Click Restore.

7.2 Secure Deletion and Destruction

7.2.1 **Distinguish between deleting and permanently deleting data.**

- Deleting data by moving it to the recycle bin does not permanently destroy the data.
- Permanently deleting data by shredding or degaussing ensures that it cannot be recovered.

7.2.2 **Understand the reasons for permanently deleting data from drives or devices.**

- Preventing identity theft
- Protecting valuable or confidential company information from being discovered by a third party
- Disposing of the drive or device safely
- Reassuring clients, customers or individuals that their data has been permanently deleted

7.2.3 **Be aware that content deletion may not be permanent on services like:**

- Social network site - Deleted content may be deleted from the page but still exist in other posts or on the provider's server.
- Blog - Deleted blog posts may still exist on the provider's server or be searchable as cached web pages.
- Internet forum - Deleted Internet forum posts may still exist on the provider's server, in other forum posts where they have been quoted or be searchable as cached web pages.
- Cloud service - Deleted data may be stored on multiple servers in various locations and also be recoverable in case of accidental deletion.

7.2.4 **Identify common methods of permanently deleting data like:**

- Shredding - Shredding disks like CDs/DVDs
- Drive/media destruction - Physically destroying drives or media
- Degaussing - Leaving the magnetic domains on a disk in random patterns rendering previous data unrecoverable
- Using data destruction utilities - Using a software utility for destroying data on a drive

For more information, visit: **www.icdl.org**