ICDL
The Digital Skills Standard

ICDL Workforce

IT SECURITY

Syllabus 2.0

Syllabus Document

Purpose

This document details the syllabus for the IT Security module. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for the IT Security module should possess. The syllabus also provides the basis for the theory and practice-based test in this module.

Disclaimer

Although every care has been taken by ICDL Foundation in the preparation of this publication, no warranty is given by ICDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ICDL Foundation be responsible or liable for any errors, omissions, inaccuracies, loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes may be made by ICDL Foundation at its own discretion and at any time without notice.

IT Security Module

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.

Module Goals

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.

CATEGORY	SKILL SET	REF.	TASK ITEM
1 Security Concepts	*1.1 Data Threats*	1.1.1	Distinguish between data and information.
		1.1.2	Understand the terms cybercrime, hacking.
		1.1.3	Recognise malicious, accidental threats to data from individuals, service providers, external organisations.
		1.1.4	Recognise threats to data from extraordinary circumstances like: fire, floods, war, earthquake.
		1.1.5	Recognise threats to data from using cloud computing like: data control, potential loss of privacy.
	1.2 Value of Information	1.2.1	Understand basic characteristics of information security like: confidentiality, integrity, availability.

CATEGORY	SKILL SET	REF.	TASK ITEM
		1.2.2	Understand the reasons for protecting personal information like: avoiding identity theft, fraud, maintaining privacy.
		1.2.3	Understand the reasons for protecting workplace information on computers and devices like: preventing theft, fraudulent use, accidental data loss, sabotage.
		1.2.4	Identify common data/privacy protection, retention and control principles like: transparency, legitimate purposes, proportionality.
		1.2.5	Understand the terms data subjects and data controllers and how data/privacy protection, retention and control principles apply to them.
		1.2.6	Understand the importance of adhering to guidelines and policies for ICT use and how to access them.
	1.3 Personal Security	1.3.1	Understand the term social engineering and its implications like: unauthorised computer and device access, unauthorised information gathering, fraud.
		1.3.2	Identify methods of social engineering like: phone calls, phishing, shoulder surfing.
		1.3.3	Understand the term identity theft and its implications: personal, financial, business, legal.
		1.3.4	Identify methods of identity theft like: information diving, skimming, pretexting.
	1.4 File Security	1.4.1	Understand the effect of enabling/disabling macro security settings.
		1.4.2	Understand the advantages, limitations of encryption. Be aware of the importance of not disclosing or losing the encryption password, key, certificate.
		1.4.3	Encrypt a file, folder, drive.
		1.4.4	Set a password for files like: documents, spreadsheets, compressed files.

CATEGORY	SKILL SET	REF.	TASK ITEM
2 Malware	*2.1 Types and Methods*	2.1.1	Understand the term malware. Recognise different ways that malware can be concealed on computers and devices like: Trojans, rootkits, backdoors.
		2.1.2	Recognise types of infectious malware and understand how they work like: viruses, worms.
		2.1.3	Recognise types of data theft, profit generating/extortion malware and understand how they work like: adware, ransomware, spyware, botnets, keystroke logging, diallers.
	2.2 Protection	2.2.1	Understand how anti-virus software works and its limitations.
		2.2.2	Understand that anti-virus software should be installed on computers and devices.
		2.2.3	Understand the importance of regularly updating software like: anti-virus, web browser, plug-in, application, operating system.
		2.2.4	Scan specific drives, folders, files using anti-virus software. Schedule scans using anti-virus software.
		2.2.5	Understand the risks of using obsolete and unsupported software like: increased malware threats, incompatibility.
	2.3 Resolving and Removing	2.3.1	Understand the term quarantine and the effect of quarantining infected/suspicious files.
		2.3.2	Quarantine, delete infected/suspicious files.
		2.3.3	Understand that a malware attack can be diagnosed and resolved using online resources like: websites of operating system, anti-virus, web browser software providers, websites of relevant authorities.
3 Network Security	*3.1 Networks and Connections*	3.1.1	Understand the term network and recognise the common network types like: local area network (LAN), wireless local area network (WLAN), wide area network (WAN), virtual private network (VPN).

CATEGORY	SKILL SET	REF.	TASK ITEM
		3.1.2	Understand how connecting to a network has implications for security like: malware, unauthorised data access, maintaining privacy.
		3.1.3	Understand the role of the network administrator in managing authentication, authorisation and accounting, monitoring and installing relevant security patches and updates, monitoring network traffic, and in dealing with malware found within a network.
		3.1.4	Understand the function, limitations of a firewall in personal, work environment.
		3.1.5	Turn a personal firewall on, off. Allow, block an application, service/feature access through a personal firewall.
	3.2 Wireless Security	3.2.1	Recognise different options for wireless security and their limitations like: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) filtering, Service Set Identifier (SSID) hiding.
		3.2.2	Understand that using an unprotected wireless network can lead to attacks like: eavesdroppers, network hijacking, man in the middle.
		3.2.3	Understand the term personal hotspot.
		3.2.4	Enable, disable a secure personal hotspot, and securely connect, disconnect devices.
4 Access Control	*4.1 Methods*	4.1.1	Identify measures for preventing unauthorised access to data like: user name, password, PIN, encryption, multi-factor authentication.
		4.1.2	Understand the term one-time password and its typical use.
		4.1.3	Understand the purpose of a network account.
		4.1.4	Understand that a network account should be accessed through a user name and password and locked, logged off when not in use.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.1.5	Identify common biometric security techniques used in access control like: fingerprint, 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, limitations of password manager software.
5 Secure Web Use	*5.1 Browser Settings*	5.1.1	Select appropriate settings for enabling, disabling autocomplete, autosave when completing a form.
		5.1.2	Delete private data from a browser like: browsing history, download history, cached Internet files, passwords, cookies, autocomplete data.
	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.
		5.2.2	Identify ways to confirm the authenticity of a website like: content quality, currency, valid URL, company or owner information, contact information, security certificate, validating domain owner.
		5.2.3	Understand the term pharming.
		5.2.4	Understand the function and types of content-control software like: Internet filtering software, parental control software.
6 Communications	*6.1 E-Mail*	6.1.1	Understand the purpose of encrypting, decrypting an e-mail.
		6.1.2	Understand the term digital signature.
		6.1.3	Identify possible fraudulent e-mail, unsolicited e-mail.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.1.4	Identify common characteristics of phishing like: using names of legitimate organisations, people, false web links, logos and branding, encouraging disclosure of personal information.
		6.1.5	Be aware that you can report phishing attempts to the legitimate organisation, relevant authorities.
		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 or 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.
		6.2.2	Be aware of the need to apply and regularly review appropriate social networking account settings like: account privacy, location.
		6.2.3	Apply social networking account settings: account privacy, location.
		6.2.4	Understand potential dangers when using social networking sites like: cyber bullying, grooming, malicious disclosure of personal content, false identities, fraudulent or malicious links, content, messages.
		6.2.5	Be aware that you can report inappropriate social network use or behaviour to the service provider, relevant authorities.
	6.3 VoIP and Instant Messaging	6.3.1	Understand the security vulnerabilities of instant messaging (IM) and Voice over IP (VoIP) like: malware, 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, unnecessary resource utilisation, access to personal data, poor quality, hidden costs.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.4.2	Understand the term application permissions.
		6.4.3	Be aware that mobile applications can extract private information from the mobile device like: contact details, location history, images.
		6.4.4	Be aware of emergency and precautionary measures if a device is lost like: remote disable, remote wipe, locate device.
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 unattended, log equipment location and details, use cable locks, access control.
		7.1.2	Recognise the importance of having a backup procedure in case of loss of data from computers and devices.
		7.1.3	Identify the features of a backup procedure like: regularity/frequency, schedule, storage location, data compression.
		7.1.4	Back up data to a location like: local drive, external drive/media, cloud service.
		7.1.5	Restore data from a backup location like: local drive, external drive/media, cloud service.
	7.2 Secure Deletion and Destruction	7.2.1	Distinguish between deleting and permanently deleting data.
		7.2.2	Understand the reasons for permanently deleting data from drives or devices.
		7.2.3	Be aware that content deletion may not be permanent on services like: social network site, blog, Internet forum, cloud service.
		7.2.4	Identify common methods of permanently deleting data like: shredding, drive/media destruction, degaussing, using data destruction utilities.