™ ICDL
Arabia

SYLLABUS

ICDL Module
Cyber Security

Syllabus Version 1.0

Purpose

This document details the syllabus for the Cyber Security module. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for the ICT in Education 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 ECDL Foundation in the preparation of this publication, no warranty is given by ECDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ECDL 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 ECDL Foundation at its own discretion and at any time without notice.

Purpose

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

Copyright © 1997 - 2015 ECDL Foundation

Disclaimer

Although every care has been taken by ECDL Foundation in the preparation of this publication, no warranty is given by ECDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ECDL 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 ECDL Foundation at its own discretion and at any time without notice.

ICDL - Cyber Security V1.0 (Part 1)

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, and external organisations.
		1.1.4	Recognise threats to data from extraordinary circumstances like: fire, floods, war, and earthquake.
		1.1.4	Recognise threats to data from extraordinary circumstances like: fire, floods, war, and 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.
		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	Recognise the serious threats posed by Internet criminals and Internet scams.
		1.3.2	Understand the term identity theft and its implications: personal, finance, business, legal.

CATEGORY	SKILL SET	REF.	TASK ITEM
		1.3.3	Identify methods of identity theft like: information diving, skimming, pretexting.
		1.3.4	Understand the term social engineering and its implications like: unauthorised computer and device access, unauthorised information gathering, fraud.
		1.3.5	Identify methods of social engineering like: phone calls, phishing, shoulder surfing.
	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.
2. Malware	*2.1 Types & 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, dialers.
	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.

CATEGORY	SKILL SET	REF.	TASK ITEM
	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 recognize the common network types like: local area network (LAN), wireless local area network (WLAN), wide area network (WAN), virtual private network (VPN).
		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 Controls (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 unauthorized access to data like: user name, password, PIN, encryption, multi-factor authentication.

CATEGORY	SKILL SET	REF.	TASK ITEM
		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.
		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, auto-save 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: https, lock symbol, 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
6. Communication	*6.1 Email*	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.
		6.2.4	Be aware of the need to apply and regularly review appropriate social networking account settings like: account privacy, location.
		6.2.5	Apply social networking account setting: account privacy, location.
		6.2.6	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, inappropriate content, age verification issues, access to profiles, online predators, and online grooming
		6.2.7	Be aware that you can report inappropriate social network use or behavior 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 applications stores like: mobile malware, unnecessary resource utilisation, access to personal data, poor quality, hidden costs.
		6.4.2	Understand the term application permissions.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.4.3	Be aware that mobile applications can extract private information 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 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.

ICDL - Cyber Security V1.0 (Part 2)

CATEGORY	SKILL SET	REF.	TASK ITEM
1. PROTECT	*1.1 Personal Security*	1.1.1	Recognise that personal information contained on your computer needs to be safeguarded.
		1.1.2	Understand the concept of user authentication.
		1.1.3	Understand ‘two-factor’ authentication: tokens, smart cards, biometric.
2. SECURE	*2.1 Backup*	2.1.1	Recognise common backup devices: CD’s, DVD’s USB Drives, External Hard Drives, cloud storage and be aware of different capacities.
	2.2 Email	2.2.1	Understand the concept of junk /Spam email and the need to filter email. Know how to scan email attachments before opening them.
		2.2.2	Turn on the Spam filter in your email.
		2.2.3	Set Spam filter rules.
	2.3 Smart Devices	2.3.1	Recognise what information your device contains and shares online and how it could be misused.
		2.3.2	Be aware of basic security features: password protect device, set automatic locking facility, install security software, install operating system updates, mobile tracking.
		2.3.3	Know how using encryption on your smartphone can help prevent data theft.
		2.3.4	Be aware of security issues with apps. Only download apps from approved sources, check apps permissions.
		2.3.5	Be aware of security threats arising from unsolicited email or text messages. Recognise symptoms of malicious software infection: unusual data charges on bill, unexplained changes in user interface.
		2.3.6	Know how to turn off automatic Wi-Fi and Bluetooth functions to prevent unauthorized access to your device and data.
		2.3.7	Know how to delete all personal information when disposing of device.
		2.3.8	Know how to enable and disable location settings. Understand the advantages and risks of enabling location settings.
		2.3.9	Only share your mobile number with people you know and trust. Keep a record of your IMEI number in case your phone is lost or stolen.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.3.10	Know how to switch on the Internet filter to block inappropriate Internet content.
	2.4. Wireless	2.4.1	Recognise the advantages and risks associated with using public Wi-Fi hotspots.
	2.5. Physical	2.5.1	Recognise physical security considerations around laptop, tablet usage.
		2.5.2	Know how to minimize risk associated with theft or loss: keep device in view, use security cable (if appropriate), password protect, note serial number, use security pen marker.
		2.5.3	Recognise security issues around disposal of computers and the importance of data removal before disposal.
	2.6 The Digital Underworld	2.6.1	Be aware of the content to which people can get access outside the World Wide Web (.com, .org, etc.)
		2.6.2	Be aware of the terms 'Deep Web' and 'Dark Net' and how people can use them outside the World Wide Web (.com, .org, etc.)..
		2.6.3	Understand what The Onion Router (TOR) is and how people can deliver messages through them.
3. BEWARE	*3.1. General Online Risks*	3.1.1	Recognise how pervasive inappropriate material is on the Internet.
		3.1.2	Be aware of common threats: recognise suspicious email requests, potentially malicious web sites.
	3.2 Social Networking	3.2.1	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, inappropriate content, age verification issues, access to profiles, online predators, and online grooming.
4. IDENTITY	*4.1 Personal Identity*	4.1.1	Consider who can access your personal information: friends, work colleagues, employers, criminals, predators.
		4.1.2	Be aware of the range of devices that can be used to share information: mobile phones, Smart Phones, MP3 players, iPods, Tablets etc.
5. CITIZEN PROTECTION	*5.1 Videos/ Blogs*	5.2.4	Understand how file sharing web sites work, and the potential for viruses and malware from using file sharing sites.

CATEGORY	SKILL SET	REF.	TASK ITEM
	5.2 Cyber Bullying	5.2.1	Recognise and understand what Cyberbullying is.
		5.2.2	Understand the mediums through which Cyberbullying can occur.
		5.2.3	Understand the speed with which information / pictures can spread and the impact of Cyberbullying.
		5.2.4	Understand the consequences of cyber bullying. Understand the motives for bullying online, such as anonymity, bully feels they can 'get away with. it'Understand that online bullying can also be a two way process.
		5.2.5	Know how to counter Cyberbullying, how to record it and report Cyberbullying concerns to the appropriate authorities.
		5.2.6	Recognise that adults can also suffer from Cyberbullying: inappropriate comments in messages, emails, on public forums and social network sites, inappropriate texting, Cyber Stalking. Understand the difference between Cyber Stalking and Social Engineering.
	5.3 Virtual Behaviour & Responsibility	5.3.1	Do not circulate messages, pictures, or other material that can be hurtful. Share images only with people you know and trust.
		5.3.2	Know how to decline or block strangers and unwanted contacts. Be careful about planning to meet people you don't really know, even if they have become your 'online friends'.
		5.3.3	Use a webcam only with people you know – disconnect or disable it when not using it.
		5.3.4	Be aware that downloading pictures, computer programs and from the Internet may be against the law, unless it clearly says on the site you are using.
		5.3.5	Understand what 'Netiquette' means.
		5.3.6	Know why 'smart' online user names that reveal only limited personal information are used.
		5.3.7	Recognise why protecting personal information, and maintaining privacy is always important.
		5.3.8	Understand that personal and work-related social media posts, comments and messages on platforms (i.e. WhatsApp, Snapchat, Instagram, Facebook etc.) can potentially impact your employer's reputation and your career.

CATEGORY	SKILL SET	REF.	TASK ITEM
		5.3.9	Understand that organisations should have publically stated disclaimers which clarify that employees' opinions on social media are personal and do not represent the organisation.
		5.3.10	Understand why employees should be restricted from publicly releasing any comments or information that could potentially influence or impact legal, commercial or policy decision
		5.3.11	Know why it may be appropriate to create different user accounts with different access and privileges for each account.
	5.4 Online Addiction	5.4.1	Understand how Internet use can interfere with daily life, work and relationships.
	5.5 Online Radicalisation	5.5.1	Understand the terms online radicalisation and online extremism.
		5.5.2	Be aware of how extremists use social media to groom young people and commit illegal acts.
6. POLICY	*6.1 Usage*	6.1.1	Understand what an Acceptable Usage Policy (AUP) is and why it is important in organizations
		6.1.2	Know the components of a good AUP: minimize risk, encourage Netiquette & appropriate social & ethical behaviour, personal identity, password protection.
	6.2 Copyright	6.2.1	Be aware of copyright laws and their impact for illegal downloads using file sharing services.