ECDL Foundation

ECDL / ICDL IT Security

Syllabus Version 1.0

Purpose

This document details the syllabus for *ECDL / ICDL IT Security*. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for *ECDL / ICDL IT Security* 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.

ECDL / ICDL IT Security

This module sets out essential concepts and skills relating to the ability to understand the main concepts underlying the secure use of ICT in daily life and to use relevant techniques and applications 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 key concepts relating to the importance of secure information and data, physical security, privacy and identity theft.
- Protect a computer, device or network from malware and unauthorised access.
- Understand the types of networks, connection types and network specific issues including firewalls.
- Browse the World Wide Web and communicate on the Internet securely.
- Understand security issues related to communications including e-mail and instant messaging.
- Back up and restore data appropriately and safely, and securely dispose of data and devices.

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 term cybercrime.
		1.1.3	Understand the difference between hacking, cracking and ethical hacking.
		1.1.4	Recognise threats to data from force majeure like: fire, floods, war, earthquake.
		1.1.5	Recognise threats to data from: employees, service providers and external individuals.
	1.2 Value of Information	1.2.1	Understand the reasons for protecting personal information like: avoiding identity theft, fraud.

CATEGORY	SKILL SET	REF.	TASK ITEM
		1.2.2	Understand the reasons for protecting commercially sensitive information like: preventing theft or misuse of client details, financial information.
		1.2.3	Identify measures for preventing unauthorised access to data like: encryption, passwords.
		1.2.4	Understand basic characteristics of information security like: confidentiality, integrity, availability.
		1.2.5	Identify the main data/privacy protection, retention and control requirements in your country.
		1.2.6	Understand the importance of creating and adhering to guidelines and policies for ICT use.
	1.3 Personal Security	1.3.1	Understand the term social engineering and its implications like: information gathering, fraud, computer system access.
		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	Set a password for files like: documents, compressed files, spreadsheets.
		1.4.3	Understand the advantages and limitations of encryption.

CATEGORY	SKILL SET	REF.	TASK ITEM
2 Malware	*2.1 Definition and Function*	2.1.1	Understand the term malware.
		2.1.2	Recognise different ways that malware can be concealed like: Trojans, rootkits and back doors.
	2.2 Types	2.2.1	Recognise types of infectious malware and understand how they work like: viruses, worms.
		2.2.2	Recognise types of data theft, profit generating/extortion malware and understand how they work like: adware, spyware, botnets, keystroke logging and diallers.
	2.3 Protection	2.3.1	Understand how anti-virus software works and its limitations.
		2.3.2	Scan specific drives, folders, files using anti-virus software. Schedule scans using anti-virus software.
		2.3.3	Understand the term quarantine and the effect of quarantining infected/suspicious files.
		2.3.4	Understand the importance of downloading and installing software updates, anti-virus definition files.
3 Network Security	*3.1 Networks*	3.1.1	Understand the term network and recognise the common network types like: local area network (LAN), wide area network (WAN), virtual private network (VPN).
		3.1.2	Understand the role of the network administrator in managing the authentication, authorisation and accounting within a network.
		3.1.3	Understand the function and limitations of a firewall.
	3.2 Network Connections	3.2.1	Recognise the options for connecting to a network like: cable, wireless.

CATEGORY	SKILL SET	REF.	TASK ITEM
		3.2.2	Understand how connecting to a network has implications for security like: malware, unauthorised data access, maintaining privacy.
	3.3 Wireless Security	3.3.1	Recognise the importance of requiring a password for protecting wireless network access.
		3.3.2	Recognise different types of wireless security like: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
		3.3.3	Be aware that using an unprotected wireless network can allow wireless eavesdroppers to access your data.
		3.3.4	Connect to a protected/ unprotected wireless network.
	3.4 Access Control	3.4.1	Understand the purpose of a network account and how it should be accessed through a user name and password.
		3.4.2	Recognise good password policies, like: not sharing passwords, changing them regularly, adequate password length, adequate letter, number and special characters mix.
		3.4.3	Identify common biometric security techniques used in access control like: fingerprint, eye scanning.
4 Secure Web Use	*4.1 Web Browsing*	4.1.1	Be aware that certain online activity (purchasing, financial transactions) should only be undertaken on secure web pages.
		4.1.2	Identify a secure website like: https, lock symbol.
		4.1.3	Be aware of pharming.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.1.4	Understand the term digital certificate. Validate a digital certificate.
		4.1.5	Understand the term one-time password.
		4.1.6	Select appropriate settings for enabling, disabling autocomplete, autosave when completing a form.
		4.1.7	Understand the term cookie.
		4.1.8	Select appropriate settings for allowing, blocking cookies.
		4.1.9	Delete private data from a browser like: browsing history, cached internet files, passwords, cookies, autocomplete data.
		4.1.10	Understand the purpose, function and types of content-control software like: internet filtering software, parental control software.
	4.2 Social Networking	4.2.1	Understand the importance of not disclosing confidential information on social networking sites.
		4.2.2	Be aware of the need to apply appropriate social networking account privacy settings.
		4.2.3	Understand potential dangers when using social networking sites like: cyber bullying, grooming, misleading/ dangerous information, false identities, fraudulent links or messages.
5 Communications	*5.1 E-Mail*	5.1.1	Understand the purpose of encrypting, decrypting an e-mail.
		5.1.2	Understand the term digital certificate.
		5.1.3	Create and add a digital signature.

CATEGORY	SKILL SET	REF.	TASK ITEM
		5.1.4	Be aware of the possibility of receiving fraudulent and unsolicited e-mail.
		5.1.5	Understand the term phishing. Identify common characteristics of phishing like: using names of legitimate companies, people, false web links.
		5.1.6	Be aware of the danger of infecting the computer with malware by opening an e-mail attachment that contains a macro or an executable file.
	5.2 Instant Messaging	5.2.1	Understand the term instant messaging (IM) and its uses.
		5.2.2	Understand the security vulnerabilities of IM like: malware, backdoor access, access to files.
		5.2.3	Recognise methods of ensuring confidentiality while using IM like: encryption, non-disclosure of important information, restricting file sharing.
6 Secure Data Management	*6.1 Securing and Backing Up Data*	6.1.1	Recognise ways of ensuring physical security of devices like: log equipment location and details, use cable locks, access control.
		6.1.2	Recognise the importance of having a back-up procedure in case of loss of data, financial records, web bookmarks/history.
		6.1.3	Identify the features of a back-up procedure like: regularity/frequency, schedule, storage location.
		6.1.4	Back up data.
		6.1.5	Restore and validate backed up data.
	6.2 Secure Destruction	6.2.1	Understand the reason for permanently deleting data from drives or devices.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.2.2	Distinguish between deleting and permanently destroying data.
		6.2.3	Identify common methods of permanently destroying data like: shredding, drive/media destruction, degaussing, using data destruction utilities.