

ICDL Cyber Security

Applying for this course:

To apply for this course, you should have completed compulsory schooling and ideally hold at least an 'O' Level standard of education in order to allow you to follow terminology and course notes with greater facility. In case of any difficulties regarding the entry requirements kindly contact us on qa.jobsplus@gov.mt.

Course Duration

This course is of 12 hours duration and consists of one Module (including 45-minute assessment)

General pedagogical guidelines and procedures for this course:

The delivery of this course will be mainly held through a series of practical, hands-on exercises. The trainer will be holding lessons with the learners in a computer lab set-up, which will consist of various discussions and client-specific case studies.

This course can also be delivered online. In such cases, the learner is required to have a working camera and a working microphone.

General assessment policy and procedures for this course:

The learner will be assessed through an ongoing assessment for learning by way of oral, written or practical exercises that will take place throughout each module, to assess and consolidate the learning being covered. The learners will also be given a mock test prior to the actual assessment.

The final assessment is carried out in one of the computer labs since the assessment needs to be conducted on a PC.

Module 1 Learning Outcomes - Cyber Security

✓ 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
--	--

Module Assessment:

A summative assessment will be held at the end of the unit. This will take the form of an online assessment based on multiple choice questions and simulations. This assessment will be on a Pass/Fail basis.

The duration of this assessment is of 45 minutes and the pass mark is that of 75%.