# 16hrs - ICDL Secure Use of IT (IT Security)

**Course Duration:** 2 days (16 hours), 9:00am - 6:00pm

## Course Outline:

***Security Concepts***

- Recognize Data Threats from various sources
- Understand Cybercrime and Hacking
- Understand the Confidentiality, Integrity & Availability of Information
- Identify privacy protection, retention and control principles
- Understand the term Identity Theft and its implications for Personal Security
- Methods of identity theft : skimming, pretexting and information diving
- File Security using encryption and it's limitation

***Malware***

- Definition and Function
- Recognized types of malware and how it works. Eg. Adware, ramsonware, keystroke loggin
- Use of Protection methods such as scanning and Anti-virus software
- Minimize risks of obsolete and unsupported software

***Network Security***

- Network administrator role to manage authentication, authorization, installing updates on Network Connections
- Different Wireless Security and limitations of WEP, WPA2, MAC and SSID
- Access Control by username, password, PIN, encryption and multi-factor authentication

***Secure Web Use***

- Methods to identify Authenticity of Website such as security certificate and validating domain owner
- Potential danger in Social Networking such as malicious links, cyber bullying and fraudulent content

***Communications***

- Identify fraudulent and unsolicited E-mails
- Security vulnerabilities in Instant Messaging and VoIP

***Secure Data Management***

- Securing and Backing Up Data using the physical locks and access control
- Distinguish types of Secure Destruction
- Non-permanent content deletion in social network, blog or cloud services