ICDL Arabia

4- CYBER SECURITY (MILITARY AND POLICE)

This module will help candidates understand the concepts essential to safeguard sensitive information and infrastructure from cyberattacks.

On completion of this module the candidate will be able to:

- Understand the key differences between military-grade cyber security and civilian cybersecurity
- Know the fundamentals of Cyber Defense, Federated Security and Cyber Terrorism
- Get sensitized to potentials risks such as cyber warfare and know why their profession makes their personal information highly sensitive
- Understand online risk, and basic security concepts, including data threats, the value of information, personal security, and file security
- Know what viruses, spyware, ransomware, and dark web are; know how to stay protected against threat actors online.
- Recognise globally leading cybersecurity technologies developed by homeland and military security
- Understand the basics of network security, including networks and connections, and wireless security
- Undertake information access control through various methods, and manage passwords effectively
- Use the web securely through browser settings, and adopting browsing best practices
- Secure communications channels such as Email, Social Networking, VoIP, Instant Messaging, and Mobile
- Implement secure data management practices, including securing and backing up data, and securely deleting/destroying data
- Understand common threats to citizens' security, including Online Addiction, and Online Radicalisation
- Understand the criticality of an incident response mechanism against cyber attacks
- Know what the vital components of a Cyber Security policy are, and understand the importance of cyber security policy-adherence audits

WHAT ARE THE BENEFITS OF THIS MODULE?

- Covers the key information and skills needed to safeguard sensitive information and infrastructure from cyber attacks
- Can be applied to various threat scenario where cyber security of critical military and police resources are at stake
- Certifies best practice in Cyber Security (Military & Police
- Developed with input from computer users, subject matter experts, and practising computer professionals from all over the world. This process ensures the relevance and range of module content

SYLLABUS OUTLINE

CATEGORY	SKILL SET
Introduction	• Anti-virus, anti-spyware, anti-ransomware and dark web
Protect	• Identify Risk • Secure personal information • Digital footprint • User authentication • Anti-virus, anti-spyware, anti-ransomware and dark web
Secure	• Military-grade cyber operations • Securing email, wireless communications, and social media • Encryption • Destruction of sensitive information • Internet of Things in military and police
Apply	• Secure online presence • Software and applications • Due diligence • Back-ups
Encourage	• Cybersecurity policy • Contingency and continuity • Incident Response • Culture of cyber security