

DOEACC Certified Information Security Associate (DISA)

As much as it is important to know how to use a computer, so is it necessary to know how to protect your computer on a network. The information on the computer is an asset and the risks are very high. There are no geographical limitations to computer attacks.

The certification outlines every thing about Information security that a computer user (at all levels) should know. This foundation level certification will enable an individual to take other higher level certifications in the field.

Objective:

The objective of this certification is to validate the awareness of an individual (any computer user) on Information security concepts and principles relevant in day to day usage of computers. A certified individual has proven his understanding on key concepts of Information security like the possible security threats and attacks, security concerns while using a computer, Internet, Email, wireless LAN etc. and their countermeasures.

Pre-requisites: Candidates are recommended to have experience using computers and Internet.

Syllabus

	Topics	Weightage
1	Information Security basics	35%
2	Workstation Security	25%
3	Internet Security	20%
4	Email Security	15%
5	Wireless Security	5%

(Approximate hours of preparation required is shown in the bracket)

1 Information Security basics

Basics of computer networks (12 hrs)

Network topologies

Network media

Introduction to TCP/IP

Understand the following information security concepts (8 hrs)

Confidentiality

Integrity

Availability

Accountability

Recognize the following attacks and vulnerabilities and specify the appropriate actions to take to mitigate vulnerability and risk (20 hrs)

Open Sharing

Password guessing

Unwise Programming

Social Engineering

Buffer Overflows

Denial of Service

Sniffing

IP Spoofing

- Malicious Code (Viruses, Trojan Horses, Worms)
- Security Technologies (20 hrs)
 - Encryption, Decryption, Digital signature
 - Firewall
 - VPN
 - Intrusion Detection
- Understand the concepts and uses of the following types of policies and procedures (8 hrs)
 - Security Policy
 - Computer Use Policy / Workstation Security Policy
 - Internet Use Policy
 - Mail Policy
- Understand the following concepts of disaster recovery (8 hrs)
 - Backup
 - Disaster Recovery Plans
- Understand the legal issues in Information Technology (4 hrs)

2 Workstation Security (24 hrs)

Be able to configure your computer and OS (Windows XP) with respect to the following

- Password protection – Pre boot, Screen saver, Creating Strong Passwords
- Creating User Accounts and groups
- File and Folder security
- File Sharing and Security
- Enabling and Disabling Services
- Updating OSs, Patches, Enabling automatic updates
- Anti Virus Protection, installing and configuring Anti Virus
- Protection against malicious code
- Spyware, protection against spyware
- Privacy Snoops, Removing trails
- Installing and configuring a Personal firewall
- Computer use - best practices

3 Internet Security (24 hrs)

Recognize and understand the following Internet security concepts

- Cookies
- Anonymous surfing, Phishing
- Customizing Browser Security Settings
- Shopping Safely – SSL and Certificates
- Understanding the concepts and configuration of a basic Firewall
- Content Filtering
- Internet use - best practices

4 Email Security (16 hrs)

Recognize and understand the following Email security concepts

- Precautions to take with e-mail file attachments
- POP3 vs. Web-based e-mail
- Blocking spam
- E-mail hoaxes and phishing attacks
- Email use - best practices

5 Wireless Security (8 hrs)

Understand the current wireless technologies and security concerns

WLAN detection

Eavesdropping

Suggested reference material

Main Reading

1. Fundamentals of Network Security by Eric Maiwald , Dreamtech Press
2. Absolute Beginner's Guide To: Security, Spam, Spyware & Viruses By Andy Walker, Publisher: Que
3. Computer Security Basics, 2nd Edition By Rick Lehtinen, Publisher: O'Reilly

Supplementary Reading

4. Foundations of Computer Security by David Solomon, Publisher: Springer
5. Security+ In depth by Paul Campbell, Publisher: Vijai Nicol Imprints Chennai
6. Digital Security – Concepts and Cases , ICFAI University Press, Hyderabad
7. How to do everything with Email, Spam and Viruses: Degunking your Email, spam and Viruses by Jeff Duntemann, Publisher: DreamTech Press New Delhi
8. Network Security Essentials- Applications and Standards, Publisher: Pearson Education

Recommended Web sites

1. <http://www.cert-in.org.in>
2. <http://www.sans.org>

Suggested Practical Exercises

Configuring TCP/IP, managing user accounts and groups, Sharing files and folders with security privileges, Enabling and disabling Services, Setting screensaver and BIOS passwords, choosing strong passwords, Installing and configuring Antivirus software and Anti spyware software

Installing and configuring POP3 based Email client, detecting Spam or Junk mails, Sending and Receiving encrypted emails.

Installing patches and updates, Enabling Automatic updates, Using Security Analyzer

Configuring Browser for disabling popups, enabling and disabling cookies, managing and using SSL certificates, configuring a personal firewall

Examination / Evaluation scheme

The evaluation will be done based on one examination of 90 minutes duration and will contain 100 objective type questions with maximum marks of 100. The questions will be in proportion to the weightage of the modules described in this curriculum.

The passing score is 55%. When there are differences in the difficulty level of different examinations, a mathematical procedure will be used to make the scores equal.

Sample Questions

1. The integrity Service provides for _____ of Information
 - a. Modification
 - b. Backup
 - c. Storage
 - d. Correctness
2. Digital signatures are a form of encryption that
 - a. Provides an unbreakable system
 - b. Provides for authentication
 - c. Provides for web encryption
 - d. Provides for file-level Encryption
3. Anti-virus Software identifies a virus by
 - a. Removing any code it cannot recognize
 - b. Comparing code to known virus signatures
 - c. Removing code based on unapproved vendors
 - d. Comparing code to a known vendor
4. The information stored on a client's computer by a web server is called a _____
 - a. File
 - b. Chip
 - c. Cookie
 - d. Folder
5. Which of the following correctly describes a Trojan Horse?
 - a. A program that propagates itself within a computer by infecting other programs residing on the computer system.
 - b. A program that spreads itself (without the help of any other program) over the network from one computer to another.
 - c. A program that appears innocent but capable of damaging a computer system when downloaded and executed.
 - d. A program that gets executed only when an event, such as a specific date and time occurs.
6. Which of the following can be used for secure exchange of email? [Choose 2 correct answers].
 - a. HTTPS
 - b. WEP
 - c. URL
 - d. PGP

