

The background of the lower half of the page is a dark, blurred image of a person in a business suit. Overlaid on this image is a grid of hexagons. Some hexagons contain white text related to cybersecurity, including "SAFETY", "ENC", "PASSWORD", "SECURITY", "DIGITAL", "DA", "PROTECTION", and "ANALYSIS".

INCREASING CYBER SECURITY AWARENESS

AGINFOSEC001



COURSE OVERVIEW

COURSE OUTLINE

Cyber security has emerged as a constant struggle for all organisations, and it is becoming more critical day by day with the average cost of a single data breach reaching \$3.62USD million globally.

Your company is only as strong as its weakest link, and those who have access to information and networks need to be security aware. With recent statistics indicating that human error is responsible for over a quarter of all data breaches, it has never been more important to be security aware from top-to-bottom to help prevent accidental breaches as well as to help protect against malicious and criminal activities.

This cyber security awareness course has been designed by Agilient to provide a guide that is suitable for the entire business. The aim of the course is to increase cyber security knowledge and awareness at all levels of your organisation as well as increase employee understanding of the ISO27001 standard to aid in your top to bottom security awareness.

BENEFITS

1. This course will provide guidance and best practice advice for cyber security within your organisation.
2. The course looks at various aspects of cyber security that will help to improve your organisation's security posture. This includes both physical and personnel security as they relate to securing data and networks.
3. A greater understanding throughout the organisation of both the cyber threat and risk environment for all employees.
4. Identifying the key concepts and benefits of ISO27000.

PRE-REQUISITES

There are no pre-requisites for this course.

WHO SHOULD ATTEND

- This course is suitable for all members of your organisation.

STUDENT LEARNING OUTCOMES

After this course, you will be able to:

1. Understand the broad concepts of cyber security and its importance to all organisations.
2. Understand what threat and risk mean in relation to Cyber Security.
3. Understand the general concepts of ISO27000 series of standards and how they relate to your organisation.
4. Understand the importance of being security aware to minimise potential data breaches.

TEACHING STRATEGIES AND APPROACH TO LEARNING

This is an online only course that is designed to be distributed to all members of your organisation. It should be used as part of a regular refresher programme within your organisation to increase and maintain cyber security awareness. There is a short quiz component that is used to reinforce the information presented in the course as well as provide assurance that the material was understood.

COURSE LOGISTICS

Location or delivery mechanisms

As this is a self-paced online training package, participants should ensure they give it their full attention and answer all of the final questions to their best ability to get the most out of it.

If the participant cannot answer any of the quiz questions, they should go back through the course and review the information before attempting the quiz again.

Duration

The course will take approximately 1 hour to complete.

Assessment

Although this training package is not pass/fail it is suggested that participants complete the quiz to their fullest to ensure that they get the most benefit for themselves and the company.

Course registration

You can register for this course by calling Agilient on 1300 341 692 or emailing us on securityinsights@agilient.com.au.

More information about Agilient can be found at our website.
See: www.agilient.com.au.

For more information on the course call Agilient on 1300 341 692 or email us on securityinsights@agilient.com.au.

COURSE CONTENT

Participants will be guided through the following topic areas:

1. Cyber Security– The concept of cyber security is defined and explained.
2. Physical Security – Physical security's relevance to cyber security is examined.
3. Risk – The concept of risk is explained.
4. Threat – The concept of threat and threat sources is explained.
5. ISO 27000 – the history and key benefits of the series of standards are examined.
The various clauses and controls are also explained.
6. User Responsibilities – Best practice behaviour for individuals to improve cyber security is explored.

PASSWORD

SAFETY

ENCRYPT

SECURITY

DIGITAL

DATA

Sydney Head Office:
Level 4, 655 Pacific Highway
ST LEONARDS NSW 2065
Australia

Melbourne Office:
Level 9, 440 Collins Street
Melbourne Vic 3000
Australia

Canberra Office:
Suite 117, 2 Endeavour House
Captain Cook Crescent
MANUKA ACT 2603

Brisbane Office:
Level 54, 111 Eagle Street
Brisbane Qld 4000
Australia