agilient

SECURITY AWARENESS TRAINING

AGGOVSEC001

COURSE OVERVIEW

COURSE OUTLINE

With a common goal of optimum security levels amongst all your staff, the organisation becomes almost uncompromisable. However, without providing annual security awareness training the risk of indifference creeping in rises within a workplace.

Staff that are inadequately training in security or careless actions can lead to loss of revenue, reputational damage, loss of competitive advantage and legal cost to name a few.

Studies show that with annual security awareness training the likelihood of an incident can be significantly reduced, providing your staff with the tools they need to identify and report threats.

This course will provide your organisation's staff with the knowledge, skill and practical experience they need to help reduce the likelihood of security incidents occurring within the workplace.

BENEFITS

1. All staff within your organisation will be aware of the organisation's security culture, security policies and procedures including the roles they play which will help reduce the prevalence of security incidents and the associated cost.

2. This course will provide awareness to all staff of the importance of reporting incidents and suspicious behaviours, and how maintaining or improving the quality of reports assists to enhance the protection of people, property and critical assets.

PRE-REQUISITES

There are no pre-requisites for this course.

WHO SHOULD ATTEND

- Organisational Executives
- Managers and Supervisors
- Frontline Staff
- Contractors and Volunteers

STUDENT LEARNING OUTCOMES

After this course, you will be able to:

1. Define what security is and how security improves your work environment.
2. Identify who is responsible for security within your organisation and understand the importance of incident reporting.
3. Provide details of the main threats to your organisation and explain the importance of physical and information security.
4. Create passwords that can assist with defeating attempts to infiltrate your IT network.
5. Have a clear understanding of the security roles and culture within your organisation and how that assists in protecting all staff while working in facilities, in the field or on travel overseas.

TEACHING STRATEGIES AND APPROACH TO LEARNING

This course will provide all staff with an understanding of the importance of security within your organisation with real-world examples of current threats and security incidents. These examples will be provided through the use of case studies, audio-visual snippets, quizzes and practical workshops, and will offer best practice guidance for ensuring the adherence to security policies and procedures and nowledge of how to maintain updated awareness of current security trends.

COURSE LOGISTICS

Location or delivery mechanisms
This program will be delivered as an instructor led course for all organisation staff either in-house or at a pre-determined location.

Duration
The course will take approximately 4 hours to complete.

Assessment
Although this training package is not pass/fail it is suggested that participants complete questionnaires and tests 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 : 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. Define Security – Understand what constitutes security and how it helps to improve your working environment.
2. Threat and Incident Trends – Creating awareness of the ever-changing threat environment including terrorism, cyber crime, and espionage and the impacts they can have on an organisation.
3. Security Culture and Roles – Knowing what your security rights and responsibilities are within your organisation in relation to the key organisational policies and procedures.
4. Physical Security – Understanding the requirement to protect valuable assets through basic lock-up procedures and the layered security approach.
5. Information Security – Protecting your organisation and client's information and intellectual property from unauthorised access, data breach requirements and the use of a clear desk policy.
6. Creating and Securing Passwords – How to create a strong password, things not to do to ensure your password stays protected and tools that can assist you.
7. Overseas Travel – Protecting your organisational interests while travelling overseas with robust travel policies for business and personal travel.
8. Personnel Security – Personal safety and security measures for your staff to ensure a safe work environment both while working in your facility or in the field.
9. Staff Separation – This section will identify strategies that can be used to protect intellectual property when staff leave the organisation.
10. Incident Reporting – Identifying reportable incidents and suspicious behaviours that must be reported and the information required to improve security procedures and reduce repeats.

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

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

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

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