Vigil CyberSec Inc. Cybersecurity Awareness Training

Course Outline

Session 1 – Information security risks

Participants successfully completing this Session should be able to:

1. Explain what information security means.
2. Define the four aspects of information security.
3. Understand their role in supporting information security.

- What is information security?
- Why is information security important?
- Consequences of security breaches
- the essential role you play: highlights the importance of everyone in the workplace doing their part to support information security policies and procedures.

Assessment: *comprising multiple choice questions to evaluate participants' understanding of key concepts of the Session*

Session 2 – physical security

Participants successfully completing this Session should be able to:

1. Define what is meant by physical security.
2. Give examples of physical security measures in the workplace.
3. List some good work habits that help maintain physical security.

- What is meant by physical security with examples relevant to the workplace environment
- Importance of developing good work habits that help to maintain physical security.
- Outlines of some of the information security risks that can be encountered when working outside the workplace, for example working from home or travelling to other locations.
- Particular risks that are associated with carrying electronic devices such as smartphones.

Session 3: computer and network security

Participants successfully completing this Session should be able to:

1. Recognize the importance of complying with computer and network policies.
2. List some examples of the risks posed by computers and networks.
3. explain the meaning of technical terms such as 'virus', 'malware', 'encryption' and 'firewall'.
4. Understand the importance of reporting and responding to security incidents quickly.

- Importance of following the proper workplace policies and procedures, even if the reasons for them are not understood.
- Non-technical explanation of key terms related to computers and computer networks.

- Importance of reporting computer and network security issues and responding quickly.

Session 4 – Communications security

Participants successfully completing this Session should be able to:

1. Recognize what is meant by communications security.
2. Explain some of the particular risks associated with email.
3. Put into practice some tips to avoid communications security breaches.

- Concept of communications security with examples of what it covers.
- Risks that can be posed by email use, such as malicious attachments, misleading links, and phishing attacks.
- Information security risks to be aware of when communicating outside the workplace (for example, working from home or in public places).

Session 5 – Personnel security

Participants successfully completing this Session should be able to:

1. Explain what is meant by personnel security.
2. List the main areas of risk associated with personnel security.
3. Understand what social engineering is, and recognize the threat is can pose.

4. be aware of the risk that deliberate acts by personnel can cause security breaches.

- Concept of personnel security and outlines four main areas of risk associated with it.
- Concept of social engineering and how it can be used to breach information security.
- Risk posed by personnel deliberately acting in ways that breach security, and that everyone should be alert to this risk.

Training Fees

Option 1: **KES 2,000 per session**. Maximum sessions per day is 3.

Option 2: **KES 1,500 per hour**. Maximum hours per day is 4.

N:B a session can take more than 1 hour.