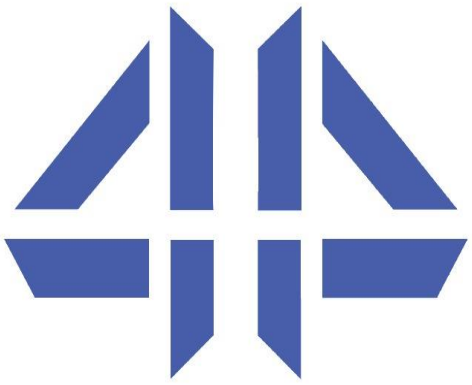
V1.0

Training Program on

Information & Data Security Basics



What is Information & Data Security?

Information and data security refers to the practice of protecting sensitive and confidential information from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes a range of practices, technologies, and policies that are used to ensure the confidentiality, integrity, and availability of data and information assets. Information and data security aims to prevent unauthorized access to data and information, and to ensure that data and information are only accessed by authorized individuals or systems. It is a critical component of any organization's overall security strategy and is essential to protect against cyber threats and data breaches.

Why is Information & Data Security?

- Protecting sensitive information: Sensitive information such as financial records, customer data, and personal information must be protected to prevent unauthorized access or misuse.
- Regulatory compliance: Failure to comply with specific industry-centric regulations can result in significant financial penalties and reputational damage.
- Intellectual property protection: Companies often have proprietary information that must be protected to prevent theft or unauthorized use.
- Mitigating risk: Protecting data and information can help mitigate the risk of data breaches, cyber-attacks, and other security incidents that can result in financial loss, legal liability, and damage to an organization's reputation.
- Business continuity: Ensuring the security of critical data and information is essential for maintaining business continuity in the event of a security incident or disaster.

Why learn about Information & Data Security?

- Protect company assets: To ensure the confidentiality, integrity, and availability of that data.
- Compliance requirements: Failure to comply with specific regulatory requirements can result in significant financial and reputational damage.
- Protection of personal data: Be aware of the importance of protecting their own personal data, as cyber threats can also target individual employees.
- Increased awareness: Learn how to prevent potential cyber threats, which can help in protecting themselves and the organization.

Audience

The audience for this training program would typically be individuals who are interested in or working in information technology. This may include IT professionals, system administrators, network engineers, or software developers. It is also for the students who are likely to join large organizations in entry-level positions.

Learning Objectives:

- Understanding the fundamental concepts and principles of information and data security, including confidentiality, integrity, availability, and access control.
- Familiarizing oneself with different security frameworks and standards, such as NIST and ISO 27001.
- Understanding data protection regulations and how to comply with them.
- Understanding the importance of security and how to use within the organization.

Candidate Prerequisites

- Basic computer skills: Candidates should have a basic understanding of computer operations, such as using a mouse, keyboard, and operating system.
- Basic understanding of the importance of data protection

Lab requirements for the classroom:

(Note: The requirements are tentative and may change based on the final content)

Software:

- Microsoft Windows 11 Operating System

Hardware:

- Desktop or a laptop computer per student with a good internet connection

Training Outline:

Day 1

Session 1: Introduction to Information and Data Security

- *Overview of information and data security Key terminology and concepts Activity: Password creation and policy implementation on a Windows machine*

Session 2: Basics of Information Security

- *Confidentiality, Integrity, and Availability (CIA) Security frameworks and standards: NIST, ISO 27001 Activity: Identifying and classifying data based on CIA principles*

Session 3: Access Control and Authentication

- *Overview of access control and authentication User authentication methods Activity: User account creation and access control implementation on a Windows machine*

Session 4: Network Security

- *Overview of network security Types of network attacks and threats Activity: Configuring a basic firewall rule on a Windows machine*