

IT SECURITY AWARENESS – COURSE CONTENT

Duration: Two hours.

- **Introduction to Information security.**
 1. What is Information Security.
 2. Compliance requirements from regulatory bodies.
 3. Data protection.
 4. Clean Desk policy.
 5. Corporate Security Policy.
 6. Protect your company data.
- **On-line security threats**
 1. What information to be protected.
 2. Virus and worms.
 3. Social Engineering.
 4. Phishing.
 5. Acceptable User policy and Ethics
 6. Password Management.
 7. Protecting Mobile Data.
- **IT Security Incidents.**
 1. What is security Incident.
 2. Actions taken in case of incident
 3. How to report an incident.
 4. Security measures.
- **Information Protection.**
 1. Information storage
 2. Information distribution
 3. Information disposal.
 4. Confidentiality, integrity, and availability of In
- **Social Media**
 1. Use of social media platform in corporate.
 2. Advantages and disadvantages of Social media in corporate Environments.

Outcome of the Training: A security awareness program is a formal program with the goal of training users of the potential threats to an organization's information and how to avoid situations that might put the organization's data at risk.