Effective Information Security Management

Duration: 5 Days

Language: en

Course Code: PI1-106

Objective

Upon completion of this course, participants will be able to:

- Protect your business' personal information.
- Create policies and procedures to empower your team to remain secure.
- Inspire a passion for security and help others understand its importance.
- Assess the risks to your data and devise mitigation procedures.
- Develop a log of security incidents and create a 'lessons learned' process to aim for

continuous improvement.
- Understand threats and how to defend your service against them.

Audience

This course is designed for anyone responsible for information security, process design, or contractual deployment of new IT systems. It would be particularly beneficial for:

- Project Managers
- Business Owners
- Change & Control Managers
- Financial Managers
- IT Managers
- Technical Support Teams
- IT Security Auditors

Training Methodology

This course uses various learning methods, including seminars to discuss the effects of data loss and practical group exercises to uncover potential risk areas and devise solutions to mitigate security breaches.
You will be provided with real-life case incidents to discover the implications of data breaches and create solutions for data recovery and process change to prevent further data spread.

Summary

The information and data collected from customers, employees, and external data sources are essential to keeping any business running. They help to keep track of customer accounts, reach out to new potential customer bases using intelligent data sets to select the right target market and understand our employee and resource costs to create a cost-benefit analysis for any new projects effectively.
Because information is unique to any business and so important to help it run effectively, it may also be incredibly valuable to external parties. This can put your data at risk through technological bugs or hackers, external sources that may be affiliated with your business, or even internal employees and partners that may innocently remove data from secure places to put you at risk.
To protect your business from security risks, you must empower your management

personnel to understand the implications of data loss and the importance of enforcing strong security processes and procedures.

Course Content & Outline

Section 1: The Importance of Data Security
The purpose of information security.

- Understanding why your data is valuable.
- Your water-tight privacy policy.
- Data removal under GDPR.
- Information confidentiality and integrity.

Section 2: Understanding Areas of Risk

- IT systems, phone records, and social media.
- Reacting to audits and how to keep accurate records.
- Threats, risks, and countermeasures.
- The legislation around data collection.
- ISO 27002.
- Your obligations towards public protection.

Section 3: Evaluating IT Security Measures

- Your key data and encryption.
- 2-step verification methods.
- Your digital signature.
- Identifying your key information assets.
- Information security management systems (ISMS).
- The problems of large-scale distribution.

Section 4: Secure Communication Methods

- Secure file sending and email encryption.
- Communicating with your team on a secure platform.
- Your data integrity.
- Communicating with partners or stakeholders.
- Customer communication and fail safes.

Section 5: Physical Security with Your Team

- Creating a passion for security.
- Motivating a team to monitor their own movements.

- Building security.
- File security and data protection.
- Computer and equipment security.
- Homeworking security precautions.
- Using the hash function.

Section 6: Public Key Infrastructure

- Social engineering.
- What is cryptography?
- Cryptography algorithms - DES, Triple DES, and AES.
- Information security governance.
- Your policies - are they effective?

Section 7: Risk Mitigation & Process Change

- Creating an effective risk management process.
- Assessing risks and prioritising changes to protect information.
- Working with the ICO.
- Obtaining security certificates.

Section 8: Incident Response & Recovery

- Examples of incidents and recovery scenarios.
- The implications of data breaches.
- Planning a security incident response.
- Removing the potential for a single point of failure.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Assessment Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

IT & Computer Application, Management & Leadership, Technology, AI, Data and Visualisation

Tags

IT, technology, Information Security Management, information technology, IT security, data protection

Related Articles

Navigating Cyber Threats: A Full Guide to Risk Management

In the digital era, cybersecurity risk management is paramount. This blog post delves into the process of identifying, assessing, and mitigating cyber risks. Learn about AI-driven solutions, UK laws, and how to integrate risk management with your business objectives.

YouTube Video

https://www.youtube.com/embed/6oN2C8hSmq4?si=kQoOoLBahQzoHzeo