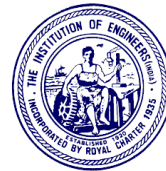




Engineering Staff College of India

Autonomous Organ of The Institution of Engineers (India)
Old Bombay Road, Gachi Bowli, Hyderabad – 500 032. Telangana, India



INFORMATION TECHNOLOGY DIVISION

PROFESSIONAL DEVELOPMENT PROGRAMME



Cyber Security Policies & Crisis Management Plan

11 – 13 Oct 2023

At , Shimla Himachal Pradesh

Introduction

In today's world, Information Technology is playing a pivotal role in business, most of the organizations depend on different kinds of Information Technology solutions and applications, say, e-commerce, e-governance, e-banking etc.. Rising incidents of cyber attacks, such as hacked websites, breached networks, and denial-of-service attacks, have turned cyber security from just an operational challenge into a business Challenge. It's almost impossible to shield your business completely from cyber attacks, but what you can do is create an effective response plan that instructs your IT team on how to respond to an attacks.

Having a Cyber Security Policy & Crisis Management Plan will help you respond more quickly to cyber attacks, deliver consistent communication to internal and external stakeholders, and take timely remedial actions..

A cybersecurity policy, however, can mean different things for different organisations. It can take different shapes or forms, depending on the type of organisation, nature of business, operational model, scale etc

Objectives

- This instructor-led course will provide you knowledge in Cyber Security Policies
- This Course provides in-depth knowledge to Create Cyber Security Policies & Crisis Management Plan for your organization.

Course Coverage

- **Cyber Security Overview**
- Types of Attacks
- Security Threats and Vulnerabilities
- **Importance of Cyber Security policy**
- ISMS 27001 Implementation
- Identify and Prioritize Assets, Risks, Threats
- Password Policy
- Outline email security measures
- Explain how to handle sensitive data
- Set rules around handling technology
- Set standards for social media and internet access
- Acceptable use policy (AUP)
- Access control policy
- Business continuity plan
- Data breach response policy
- Disaster recovery plan
- Remote access policy
- Prepare for an incident
- Keep your policy up-to-date
- **Create a Cyber security Crisis Management Plan**
- Form an emergency cybersecurity incident response team
- Define what a cybersecurity crisis means to your organization
- Create escalation process flowcharts for crisis situations
- Create cybersecurity crisis communication templates
- Create RACI charts and list emergency contacts for speedy communication and collaboration

Methodology

Methodology of the programme includes class room sessions with Lecture / Discussion with Hands- on Practical, with tools, audio visual aid, bench marked video shows, Chalk & Talk sessions, group discussions, case studies, debates, sharing of experiences etc. All the sessions will be interactive demanding active participation from all the members

(An ISO 9001:2015 Certified, AICTE & CEA Recognized Institution)

Centre for Promotion of Professional Excellence

Target Participants

- System Administrators / Network Administrators/ IT Managers
- IT / OT Professional of Power Sector Companies
- The program is designed for all IT professionals of PSUs/ Power / Govt Organizations involved with Cyber Security.

Programme Dates & Timings

Dates: 11 – 13 Oct 2023

Session timings will be from 10:00 – 17:00 hrs. with 15 Minutes Tea break., One Hrs Lunch Break

Venue:

At Shimla, Himachal Pradesh

Course Director

Mr. Syed Azgar, MBA(IT), RHCE, MCSA
Sr Faculty & Head IT,
Information Technology Division,
Engineering Staff College of India, Hyderabad.

Course Fee for Offline Training

₹ **18,000/- (Non Residential Fee)** per participant. Fee includes course material, course kit, Lunch, Tea / Coffee and Snacks during the actual days of the training program.

₹ **35,000/- (Residential Fee)** per participant. Fee includes course material, course kit, single / Double AC accommodation as per availability, Breakfast, Lunch, Dinner, Tea / Coffee and Snacks during the actual days of training programme.

Important Note : We will confirm 20 days before the commencement of the program, Please book your tickers & accommodation after receiving the confirmation letter.

GST @18% is to be paid extra and above the training fee as training. **PAN Card No.** AAATT3439Q. **GST No:** 36AAATT3439Q1ZV, **HS No.:** 999293 (under commercial training or coaching services – clause 65(105) (ZZC) of Finance act – 1994).

Programme fee is to be paid in in favour of “**THE INSTITUTION OF ENGINEERS (INDIA) – ENGINEERING STAFF COLLEGE OF INDIA**” in the form of demand draft payable at Hyderabad. Alternatively the payment may be made by **Electronic Fund Transfer (EFT)** to ESCI – **Axis Bank** A/c No. **912010049234564** with The Axis Bank Ltd, Old Mumbai Hwy, Cyberhills Colony, P Janardhan Reddy Nagar, GachiBowli Hyderabad-500032 by NEFT/ RTGS/ IFSC Code No. UTIB 0000733 – MICR No.500211020. **While using EFT method of payment, please ensure to communicate us your company name, our invoice reference and programme title.**

Registration

Online registration shall be available on ESCI web portal <https://escihyd.org/division/it>

To register manually please send your nominations giving details of name, designation, contact address, email address, mobile no, telephone and fax number of the participant along with the details of mode of payment of fee, addressed to : it@escihyd.org

A Certificate of participation will be awarded to each participant on conclusion of the programme

Information Technology Division, Engineering Staff College of India

Gachi Bowli, Hyderabad – Telangana 500 032

Phone: 040 – 66304100 (EPABX) 66304123/24/25 (Direct), 8886661060 **Fax:** 040 – 66304103

Email: it@escihyd.org, **web portal:** www.escihyd.org