Enhance awareness about the importance of information security is to protect yourself and your company!

- How to enhance employees' awareness about the importance of information to be kept confidential, such as: personal information, business information, etc. and impact of information leakages?
- How to handle information leakages due to cyber attack, phishing, etc. and keep employees highly vigilant while information theft is getting more and more cunning and complex?
- How to build and operate the information security policy for company, so that there's a clear system for employees to comply with?

⇒ "**Enhance awareness of information security**" training and **"Building information security policy"** consulting program shall support employees and company to enhance awareness, and provide knowledge, skills and solutions to use internet, email, social media and internal network safely and confidentially.

ENHANCE AWARENESS OF INFORMATION SERCURITY

Target: Vietnamese staff, internal trainer, Information Security Officer

Objective

- Understand basis of information sercurity, such as confidential information, sercurity hole, cyber attack, etc.
- Identify risks to personal and company information sercurity, and develop specific countermeasures to prevent the risks
- Enhance awareness of protecting personal and company data and information from risks of internet, computer and data storage devices usage

TRAINING CONTENT (1 day)

Part 1: What is information security?

1. Overall of information security
2. Types of personal and company confidential information
3. Importance of personal and company information security

Part 2: Safe usage of computer and external portable devices

1. Safe usage of computer: ID, Password, copyright software
2. Overall of threats: computer virus, malware/ spyware, security holes, etc.
3. Notes of computer usage: actions when leaving your computer, using computer out of office, etc.
4. Usage of external portable devices

Part 3: Safe usage of email and internet

1. Notes for sending and receiving email safely
2. Detection and countermeasures to phishing
3. Notes of "web surfing" and online transaction
4. Notes of using social media
5. Threats of wireless LAN
6. Precautions for remote work
7. Protection from social engineering attacks

Part 4: Internal threats of information leakages and countermeasures

1. Common threats and countermeasures
2. Solutions to information leakages

Part 5: Summary and Action Plan

"Building information sercutity policy" Consulting

Objective:
Support client to develop information sercurity policy to ensure the confidentiality of company's information and document

Procedure of service:

Aimnext proposes information sercurity policies based on client's requests → Client checks and gives feedback → Aimnext revises based on client's feedback → Finalize "Information sercurity policy"

We can customize the service based on client's issues and request.

Sample of "Information sercurity policy"

1. Overall
   - What is information sercurity?
   - Company's responsibilities
   - Employees' responsibilities
2. Rules of document usage
   - Hard-copy document management
   - Solf-copy document management
3. Computer usage and management
4. Software usage management
5. Email usage management
6. Password management
7. Usage management of external drives

AIMNEXT VIETNAM CO., LTD.
Nam Giao Building 1, 261 – 263 Phan Xich Long,
Ward 2, Phu Nhuan District, Ho Chi Minh City
TEL : (028) 3995 8290
FAX : (028) 3995 8289
Email : training-vn@aimnext.com
URL : www.aimnext.com.vn