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

Obje ctive	▪ Understand the importance of personal information, company's information and information security. ▪ Identify information security threats of individuals and company's information, and develop specific countermeasures to prevent the risks. ▪ Understand the principles and basic steps when dealing with information leakage incidents.

TRAINING CONTENT (1 day)

Part 1: What is information security?
1. What is personal information and company's information?
2. Importance of company's information
3. What is information security?

Part 2: Threats against the enterprises' information sercurity
1. Malware: computer viruses, malware, spyware, etc.
2. Phishing
3. Zero-day attack
4. Social engineering attacks
5. Human errors

Part 3: Information security countermeasures
1. Notes for using computer
2. Notes for using external portable devices
3. Notes for sending and receiving email safely
4. Notes of "web surfing" and online transaction
5. Threats of wireless LAN
6. Notes for using social media
7. Precautions for remote work

Part 4: Dealing with information leakages
1. Principles of troubleshooting
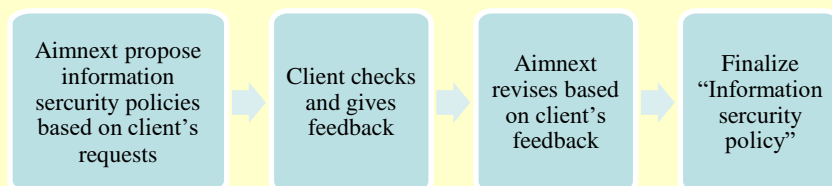2. Process of dealing with information leakages

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 propose 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