



# Security Tips for IT Protection

## - Convergence of physical and logical access control systems



Protected  
by  
**SECOM**

Historically, providing physical protection of computer systems has been the extent of the integration of physical and logical security. For example: Data center systems are protected by firewalls on the network, antivirus software on the servers, intrusion detection, etc. The server room is also physically secured from unauthorized access using door access control, alarm controls, fire suppression, temperature control, uninterrupted power supply – UPS, and etc.

If the physical access to the computer system can be monitored and controlled, gaining logical access to the information on that computer system is regulated and safeguarded. In this era of virtual communications, the physical security of your network is vital for your business. Controlled areas should be made accessible only to support personnel, and back-ups must be kept of all essential data in case of physical damage to the system. Here are some tips on how to equip yourself in the battle to prevent physical thefts, logical threats such as viruses, worms and other threats away from your computer.

3 types of control to prevent and secure your IT in your organization

### 1. Administrative controls

- Comprised of approved written policies, procedures, standards and guidelines.
- Form the basis for the selection and implementation of logical and physical controls.

### 2. Physical controls

- Monitor and control the environment of the work place and computing facilities. Alarm system, CCTV, door access control are in place to take over the guardian tasks
- Prevent unauthorized access into the computing premises such as server room, data centre by equipped with alarm system and monitoring systems, setting up access time zone, authorized personnel.
- Consider the use of CCTV cameras with monitored screens and video recorders.
- Be particularly wary of the danger posed by roof/ceiling access and windows without locked grills.
- Install an intruder alarm system.
- Install panic buttons at key locations throughout the premises.
- For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, temperature control systems, cameras, fencing, security guards, cable locks, etc.

### 3. Logical controls

- Use of software and data to monitor and control access to information and computing systems.
- Back up data regularly by saving it to disks or CDs. In the event that a virus does infect your computer, this will prevent the loss of important information.
- For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption.
- Firewall products keep intruders away from databases containing private & confidential data, and prevent people from viewing or saving private information in attachments when using public computers.
- E-mail security products help to block outbound messages containing confidential text or files and protecting against harmful viruses and other attacks.
- Rights management technologies prevent employees from copying or printing sensitive files.
- Deploying information leak-prevention tools (also known as data loss-prevention tools) monitor messages and files moving across your network and stop employees from distributing confidential information inappropriately.



**SECOM**  
Access Control

Equipped with  
**SECOM**  
Alarm System



Link to  
**SECOM**  
Control Centre

If you do not wish to receive e-Newsletter from us, just email to [sales@secom.com.my](mailto:sales@secom.com.my) with subject 'Unsubscribe SECOM e-Newsletter'