

General

1. What is Information Security?

Information Security refers to all aspects of protection covering information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. The aim is to provide confidentiality, integrity, and availability of information systems and the information within.

- 1) Confidentiality: only authorised persons are allowed to know or gain access to the information stored or processed by Information Systems in any aspects;
- 2) Integrity: only authorised persons are allowed to make changes to the information stored or processed by Information Systems in any aspects;
- 3) Availability: Information Systems should be available to users at any given or specified period of time.

2. What is IT Security?

There is no exact definition, but the term is generally used to refer to protection of any IT infrastructure, information systems and related resources with respect to confidentiality, integrity and availability.

3. How can we ensure IT Security?

It is always a good idea to use a systematic approach to IT security.

First, the security requirements of the organisation should be clearly identified and understood.

Second, a clear security policy and procedures should be established and enforced.

Third, periodic security risk assessments and audits should be conducted, as well as continuous monitoring of systems to ensure that effective and efficient security policies and procedures are properly implemented.

4. How can I identify my organisation's security requirements?

As a business owner, you should consider the value of your information systems and other IT assets in terms of the daily business of the organisation in order to determine the appropriate level of security. The impact of any security incident to your reputation, as well as the proper continuity of your business, should be considered. A process called risk analysis is normally used to identify what assets to protect, their relative importance to the proper operation and business of the organisation, and the priority ranking or level of security protection. The result should be a well-defined list of security requirements for your organisation.

5. What is a security policy? How is it related to security standards, guidelines and procedures?

A security policy sets the standards for a set of security specifications. It states what aspects of Information Security are of paramount importance to the organisation, and thus a security policy can be treated as a basic set of mandatory rules that must be observed. The policy should be observed throughout the organisation and should be in accordance with your security requirements, and your organisation's business objectives and goals.

Security standards, guidelines and procedures are tools that can be used to implement and enforce a security policy. More detailed managerial, operational and technical issues can be addressed. These documents provide detailed steps and advice to assist users and system administrators in complying with the requirements in security policy. Standards, guidelines and procedures may require more frequent reviews than the security policy itself.

6. What should be considered when drafting a security policy?

A security policy should be practical, and work for your organisation. The following should be considered:

- The sensitivity and value of the assets that need to be protected
- The legal requirements, regulations and laws of the Government in your jurisdiction
- Your organisation's goals and business objectives
- The practicalities in implementation, distribution and enforcement

7. Who should be involved in the development of a security policy?

Developing a security policy requires the active support and ongoing participation of individuals from multiple ranks and functional units within the organisation. A working group or task force can be formed to develop the policy. In general, this group can include empowered representatives from senior management, technical personnel, operational personnel, and business users. Senior management represents the interests of the organisation's goals and objectives, and can provide the overall guidance, assessment and decision-making. Technical personnel can provide technical input and feasibility assessments for

various security mechanisms or aspects of technology. Business users represent the users of related systems who may be directly affected by the policy.

Sometimes, a third party consultant may need to be involved, to review the draft security policy.

8. How can I develop a security policy for my organisation?

First, identify a group of personnel who should be involved in developing the security policy. Second, make all necessary plans for activities, resources required and schedules. Third, determine the core security requirements, and establish the organisation's security policy accordingly. A draft security policy should then be reviewed and agreed by various stakeholders. The process of drafting might require several iterations before a security policy can be established.

As technologies, business environments and security requirements change over time, the security policy should be reviewed periodically (e.g. once every two years) in order to keep abreast of changes.

9. What should be included in a security policy?

An IT security policy must address procedures and behaviors that can be changed. It is also important to recognize that there are always **exceptions** to every security rule. Keep the policy as **flexible** as possible in order that it remains viable for a longer time.

The **CONTENTS** of an IT security policy should address the following questions:

- What are the policy objectives and scope?

- Which information resources need to be protected?
- Who does the policy affect?
- Who exactly has what authorities and privileges?
- Who can grant authorities and privileges?
- What are the minimum measures required to protect information resources?
- The expectations and procedures for reporting security violations and crimes
- Specific management and user responsibilities for ensuring effective security
- The effective date of the policy, along with revision dates or appropriate review intervals

10. What are the benefits of a security policy?

With a security policy in place, all staff will be able to clearly understand what is and is not permitted in the organisation relating to the protection of information assets and resources. This helps raise the level of security consciousness of all staff. In addition, a security policy provides a baseline from which detailed guidelines and procedures can be established. It may also help to support any decision to prosecute in the event of serious security violations.

11. What should I consider when implementing a security policy?

Even if a security policy has obtained formal approval, putting a good security policy in place is another story. This requires a series of steps:

Security Awareness & Training

Security Awareness is crucial to ensuring that all related parties understand the risks, and accept and adopt good security practices. Training and education can provide users, developers, system administrators, security administrators and

related parties with the necessary skills and knowledge needed to implement appropriate security measures.

Commitment and communication

No policy can be fully implemented unless all users and related parties are fully committed to complying with it. Good communication is ensured if users and third parties:

- are informed about the policy through briefings or orientations when they join the organisation
- are invited to participate in developing policy proposals
- are trained in the skills needed to follow policies
- feel that security measures are created for their own benefit
- are periodically reminded and refreshed on new issues
- have signed an acknowledgement agreement
- are provided guidance on implementing the policy

Enforcement And Redress

This refers to the task of enforcement of rights arising from implementation of the policy, and redress for any violations of those rights. Organisations should set up procedures to provide prompt assistance in investigative matters relating to breaches of security.

On-going Involvement of All Parties

An effective security policy also relies on a continuous exchange of information, consultation, co-ordination and co-operation among users and business units. Injection of knowledge on standards, methods, codes of practice and other expertise on security from external organisations will also help keep the security policy up-to-date and relevant.

12. What is meant by a security assessment?

A security assessment is the process of evaluating the security of an IT environment, including the network and the information systems. Security administrators or third party consultants usually use software tool called a vulnerability scanner specially designed to search out the security risks and vulnerabilities on internal hosts and workstations. In addition, adequacies in operation procedures would also be evaluated as part of the security assessment.

In general, a security risk assessment is conducted at the very beginning of a system deployment project to identify what security measures are required; or when there is a major change to the information assets or their environment. As new security vulnerabilities emerge from time to time, security risk assessments should be conducted regularly, for example once every two years.

13. What is a security audit?

A security Audit is a process or event where the IT security policy or standards are used as a basis to determine the overall state of existing protection, and to verify whether existing protection is being performed properly. It aims to determine whether the current environment is securely protected in accordance with the defined IT security policy.

Before performing a security assessment or audit, the organisation should define the **scope** of the security audit, and the **budget** and **duration** allowed for the assessment / audit.

14. How often should a security audit be performed?

A security audit only provides a snapshot of the vulnerabilities in a system at a particular point in time. As technology and the business environment changes, periodic and ongoing reviews will inevitably be required. Depending on the criticality of the business, a security audit might be conducted yearly, or every two years.

15. Who should perform a security audit?

A security audit is a complex task requiring skilled and experienced personnel; it must be planned carefully. To perform the audit an independent and trusted third party is recommended. This third party can be another group of in-house staff or an external audit team, dependent on the skills of the internal staff and the criticality / sensitivity of the information being audited.

16. What is an IT security incident?

An IT security incident is an adverse event in an information system and/or network that poses a threat to computer or network security with respect to availability, integrity and confidentiality. Such incidents can result in the destruction of data and disclosure of information.

However, adverse events such as natural disasters, hardware/software breakdowns, data line failures, power disruptions, etc. are generally excluded.

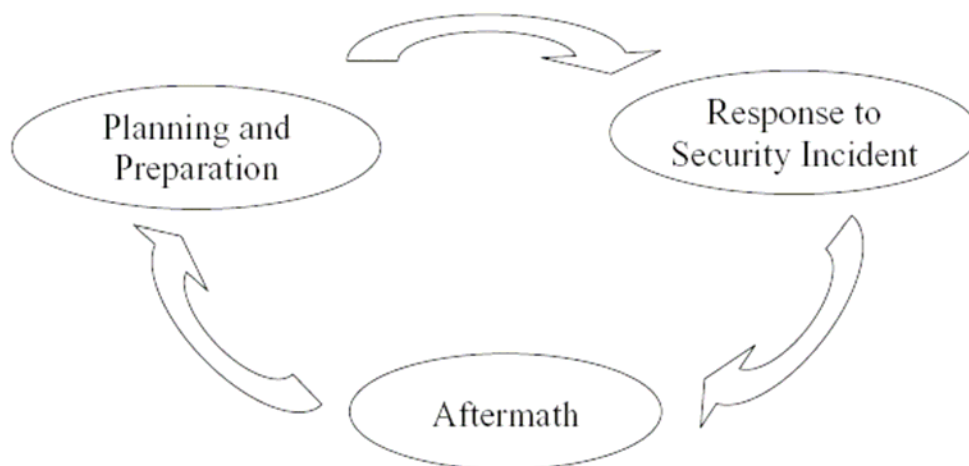
17. How can I handle a security incident?

Security incident handling is a set of continuous processes governing the activities before, during and after a security incident occurs.

Security incident handling begins with planning and preparing the right resources, then developing proper procedures to be followed, such as escalation and security incident response procedures.

When a security incident is detected, a security incident response is initiated by responsible parties using predefined procedures. A security incident response represents the activities or actions carried out to tackle the security incident and to restore the system to normal operation. Specific incident response teams are usually established to perform certain tasks within the security incident.

When the incident is over, follow up action is taken to evaluate the incident and to strengthen security protection against a recurrence. Planning and preparation tasks will be reviewed and revised accordingly to ensure that there are sufficient resources available (including manpower, equipment and technical knowledge) along with properly defined procedures to deal with similar incidents in future.



18. What is an intrusion, and what is intrusion detection?

An intrusion is a set of actions that attempt to compromise the availability, confidentiality and integrity of an information system.

Intrusion detection is the methodology by which intrusions are uncovered. This includes the detection of external intruders breaking into a system as well as internal users misusing system resources.

19. Why do I need an intrusion detection system (IDS) or an intrusion prevention system (IPS) if my network already has a firewall?

Firewalls are only part of a total integrated security system, and they have limitations. Firewalls can neither alert you to ALL intrusions, nor stop ALL security breaches. Unless you are constantly monitoring for intrusions, you cannot know for sure if your firewall is blocking all intrusions. IDS / IPS can be installed and used at strategic locations to continuously collect and examine information for suspicious activity 7 days a week, 24 hours per day. IPS also provides an active response system to stop the source of attacks or to minimize the impact of any attacks.

20. What are the limitations of an intrusion detection system?

An intrusion detection system cannot help you to solve or fix all security incidents. It cannot tell you exactly who and how the attack occurred, nor can it tell you the intention of the attacker. It can only provide information about the origin of the

attack and the IP address of the originating attack. You will need to analyse all relevant logs in order to identify the real attacker.

21. What is a network firewall, and what can a firewall protect my systems against?

A firewall is a system that enforces an access control policy between two networks. In general, a firewall is used to block network traffic coming from outside the network to the inside, and permit traffic from the inside to communicate to the outside world. A firewall can also provide logging and auditing functions to record all traffic passing through. In other words, a firewall can protect the internal network against attacks from outside by defining an access control policy to permit or deny traffic. However, a firewall cannot protect against attacks that do not go through the firewall itself, and cannot protect against attacks like viruses or data driven attacks that ride inside network traffic permitted by the firewall (such as web traffic). Proper configuration of a firewall plays a very important role in ensuring its effectiveness in terms of security protection.

22. What are the general considerations for protecting a network?

The following network protection guidelines will help:

Keep your network simple (i.e. minimise the number of network interface points between “secured” and “non-secured” networks)

Only allow authorised traffic to enter your “secured” network

Set appropriate controls to limit connections to external/’non-secured’ networks

Use multiple mechanisms to authenticate users (e.g. a password system plus pre-registered IP/IPX network, plus pre-registered MAC address/terminal numbers)

Manage the network using a proper network management system

Encrypt sensitive data with proven encryption algorithms before transmitting over the network

23. What is meant by physical security?

Physical security refers to the protection of hardware, computer equipment, and other IT assets from external physical threats, such as unauthorised access, theft, or loss of backup media during transportation to external sites.

24. What is meant by application security?

Application security refers to the security measures built into a software application itself in order to provide a secure computing environment. Common application security measures include authentication of the application, an access matrix for different levels of users, input validation to avoid the possibility of application flaws such as a buffer overflow, and application logging features, etc. Application owners should determine with the development team application security requirements according to the criticality of the application in the design phase, as well as the sensitivity of the data to be processed.

25. What needs to be considered when it comes to Internet security?

The Internet is a world-wide “network of networks” that uses the TCP/IP protocol suite for communication. Internet connectivity offers enormous benefits in terms of increased access to information. However, the Internet suffers from significant and widespread security problems.

The fundamental problem is that the Internet was not designed to be secure. A number of TCP/IP services are vulnerable to security threats such as eavesdropping and spoofing. Email, passwords, and file transfers can be monitored and captured using readily available software.

Internet services need stronger authentication and cryptography mechanisms, and these mechanisms must be interoperable. Internet information enquiry or transaction processing requires user authentication. Audit and backup of authentication information may also be required. Sensitive and personal data should be properly encrypted.

In general, Internet security covers a wide range of issues such as identification and authentication, computer virus protection, software licensing, remote access, dial-up access, physical security, firewall implementation and other aspects relating to the use of the Internet.

26. How can I protect my privacy online?

Do not share your personal information online. This includes your name, home address, email address, HKID number, telephone number, etc. when filling on-line forms, or chatting with people you don't know using instant messaging tools, unless there is a specific reason for them to know. Proper security measures, such as SSL should be in place when entering your personal information.

Think carefully before giving out your personal information online, as it could end up being used for other purposes you didn't intend. Secure your email by digitally signing and encrypting messages before transmission and storage. Safeguard your personal computer because it is physically open to attack or theft. Change your password regularly and keep it secret. Try not to use insecure, easy to guess passwords such those derived from a word in the dictionary.

27. How can I ensure that my user passwords are secure?

You should select a password that is difficult to guess and keep that password as secret as possible. Passwords should also be changed immediately if a password has to be reset, or upon receipt of a new password. Administrators should ensure that each new user is given a strong initial password instead of using a default one known to all staff in the organisation. Procedures should be set up to ensure that only the real person requesting the password can get that password. No passwords should be displayed in plain language on screen at any time. User passwords should also be encrypted using secure algorithms when stored.

Passwords should be well protected at all times. When stored in databases or servers, security controls such as access control and encryption should be applied to protect passwords. Passwords are often a key component to any system login, so they must be encrypted when transmitted over any un-trusted or insecure communication network. If password encryption is not possible, other controls such as changing the password more frequently should be implemented.

28. How can I protect my computer data?

Follow these DOs:

- Enable the "auto update" features for any anti-virus, anti-spyware and software for latest malicious code definitions and security patches
- Install and enable a personal firewall
- Keep passwords secret and change them regularly
- Keep portable storage devices safe
- Encrypt sensitive data
- Back up important data
- Test data recovery procedures periodically

Follow these DON'Ts:

- Don't visit suspicious websites
- Don't open emails or attachments from strangers

In addition, be mindful of the safety of your data when using public wireless networks and/or public computer facilities.

29. How can I be a smart Internet user?

You'll be a smart Internet user if you protect yourself in the following areas:

- Install anti-virus and malicious code detection and repair software with the latest virus signatures and malicious code definition files; perform full system scans regularly
- Install a personal firewall software to protect your computer from network intrusions
- Apply the latest security patches to all software and applications
- Enable password-protection on your computer and change the password regularly to protect against unauthorised usage

- Be aware that it is dangerous to execute software downloaded from the Internet unless the software is from a known and trusted source
- Avoid disclosing your personal data unnecessarily
- Disconnect from the Internet as soon as you've finished using it

30. What is involved in information security management?

Information security management involves a combination of prevention, detection and reaction processes. It is a cycle of iterative activities and processes that require ongoing monitoring and control. The cycle includes the following:

- Assessing security risk: performing security risk assessment to identify threats, vulnerabilities and impacts
- Implementing & maintaining a secure framework: defining and developing policies, assigning responsibilities and applying safeguard measures
- Monitoring & recording: monitoring and recording constantly so that proper arrangements can be made when tackling a security incident
- Reviewing & improving: conducting periodic review and security audit to make sure that adequate security controls are meeting security requirements

31. How can we know whether the information of our organisation is safe?

You can check by using the following statements to determine if the information of your organisation is safe:

- Whether my organisation is confident that our web server is properly protected and managed by well-trained people
- Whether my organisation has a clear policy on who is allowed to access what information

- Whether my organisation has designated personnel for information security management
- Whether my organisation has employed security tools such as firewalls and encryption tools
- Whether my organisation has plans for emergency response and disaster recovery, and whether these plans are reviewed regularly to ensure they tie-in with the business continuity plan

If the answer to some of these statements is no, your organisation may still possess a number of security holes that are exposed to threats.

32. What are the differences between a typical organisation network and wireless network?

A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires for communication between devices. A WLAN is a flexible data communication system used as an alternative to, or an extension of a wired LAN. Wireless information communication has enabled people to interact more easily and freely. With the advent of technology, wireless accessibility is becoming increasingly deployed in the office and public places.

WLAN is based on the IEEE 802.11 standard. Different standards such as 802.11a, 802.11b and 802.11g have since then evolved supporting different frequency spectrums and bandwidths. There are two related IEEE standards — 802.1X and 802.11i. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard was created for wireless-specific security functions that operate with IEEE 802.1X.

A WLAN should be implemented with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.

33. What are the best practices for individual users when accessing a public / municipal wireless network?

- Always treat a municipal wireless service as an untrusted network and do not give out personal / sensitive information if an encryption channel such as SSL is not available. It is also not a good idea to access company servers from a municipal wireless service without the protection of a Virtual Private Network (VPN) or similar encryption mechanisms to ensure the confidentiality of communications. Split tunnelling, which allows a person to connect to the Internet while at the same time maintaining a VPN connection to a private network, should also be disabled when using VPN.
- When connecting to a public hotspot, you may be redirected to a captive portal page. Attackers have been known to set up fake captive portal pages to obtain sensitive information. Therefore, it is important to check the authenticity of a captive portal by verifying the certificate of the website in question.
- Some operating systems offer a feature for the user to create a list of preferred wireless networks. Once this list is defined, the system will keep searching for preferred networks and try to automatically connect to them when within range. By capturing information sent out from a person's system in this way, an attacker could setup a fake wireless access point that corresponds to the settings of a wireless network on the victim's Preferred Network List. In doing so, the user is automatically connected to the

attacker's wireless network. To prevent this kind of attack, the Preferred Network List feature should be disabled or removed.

- Computer-to-computer wireless networking should be avoided. "Ad Hoc" mode networking enables a person's wireless device to communicate with other computers directly through a wireless connection, but it offers minimal security against unauthorised incoming connections. This feature should be disabled to prevent attackers gaining access to information resources on the individual's device. Network shared resources should also be turned off.
- Individual users should always protect their computer when connecting to a municipal wireless service by running anti-virus / anti-spyware software with the latest signature files, applying the latest patches to system components, and turning on their personal firewall. Sensitive and confidential information stored in any wireless device should also be encrypted using strong encryption algorithms. Common security safeguards such as power-on login to a device or system login authentication, and password-protected screen savers should also be used when accessing the Internet in public places

34. What precautions should a home user take when using instant messaging (IM)?

- Don't set your IM client to automatically accept file transfers
- Before opening any file received via IM, you should verify with the sender that he or she did actually send that file to you. In addition, make sure the file has been scanned with anti-virus software before opening it
- Never click on URL links from untrusted / unknown contacts within an IM chat session
- Never send personal or sensitive information over IM. Even if there are compelling reasons to do so, ensure the information is encrypted
- Keep your IM software (and other system components) up-to-date with the latest patches; enable your personal firewall and install anti-virus software

with the latest virus signatures, malicious code definitions as well as its detection and repair engines

35. What security measures should a home user take when using Peer-to-Peer (P2P) technologies?

- Install anti-virus programs and a personal firewall on your computer. Ensure virus signatures, malicious code definitions as well as their detection and repair engines are updated regularly
- Apply the latest security patches
- Remove all unnecessary user privileges on the computer
- P2P applications need the firewall to open a number of ports in order to function properly. If file sharing is not needed, unnecessary port ranges should be blocked
- If a P2P download is necessary, it is advisable to quit the P2P client application after completion of the download
- Do not download files from untrustworthy or suspicious sources
- Child pornography and other illegal material, including pirate software, should never be downloaded

36. How should a user protect himself/herself when using a FON WiFi network?

- Change the default settings, such as the administrative password and WPA encryption key, to strengthen the protection of the FON access point
- Install a personal firewall on all machines in the home network to guard against potential attacks originating from the private WLAN
- Install anti-virus software, update security patches and enable a personal firewall on any mobile device before connecting to a FON WiFi network

- Encrypt sensitive or confidential data stored in mobile devices as well as communication connections to company servers or other transactional services
- Keep your access point patched with the latest fixes. Ensure the automatic firmware update from FON is working properly if you are using La Fonera routers

37. How can I configure my wireless broadband router securely?

- Change the default username and password because they are often well known and easy to guess. Some manufacturers might not allow you to change the username, but at least the password should be changed
- Users should disable SSID broadcasting or increase the “Beacon Interval” to the maximum
- The default SSID should be changed. The new SSID should not be named in a way that reflects your name or other personal information. This information would help an attacker trying to collect reconnaissance information about you
- Whenever possible, the WEP protocol should be avoided. Instead, use WPA2 or WPA if it is supported on your device
- Shared key mechanisms should be avoided. Instead, stronger mutual authentication as defined in the 802.11i standard should be considered
- Enabling MAC address filtering is recommended as another layer of protection
- Disabling the DHCP feature is recommended if possible, as DHCP gives any malicious attacker easier access the wireless network

38 Comparing the risk posed by a vulnerability with the risk of installing the corresponding patch: if an administrator decides not to apply a patch, or if no patch is available, what other common compensating controls are available?

When evaluating whether to apply a security patch or not, the risks associated with installing the patch should be assessed. Carefully compare the risk posed by the vulnerability with the risk of installing the patch. Other compensating controls should be on standby, and these may include:

- turning off services or capabilities related to the vulnerability
- adapting or adding access controls
- increasing monitoring of systems to detect and prevent actual attacks

39. What are the criteria for choosing a patch management solution?

In addition to matching the specific user and business requirements, including product functionality and budget constraints, organisations should also take the following factors into consideration when considering a robust and secure patch management solution:

Fewer Vulnerabilities

Some patch management products have more vulnerabilities than others. Organisations should choose an appropriate solution that looks less likely to be vulnerable itself, which in turn will reduce the need to patch the software regularly. Research should be conducted first to independently verify the product concerned. A complex product may mean more code and services that in turn might introduce more vulnerabilities. It may be wise to select a less complicated and more mature product.

System Compatibility

Some patch management solutions are agent-based while others are agent-less. Organisations should evaluate any impact to their systems (such as performance, stability and compatibility), if agents are to be deployed across a large number of machines.

Vendor Responsiveness to New Vulnerabilities

Organisations should also take note of the speed with which the solution vendor responds to new vulnerabilities with patches and updates.

Ease of Deployment and Maintenance

The easier the patch management solution is to deploy and maintain, the lower the implementation and ongoing maintenance costs to the organisation.

Audit Trail

A good patch management solution should provide comprehensive logging facilities that help system administrators easily keep track of the status of software fixes and patches on individual systems.