Seven Habits of Cyber Security

1. Security Policy and Security Management

- Define and document the security requirements with respect to cyber security risks
- Review and update regularly the security requirements and security policy
- Disseminate regularly the information on the latest security policy to staff members

2. Endpoint Security

- Install security software such as anti-virus and anti-malware software
- Keep the definition file and patches of security software up-to-date
- Keep the operating system and software of the endpoints up-to-date
- Login with a non-privileged and non-administrator account for daily usage

3. Network Security

- Protect organisation network with a firewall and minimise network ports exposed to the Internet
- Use "DENY" as default rule on firewall, and only "ALLOW" necessary traffic
- Allow only approved IP addresses to have Internet access
- Use a secured VPN connection for remote access
- Use encrypted network protocols (e.g. HTTPS)
- Review regularly the firewall rules

4. System Security

- Perform system hardening with security policies enabled and unused services disabled
- Keep all system software including operating system, security software and patches up-to-date
- Encrypt sensitive information on the system storage
- Validate and filter input from Internet users (e.g. web server forms) properly in application to avoid SQL Injection type of attack
- Perform security risk assessment and audit regularly

5. Security Monitoring

- Enable logging features in network devices (e.g. firewall) and servers
- Centralise logs within the organisation for periodic review and monitoring
- Review the logs and security alerts and respond to detected issues in a timely manner
- Monitor network traffic (e.g. Internet traffic) to detect if there is any abnormal traffic pattern

6. Incident Handling

- Develop incident response plans for handling various security incidents (e.g. ransomware, data breach, distributed denial-of-service (DDoS) attack, etc.)
- Backup systems and data regularly
- Keep backups offline (or better still offsite)
- Perform regular backup restore drills to ensure that data can be restored properly

7. User Awareness

- Remind staff members regularly on their roles and responsibilities in protecting the organisation's information assets
- Perform drills (e.g. simulated phishing attacks) to test staff readiness against common cyber attacks

GovCERT.HK
Government Computer Emergency Response Team Hong Kong

HKCERT Hong Kong Computer Emergency Response Team Coordination Centre

香港警務處 Hong Kong Police Force

For details, please visit HKCERT website at:

www.hkcert.org