For Information
on 30 May 2008

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This paper informs Members about the present situation regarding security of electronic information in the Government and public bodies, the experience gained from recent data leakage incidents and the enhancement programmes that the Government will pursue to reduce the risk of future incidents.

Government's Posture on Information Security

2. Government places great emphasis on information security and the protection of its information and computer assets. Under the Digital 21 Strategy for information and communications technology (ICT) development, establishing a secure environment is one of the key enablers in the promotion and development of ICT in Hong Kong. Various initiatives on information security have been launched to help promote the public confidence in conducting electronic transactions, which in turn facilitate e-government and e-commerce to flourish. Over the years, we have made substantial progress on a number of information security related initiatives to develop a public information security infrastructure to facilitate e-business and the use of ICT in the community.

3. Government has formulated and implemented a comprehensive information security framework to establish the governance and measures to protect information assets it manages. In view of the fast changing business environment, technologies and community needs, Government continuously update the framework to keep in pace with the latest developments. In the

spate of recent information leakage incidents, Government is putting in efforts to enhance the framework to uphold a high standard of information security and minimise the impacts of security incidents.

4. Notwithstanding the extensive arrangements that are currently in place to protect the Government's information assets and the personal data of our citizens, we recognise that there is a continuing need to enhance our efforts to take account of new threats and risks, and lessons learned when data security incidents occur.

Existing arrangements for protecting information assets and personal data

Information Security Governance

5. Government has developed a comprehensive set of information security regulations and policies[1] and has promulgated these to bureaux and departments (B/Ds). These regulations, policies and associated procedures and guidelines were developed with reference to international best practices and professional sources, and are reviewed from time to time to reflect changes in technology and security threats. B/Ds are responsible for the overall management of information security in their departments, taking account of operational, organisational, management, technical and procedural considerations in building up their information security framework and practices. Individual employees and contract staff are responsible for personally complying with the prescribed practices.

6. To oversee and enforce information security within the Government, an Information Security Management Committee (ISMC) was established in 2000[2]. An executive arm of the ISMC, the IT Security Working Group (ITSWG) was also set up to promulgate and monitor compliance of IT security policy and guidelines among B/Ds. Since May 2007, a centrally managed security audit is carried out for each department periodically to monitor the compliance of security risk assessment and review.

(i) Service-wide Information Security Requirements

[1] They include the Baseline IT Security Policy, IT Security Guidelines, Security Risk Assessment and Audit Guidelines, Information Security Incident Handling Guidelines, and Guidelines on Software Asset Management (SAM)

[2] Core members of the ISMC comprises senior officers of the Security Bureau (SB) and the Office of the Government Chief Information Officer (OGCIO).

7. In respect of data protection, the Government Security Regulations (SR) have stipulated the rules for classification and handling of data held by Government. In many cases, personal data has a classification of "restricted" or higher. Security of classified information, including documents containing personal data, is the personal responsibility of every government officer. The SR also specifies the information security requirement of IT systems and related topics including the storage, processing and transmission of information.

8. The Office of the Government Chief Information Officer (OGCIO) has developed guidelines to advise B/Ds on implementation of information security measures. Examples of the topics covered by these guidelines are set out in the **Annex-1**. The guidelines on Software Asset Management (SAM) specifically address the proper management and use of computer software. In addition, guidelines on the proper use of the Internet have been issued to all government staff to assist them in accessing the Internet. OGCIO also requires and facilitates the conduct of Privacy Impact Assessments and Security Impact Assessments whenever B/Ds undertake system development projects.

(ii) Bureaux and Departments

9. B/Ds have to establish departmental information security policy based on the Baseline IT Security Policy and implement the necessary information security management and protection mechanisms[3] including departmental information security circulars, instructions and procedures to coordinate and administer business applications, IT resources, information security protection and incident response handling.

10. To protect departmental information systems and computer facilities, B/Ds have implemented necessary measures to ensure the integrity of business transactions and information[4] as well as a biennial security risk assessment exercise on their information systems, networks and services. In addition, the OGCIO has provided a self-assessment proforma to B/Ds for

[3] They include appointing key functions taken up by senior staff as departmental E-Business coordinator, departmental IT security officer (DITSO), network administrator and an Information Security Incident Response Team (ISIRT). The DITSO is charged with the responsibilities of management and operation of overall information security matters of the department. The ISIRT deals with all matters on a day-to-day basis relating to security incident reporting and response.

[4] These measures include physical security, access control procedures and electronic authentication mechanisms.

their completion and return for security improvement study on a yearly basis.

11. On the occurrence of information security incidents, B/Ds are required to report their security incidents to the Government Information Security Incident Response Office (GIRO) depending on the severity of the case.

12. B/Ds are responsible to ensure that their staff receive adequate and appropriate training on information security, and maintain maximum awareness, knowledge and skills in handling information by circulating[5] the relevant regulations, policies, guidelines, procedures, information notices and security alerts in a timely manner to all staff including outsourcing contractors.

(iii) Government Staff

13. All government staff are obliged to observe the regulations and instructions promulgated on information security and protection of personal data related to their work. It is the personal responsibility of every member of staff to comply with the security requirement of handling classified information including documents containing personal data by acquiring the knowledge, understanding, following and applying all the possible and available security mechanisms to the maximum extent possible, especially preventing any unauthorised access to their computers and workstations at their best effort.

(iv) Public Bodies

14. B/Ds who have purview over public bodies will take into account the government security regulations and policies in their respective regulatory or administrative arrangements with the public bodies. In order to oversee the proper functioning of the public bodies, it is necessary for both parties to liaise on the protection of the information assets to prevent any information security incidents that may affect the provision of public services. Responsible B/Ds have been coordinating with their respective public bodies on information security planning and implementation of measures to ensure the necessary

[5] Moreover, B/Ds are required to remind staff periodically by re-circulating these documents.

protection and incident response capabilities are effectively put in place and operable. Public bodies are generally recommended to adopt or customise government information security related policies, guidelines and technical information when formulating their own information security policy, programme plans and implementation. Most importantly, public bodies should stay vigilant of online threats and continue to enhance their security posture to protect their computer assets and citizens' data held by them.

Implementation of Protection Measures

(i) Technical Measures

15. Government adopts the principle of 'protect, detect, react and respond' to ensure the integrity of business transactions and information. In order to guard against different types of cyber attacks[6], we have implemented necessary measures including deploying state-of-the-art technologies service-wide or for specific IT projects[7]. Besides advising on the information security requirement, standards, design and solutions for certain major IT projects, the OGCIO also helps B/Ds to source software and IT security professional services that they need. To facilitate B/Ds in handling information security related tasks, the OGCIO has put in place standing offer agreements for engaging information security professional services to assist B/Ds that need to procure external resources.

16. Appropriate sign-on procedures and access authorisation have been implemented for controlling access to various service-wide and departmental IT systems and networks in order to protect classified/personal information or services from security exposure. To further strengthen access control to information systems and services, the OGCIO published a Risk Assessment and e-Authentication Framework in 2004 to ensure that risk assessment and appropriate protection measures are carried out by B/Ds when implementing their e-government services. In December 2007, we promulgated the Unified Identity Management Framework to ensure that citizens will be provided a unified customer interface and account management process during user registration, service enrolment and user authentication when new

[6] These include computer worms and viruses, hacking, spamming and computer crimes.

[7] These measures include firewalls, anti-virus software, intrusion detection systems and other defensive mechanisms to monitor, detect and block suspected and potential attacks on our computer networks and systems which are kept up-to-date by applying the necessary patches and fixes regularly.

e-government services are introduced. The framework strikes a balance between convenience to the public on the one hand and safeguarding information assets on the other. Nevertheless, regular security reviews and audits of the technical and procedural measures are performed to ensure that they can keep up with technology advancements and industry best practices, and changes in the system, network, or organisational environment.

(ii) Compliance Requirements

17. Since May 2007, a centrally managed security audit is carried out for each department periodically to confirm compliance and that identified improvements are properly implemented. The initial series of security audits will be completed by May 2009 for all B/Ds.

(iii) Staff Awareness and Education

18. Government puts emphasis on staff training on information security and is committed to facilitating staff in acquiring the knowledge and skills in information security. To raise staff awareness on information security and associated best practices at both management and operational levels, OGCIO has published extensive guidelines on the planning, management and technical aspects of security for reference by B/Ds, and has communicated them through seminars, thematic webpages and quick reference guides. These guidelines are updated from time to time to take into account of new security threats and measures to avert them. A comprehensive communications network has also been established to disseminate relevant information on security threats and alerts to the entire government. The OGCIO also issues reminders to B/Ds periodically to draw their attention to emerging software vulnerabilities, security threats and providing guidance in protecting their information assets.

19. Various B/Ds have been jointly organising seminars and training on information security in thematic areas including data protection, incident response handling, web application security, IT outsourcing security, etc. Besides, tailored classes jointly organised by the OGCIO, and the General Grades Office (GGO) of the Civil Service Bureau (CSB), were run for Executive Officer (EO) grade staff on "Government Information Security" to address their special knowledge and working needs in their daily departmental

operations. Two Internet-based courses on data protection have also been launched for all government staff on the "Cyber Learning Centre Plus" which is an e-learning portal managed by the Civil Service Training and Development Institute (CSTDI).

20. The OGCIO makes use of multiple information dissemination channels including websites[8], leaflets, booklets, radio and TV broadcasts to promote awareness and education to government staff as well as general public on thematic security topics. In particular, the OGCIO distributed a leaflet[9], "Protect Your Computer Data" in 2007 which contained the key messages of "Keep portable storage devices safe" and "Encrypt sensitive data". To guide users on the proper use of Internet services and emphasize the relevant laws, the OGCIO has also published for government staff and public access a set of guidelines on "Acceptable Use of Internet"[10].

(iv) Incident Response Mechanisms

21. In case security incidents do occur, individual B/Ds are responsible for conducting the initial investigation in the first instance. They are required to report security incidents to the GIRO depending on the severity of the case, e.g. if the incident affects public services or the Government. Leakage of confidential materials and personal data are required to be reported as a normal practice. The GIRO coordinates and supports B/Ds in the handling of Government information security incidents.

Experience Gained from Recent Incidents

22. Since mid-April 2008, a number of security incidents occurring in government agencies and public bodies involving leakage of personal information have caused public concern (please refer to **Annex-3** for a summary of the recent incidents). While the investigations for some of these incidents are still in progress, the preliminary findings are that most of the

[8] Government is keen to share its knowledge and experience with the community on information security to grow the public support for building a healthy e-community. The OGCIO continuously publishes technical guidance and reference resources on information security on the one-stop information security portal (INFOSEC) (www.infosec.gov.hk) for public access.
[9] Please refer to **Annex-2** for the index page in the website and the content of the leaflet.
[10] Specifically, the guidelines stipulate that users should not publish, post, transmit, link to, disseminate or subscribe any information, malicious codes or materials that are fraudulent, obscene, seditious, offensive, defamatory, threatening or unlawful.

incidents are caused by lack of awareness and/or alertness of the established information security regulations, policies and guidelines especially on the use of portable electronic devices and the file sharing software. Staff awareness of the additional potential security risks on data protection and security in handling official documents outside the office, e.g. at home is also important.

23. In the computing environment nowadays, new security threats are constantly challenging the confidentiality of information stored on end user devices, such as personal computers, consumer devices (e.g. personal digital assistant, smart phone), and portable electronic storage devices (e.g. USB flash drive, memory card, external hard drive). The popular use of and reliance on the Internet as a platform for doing business, work, study, leisure, etc. also creates online threats. Some of these threats may be unintentional or caused by human errors, many others have malicious intents including undue financial gains, causing mischief and disruption as well as attempting identity theft and other frauds.

24. The recent incidents have highlighted a number of desirable improvements in our arrangements for safeguarding electronic information. These include: enhancing the awareness of information security requirements amongst all staff and making sure they know how to comply, ensuring they have access to the software and infrastructure that they need in order to comply with the regulations and to minimise the occasions on which data is stored on portable devices, strengthening the management mechanisms that assure compliance throughout the Government and public sector and provide such bodies with the advice and assistance that they need, planning longer-term technical enhancements that make it easier for staff to comply and easier for the Government to prevent and detect incidents of non-compliance.

Government Information Security Enhancement Programmes

25. Drawing the experience from these incidents, the Government has promptly reminded all staff of their obligations to comply with the information security requirement regarding the protection of information systems and classified/personal data. We have introduced new requirements and advice to reduce the risk of future incidents involving portable electronic storage devices. We have also issued further technical information and guidance to improve staff understanding of the relevant regulations,

procedures and IT solutions. Corrective actions have been taken immediately by the B/Ds involved in the incidents as explained in **Annex-3**. Other B/Ds have also updated their internal standing circulars and organised urgent briefings to draw the attention of staff to these reminders and additional guidelines to ensure compliance. In addition, the Government has devised a package of enhancement measures to minimize the security risks and the associated consequences of future non-compliance incidents. The enhancement programme will be launched in the coming months and mainly covers four main areas, i.e. staff awareness and education, technical and procedural measures, security compliance checking and review of security regulations, policies and guidelines.

(i) Staff Awareness and Education

26. People are the key factor in information security because they perform roles as the owner, manager, agent and user in dealing with different kinds of data. Awareness promotion, education and training are vital in the overall security strategy to strengthen information security in the Government.

(a) Reminders and Guidelines to Enhance Staff Compliance

27. To enhance compliance of data protection, OGCIO has issued additional reminders and guidelines on 2 May 2008 to all B/Ds reminding them on protection of information systems and data, in particular advising on the secure and proper use of portable electronic devices and file sharing technologies as well as the prohibition to load unauthorised application software onto a Government information system or connect any unauthorised information system device to a Government information system without prior approval as designated by the department. Information about technical solutions on data protection including encryption, access control, asset management and physical storage had also been provided to B/Ds to facilitate their implementation of necessary improvement measures.

28. A further circular has been issued on 8 May 2008 to all Government staff to reiterate their obligations to observe the relevant regulations as well as the requirements under the Personal Data (Privacy) Ordinance, and advise them of the practical means to comply. Moreover, B/Ds have to ensure access

to information is confined strictly on a need-to-know basis. The circular also introduces new requirements of seeking prior authorisation, storing of minimum information and use of secure storage media when handling classified/personal data stored on portable electronic devices. Nevertheless, B/Ds are reminded to continue circulating these notices and reminders to their staff and provide internal trainings and other assistance to their staff to facilitate their compliance.

(b) *Enhanced staff communications*

29. OGCIO and Security Bureau (SB) with the support by CSB are working closely with departmental IT security officers to design a communication programme for Government staff aiming to build and sustain a high level of awareness of information security requirement, working knowledge and practice for compliance, and an attitude of and commitment to safeguarding sensitive and personal data. This programme will be rolled out by stages starting September 2008.

30. The programme will include the design of a new set of tools including information leaflets and posters to promote staff awareness on the secure use and safekeeping of portable electronic devices for dissemination in September 2008. To disseminate the messages of information security, we will also provide articles on information security topics for publishing on the Intranet and in the Civil Service Newsletter starting in August 2008.

(c) *Staff training*

31. OGCIO has arranged to include, starting from 2008 an information security briefing session in the induction courses for newly recruited EOs organised by GGO and those invariably designated as either departmental IT security officer or to assist in the overall management of security matters in their respective B/Ds. At the departmental level, B/Ds will enhance training to staff in management, front line and support roles by including information security into their staff induction course and refresh seminars. OGCIO is also arranging seminars and trainings to cover topics specifically on the use of portable electronic devices and protection of personal data. Emphasis will be put on promoting the ethics of using IT and the proper ways of dealing with classified/personal data.

(ii) Technical and Procedural Measures

32. New technical and procedural requirements in relation to storage of personal or classified data on portable electronic devices are being implemented by B/Ds. They are also reminded to make good use of the security features of the application software and computer equipment while maintaining a balance between ease of use and access control in order to enhance the security posture of their information systems, networks and services. As working outside the office, e.g. at home has been a particular source of risk in recent incidents, we will also assist B/Ds to enable staff to work outside the office e.g. at home where this is regarded as operationally necessary.

33. In the longer-term, we are developing a strategy for implementing a more rigorous approach to the management of electronic information, to enable it to be created, stored, retrieved, worked on, used to make and communicate decisions, published, searched for, archived and so forth. This approach will include technology that makes it convenient for individual to assure the security of sensitive information, and conversely makes it harder for them to put it at risk through carelessness, thoughtlessness or malice. It will also enhance the sharing of knowledge, improve collaborative working and reduce the cost and environmental impact of managing paper records. It will take several years for such an infrastructure to be consistently deployed across the Government.

(iii) Strengthening the management arrangements to assure compliance and to provide advice and support to B/Ds, public bodies and NGOs

34. During the centrally managed security audit, the OGCIO will place additional emphasis on the procedures of the handling and protection of classified/personal data and the use of portable electronic devices. B/Ds that have completed the audits will be asked to provide supplementary information to confirm their compliance in those aspects or otherwise provide a work plan to improve on any subsequently identified weaknesses. We will also review whether there are any other management steps we can take to assure that B/Ds, public bodies and non-governmental organisations (NGOs) delivering public services are complying with the relevant security policies and practices.

35. OGCIO will continue to advise public bodies and NGOs on information security through the coordination of the B/Ds having purview on them, e.g. by reminding regulatory bodies to review the need for tighter regulations on their regulated sectors to improve information security. We will continue to remind the B/Ds to share the security regulations, policies and guidelines adopted by the Government with these organisations for their reference in tightening their security regime. We will also invite the public bodies through their responsible B/Ds to seminars and conferences where appropriate, and will review what other assistance we could give to help them improve their information security practices.

(iv) Review of Information Security Regulations, Policies and Guidelines

36. Government has established mechanisms for reviewing our information security management framework to facilitate compliance by B/Ds and keep the supporting measures in pace with technological advancement, international/industry best practices and emerging security threats. OGCIO and SB play a leading role in this, with participation by other administrative and law enforcement agencies on a need basis. The last review exercise was completed in mid-2006 and OGCIO has already planned to conduct the next review in the second half of 2008. We will take into consideration the experiences gained from the recent incidents, e.g. requiring all cases involving the loss of personal data to be reported and appropriate measure taken to reduce the chance of abusive use of the lost data. Before the comprehensive review, a working group with representatives from relevant parties including OGCIO, SB and the Police will be set up to quickly review existing regulations and policy focusing on protection of personal data. It is planned to complete this preceding review by September 2008.

(v) Information Security in the Community at Large

37. Government has taken measures to promote awareness and educate the public on the proper use of Internet services. We will collaborate with the IT sector in further enhancing the guidelines in particular citing case examples as well as other promotion activities for businesses especially the small and

medium enterprises. We will continue to enrich the INFOSEC portal and also increase awareness especially of children and youngsters on the ethics in use of Internet services through our school visit programme.

Way Forward

38. The Government is committed to educating and assisting all staff to achieve the greatest possible degree of compliance with our information security regulations and hence the greatest level of security for the classified/personal data of the Government and our citizens.

Advice Sought

39. Members are invited to note the contents of this paper.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau

May 2008

Annex-1

The Office of the
Government Chief Information Officer

BASELINE IT SECURITY POLICY

[S17]

Version : 3.0

May 2006
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

The Office of the
Government Chief Information Officer

IT SECURITY GUIDELINES

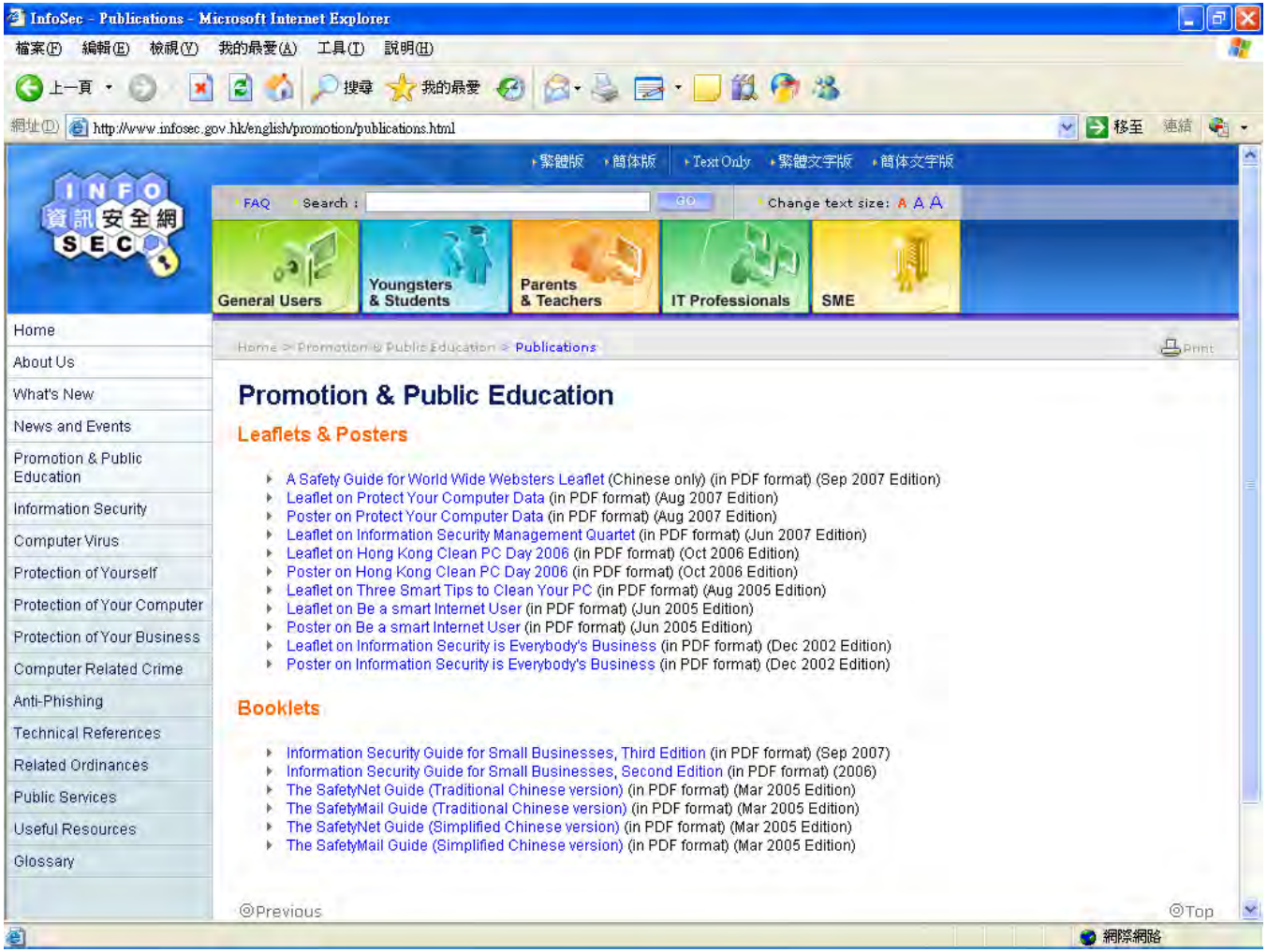
[G3]

Version : 5.0

May 2006
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

Annex-2


InfoSec - Publications - Microsoft Internet Explorer
http://www.infosec.gov.hk/english/promotion/publications.html
繁體版 簡体版 Text Only 繁體文字版 簡体文字版
FAQ Search : GO Change text size: A A A
General Users
Youngsters & Students
Parents & Teachers
IT Professionals
SME
Home
About Us
What's New
News and Events
Promotion & Public Education
Information Security
Computer Virus
Protection of Yourself
Protection of Your Computer
Protection of Your Business
Computer Related Crime
Anti-Phishing
Technical References
Related Ordinances
Public Services
Useful Resources
Glossary
Home > Promotion & Public Education > Publications
Print
Promotion & Public Education
Leaflets & Posters
A Safety Guide for World Wide Websters Leaflet (Chinese only) (in PDF format) (Sep 2007 Edition)
Leaflet on Protect Your Computer Data (in PDF format) (Aug 2007 Edition)
Poster on Protect Your Computer Data (in PDF format) (Aug 2007 Edition)
Leaflet on Information Security Management Quartet (in PDF format) (Jun 2007 Edition)
Leaflet on Hong Kong Clean PC Day 2006 (in PDF format) (Oct 2006 Edition)
Poster on Hong Kong Clean PC Day 2006 (in PDF format) (Oct 2006 Edition)
Leaflet on Three Smart Tips to Clean Your PC (in PDF format) (Aug 2005 Edition)
Leaflet on Be a smart Internet User (in PDF format) (Jun 2005 Edition)
Poster on Be a smart Internet User (in PDF format) (Jun 2005 Edition)
Leaflet on Information Security is Everybody's Business (in PDF format) (Dec 2002 Edition)
Poster on Information Security is Everybody's Business (in PDF format) (Dec 2002 Edition)
Booklets
Information Security Guide for Small Businesses, Third Edition (in PDF format) (Sep 2007)
Information Security Guide for Small Businesses, Second Edition (in PDF format) (2006)
The SafetyNet Guide (Traditional Chinese version) (in PDF format) (Mar 2005 Edition)
The SafetyMail Guide (Traditional Chinese version) (in PDF format) (Mar 2005 Edition)
The SafetyNet Guide (Simplified Chinese version) (in PDF format) (Mar 2005 Edition)
The SafetyMail Guide (Simplified Chinese version) (in PDF format) (Mar 2005 Edition)
Previous
Top
網際網路


Protect Your Computer Data
Personal Information
Bank Statement
ID CARD NUMBER
HOME ADDRESS
CUSTOMER RECORD
PASSWORD
WARNING
How do you protect your computer data?
Auto Update
Enable "auto update" features for anti-virus, anti-spyware & security patches
Keep passwords secret and change them regularly
Install and enable personal firewall
Keep portable storage devices safe
Don't visit suspicious websites
Encrypt sensitive data
Email
Don't open emails or attachments from strangers
Back up important data
Beware the safety of your data when using public wireless network and computer facilities
Test data recovery procedures periodically
Hong Kong Computer Emergency Response Team Coordination Centre
Hotline : 8105 6060
E-mail : hkcert@hkcert.org
URL : www.hkcert.org
Hong Kong Police Force
Hotline : 2528 3482
E-mail : cpu-tcd@police.gov.hk
URL : www.police.gov.hk/hkp-home/english/tcd/
INFO 資訊安全網 SEC
INFOSEC
Office of the Government Chief Information Officer
For details, please visit the InfoSec website at:
www.infosec.gov.hk
Published by the Office of the Government Chief Information Officer
Printed by the Government Logistics Department
Hong Kong Special Administrative Region Government
If you have done all of the above security measures, for sure you are a smart computer user.

Annex-3 – Summary of incidents

Case 1

The Incident

A Medical and Health Officer (MO) of the Tuen Mun Child Assessment Centre (TMCAC) reported loss of a portable USB drive at her office cum consultation room in TMCAC.

The MO reported the incident to her supervisor. On 22 April 2008, the Service Head reported the incident to the Police. The Department of Health (DH) Headquarters were informed subsequently. On 24 April 2008, DH sent letters to inform affected children and their families of the incident and offered apologies. On 25 April 2008, the Office of the Privacy Commissioner for Personal Data was informed of the incident. On the same day, DH held a press conference on the incident, made a public apology and also announced follow up actions.

A telephone hotline was set up for answering telephone enquiries.

Impacts

The lost USB device contained working files and identifiable personal data of clients. There may be leakage of personal information to the unknown.

Investigation and Findings

Investigation is still in progress.

Corrective Actions Taken

DH has updated its standing circular on the use of removable media for computers and IT systems. Staff members were reminded not to store identifiable personal data in removable storage media or transmit it out of DH by any means, unless under exceptional circumstances and with the approval of the respective Service Heads. In such cases, the information must be encrypted and such storage or transmission must be kept to a minimum that is essential for operational needs. Once finished using, the information should be erased from the portable electronic device.

Follow up Actions

Affected children and their families of the incident had been advised to stay alert and report to the Police if they were approached by suspicious persons. They were also told that treatment arrangement would not be affected as the original medical records remained intact.

Case 2

The Incident

Civil Service Bureau (CSB) reported that a portable electronic storage device containing information on two disciplinary inquiries was found missing on 23 April 2008. The names and post titles of 25 serving civil servants were stored in the storage device.

The loss was reported to the Police and the Office of the Privacy Commissioner for Personal Data. Apologies were conveyed to all 25 civil servants concerned.

Impacts

The names and post titles of 25 serving civil servants were stored in the storage device. No personal information on any member of the public was involved.

Investigation and Findings

Investigation has been completed. The officer found responsible for the loss of the portable electronic storage device has been cautioned.

Corrective Actions Taken

Action has been taken to review the security measures on the use and safe keep of portable electronic storage devices containing personal or classified information. Staff have also been reminded through briefing and the issue of updated internal guidelines to observe relevant guidelines/regulations at all times.

Security measures have been stepped up. Staff have been reminded not to use portable electronic storage devices to download, store or transmit classified data. If there is a genuine need to do so, staff should seek prior approval and only use devices with appropriate security protection provided by the bureau. Staff are also advised not to bring home any classified data in all circumstances. If necessary, a Virtual Private Network (VPN) notebook computer using a secure network with encryption and authentication features could be provided centrally for use.

Case 3

The Incident

Immigration Department (ImmD) discovered on 7 May 2008 that some confidential information of the department could be found through the search engine of a file sharing software on the Internet.

Impacts

Some confidential information of the department was found through the search engine of the concerned software on the Internet.

Investigation and Findings

Investigation so far revealed that the case concerned a newly recruited Immigration Officer who was just posted to a control point in March 2008 after completion of the induction training. With a view to familiarising with the control point operation and his work, he obtained some softcopies of previous case documents from two colleagues with the use of their USB drives in the office and then stored them in his personal computer at home for reference. It was suspected that this caused the leakage of information

Corrective Actions Taken

Despite the information leakage happened through the Immigration Officer's computer at home, ImmD took the initiative to conduct immediate software checking on all computer workstations to ensure no unauthorised software was installed. Simultaneously, a home visit was paid to the Immigration Officer and prompt action was taken to delete all relevant document files, remove the relevant software and re-format the hard disc of his computer. The home computers of the other two officers who lent out their case documents were also checked and confirmed no such documents were stored therein.

Immediate briefings were given to all staff to remind them of relevant guidelines, regulations and instructions relating to the security in handling official documents and protection of personal data. Though the incident was caused by the lack of sufficient awareness of the relevant staff, on-going efforts will be made to raise the vigilance of all staff in handling personal data and security documents.