

**Guidelines on the Installation and Use of Software in Government**

Enclosure 1           ITSD Circular No. 3/90 - Prohibition on the Use of Illegal Software

Enclosure 2           ITSD Circular No. 13/97 - Management of Microcomputers (in particular section 3.1 of Appendix A)

Enclosure 3           ITSD Circular No. 6/99 - Security of Government Networks Connected to Internet (in particular paragraph 8)

**MEMO**

Director of Information <i>From</i> Technology Services <i>Ref. in</i> DPA 11/10 <i>Tel. No.</i> 823 4488 <i>Date</i> 16th March. 1990	<b>MEMO</b>	Heads of Branches and Departments <i>To</i> _____ <i>Your Ref.</i> _____ <i>in</i> _____ <i>dated</i> _____
--	-------------	---

**ITSD Circular No. 3/90**  
**Prohibition on the Use of Illegal Software**

This circular is to remind microcomputer users that use of illegal software is prohibited and to advise them on the necessary enforcement measures.

attached 2. Microcomputer users are reminded that possession/use of illegal software infringes copyright and that infringement of copyright is liable to both criminal and civil proceedings. Detailed information on this issue is contained in the Word Processing/Microcomputer User Guide (Issue 2) delivered with each standard micro-computer. The relevant section is attached for your ease of reference.

3. To ensure copyright is not being infringed, users are advised to verify the legality of all software currently residing on their computers. Basically, software that is individually licensed should come with a full set of manuals and original program diskettes. Therefore, software with only a hard disk copy and without program diskettes and a full set of manuals could be a duplicate or unauthorized copy. In either case, the software copy is regarded as illegal and should be removed immediately from the computer. However, in case of doubt, please check with the details of orders placed by your department in its acquisition.

4. To prevent the installation and use of illegal software in future, users should adopt the following measures:-

a. Avoidance of duplicate copies

Software to be on loan to others should be removed from the hard disk of the owner's computer before the whole package, including diskette and manuals, is delivered to the borrower.

For such legal software borrowed from another system, the borrower should remove the software from his/her computer immediately after use. before returning the software package to the owner.

b. Prohibition of illegal software

Existing and new microcomputer users should be made aware of the policy prohibiting the use of illegal software and on the copyright issue.

For systems that are used by a number of users, the officer-in-charge should conduct periodic checks of the system and stop any installation/use of illegal software if this is found.

5. To aid the implementation of 4.b above, this circular memorandum should be circulated to all microcomputer users periodically.

6. Should there be any queries on the content of this circular or on illegal software in general, please contact:-

Microcomputer Development Centre Help-Desk,  
Information Technology Services Department.  
16/F, Wanchai Tower I,  
12 Harbour Road,  
Wanchai, Hong Kong.

(Tel.: 823 4659)

(C. C. Greenfield)  
Director of Information  
Technology Services

c.c. Registrar. Supreme Court

**Relevant Section on Copyright Issue Extracted from  
Word Processing/Microcomputer User Guide (Issue 2.0)**

**13.2. Copyright issue**

- Possession/use of illegal software infringes copyright. Users are strictly forbidden to possess or use illegal copies of computer programs.
- Users should note that infringement of copyright is liable to both criminal and civil proceedings.
- The relevant acts of infringement under the Copyright Act, as regards computer programs, are listed below for your reference:-
  - I. The restricted acts of:
    - (a) reproducing the program in any material form;
    - (b) publishing the program;
    - (c) performing the program in public;
    - (d) broadcasting the program;
    - (e) including the program in a cable programme;
    - (f) making any adaptation of the program;
    - (g) reproducing in material form an adaptation of the program, publishing an adaptation of the program, performing in public an adaptation of the program, broadcasting an adaptation of the program, or including an adaptation of the program in a cable programme.
  - II. The supplementary infringing acts of:
    - (a) infringement by importation of infringing material;
    - (b) infringement by sale of infringing material;
    - (c) permitting place to be used for infringing performance.
- As regards I(a) above, it should be noted that the storing in a computer of a program, or of a copy of a program. constitutes reproduction of the program, and such storing of an adaptation of a program constitutes reproduction of that adaptation.
- Unauthorized reproduction in material form (including re-writing in the same language or code, where an essential element is taken) either of a protected program, or of an authorized or unauthorized adaptation of such program, will constitute infringement.

**MEMO**

<i>From</i>	Director of Information Technology Services	<i>To</i>	Heads of Bureaux and Departments
<i>Ref.</i>	<i>in</i> ITS 11/10	<i>(Attn.:</i>	)
<i>Tel. No.</i>	2582 4488	<i>Your Ref.</i>	<i>in</i>
<i>Fax. No.</i>	2802 4549	<i>dated</i>	<i>Fax. No.</i>
<i>Date</i>	6 October 1997	<i>Total Pages</i>	

**ITSD Circular No. 13/97**  
**Management of Microcomputers**

This circular aims to consolidate the existing practices and procedures on the following areas relating to the use of microcomputers-

- (a) management of microcomputers;
- (b) training and support services for microcomputer users; and
- (c) development and maintenance of microcomputer applications by end users.

Controlling officers and all other officers concerned with planning and implementing computerisation should read this circular in conjunction with Financial Circular No. 7/97.

## **2. MANAGEMENT OF MICROCOMPUTERS**

As stipulated in Financial Circular No. 7/97, departments are accountable for the efficient utilisation of their microcomputer systems. At the operational level, departments are advised to formulate their departmental policy/house rules on the management of their microcomputer systems and local area networks (LANs) and to allocate adequate resources for the implementation of such policies. Appendix A details the guidelines on the management of microcomputers and LANs.

## **3. TRAINING SERVICES FOR MICROCOMPUTER USERS**

### **3.1 Human Resource Management/Development Plan**

With the use of information technology (IT) increasingly becoming commonplace within Government, departments should address the needs for microcomputer training in formulating their Human Resource Management/Development Plan. Priorities should be set and resources provided in line with their departments' business plans. Departments are also encouraged to make the best use of training resources available to them, namely courses and facilities provided by the Civil Service Training and Development Institute (CSTDI) and the Information Technology Services Department

(ITSD), training programmes available in government bulk contracts administered by the two departments, departmental in-house training programmes as well as self-learning courses available in the market.

## **3.2 Training Facilities**

### **3.2.1 *CSTDI Courses and Facilities***

CSTDI organizes a number of training programs ranging from Management Information Systems for Non-IT Managers to application software courses. Train-the-PC-Trainers courses are also provided. Colleagues who want to know more about these training courses can refer to CSTDI's training prospectus.

In addition, training rooms with necessary equipment and facilities are available on loan to departments at CSTDI for organizing departmental microcomputer training.

Interested colleagues can approach CSTDI at 2805-2191 for the training prospectus or for facilities booking.

### **3.2.2 *Training Courses and Facilities Provided by ITSD***

From time to time, ITSD will organise seminars and briefings on popular software products. Interested colleagues who want to attend these seminars and briefings should apply in response to the relevant enrollment notices from ITSD.

In addition, computer-based training and video training are available in ITSD's Self-learning Centre for end users from all departments. Please contact ITSD's Training Unit at 2961-8013 for reservation or for more details on these training courses.

### **3.2.3 *Departmental In-house Training***

As mentioned in paragraph 3.2.1 above, departments are encouraged to organize in-house, job-oriented training on the use of microcomputers. Departments may reserve the training room and equipment at CSTDI as and when necessary.

### **3.2.4 *Training Arranged through Bulk Contracts***

LAN administration training is available in the Microcomputer and Network Equipment Bulk Contracts administered by ITSD. In addition, microcomputer training is available via the Microcomputer Training Service Bulk Contracts administered by CSTDI. Departments can refer to CSTDI Circular No. 3/96 for more details about the Microcomputer Training Service bulk contracts.

## **4. SUPPORT SERVICES FOR MICROCOMPUTER USERS**

### **4.1 Levels of Support Services**

While ITSD would provide central technical support services for microcomputer users through the Technology Services Support Centre (TSSC), and its Departmental Liaison Officers (DLOs) would stand ready to offer support for administrative computer systems, departments are encouraged to develop local support teams to better meet the needs of its microcomputer user community.

## **4.2 ITSD's Support Services**

### **4.2.1 TSSC**

The primary support services provided by TSSC include a centralised front-end helpdesk providing a single point of contact to all computer users and departmental support personnel. For general enquiries on technical and administrative matters related to microcomputers, LANs and office automation tools, users may contact the TSSC Helpdesk at 2827-8585.

In order to promote the effective use of IT within Government, TSSC also publishes the Bulletin Board System (BBS) and newsletters, and organises exhibitions, technical seminars and special interest groups regularly. Other services offered by TSSC include anti-virus support and common facilities for document conversion, document scanning and Optical Character Recognition conversion.

The TSSC BBS provides a two-way communication channel for departmental local support personnel to communicate with TSSC support staff as well as with end users and support personnel in other departments. The BBS is an effective media for information dissemination and experience sharing. You may consider subscribing to our BBS if you have not yet done so.

Users who wish to join our special interest groups<sup>1</sup>, subscribe to the TSSC Newsletter/BBS or use any of the TSSC facilities/services may contact the TSSC Helpdesk at 2827-8585.

### **4.2.2 DLOs**

For project-specific technical support service, users may contact the relevant DLOs.

## **4.3 Local Support Services**

We encourage departments to set up their local helpdesk service. These local support units provide first line support to the local microcomputer user community. They can be more responsive and effective because they understand more about the business of their department and have more knowledge of the supported hardware/software/network configuration. These local support units may refer difficult problems to the central TSSC Helpdesk. Departments may contact TSSC or their DLOs for advice on the setting up of local helpdesks.

---

<sup>1</sup> ITSD has so far set up three special interest groups. They are the Advanced Microcomputer User Special Interest Group, the LAN Administrator Special Interest Group and the Chinese Office Automation Special Interest Group.

Departments may also consider forming internal user groups for information and experience sharing.

For departments with LANs, a LAN administrator should be assigned to manage the server, user accounts and perform first-line problem diagnosis.

## **5. DEVELOPMENT AND MAINTENANCE OF MICROCOMPUTER APPLICATIONS**

With suitable training, users are encouraged to implement non-complex microcomputer applications in order to satisfy their business requirements. As end users know their business and requirement best, provided that due attention has been made not to affect the operational environment of the existing administrative systems, they can apply microcomputer tools more flexibly and effectively to enhance their productivity and improve the quality of their services. In order to realise this potential benefit, careful planning and coordination is required. Departments are therefore advised to ensure that adequate resources are available for managing and coordinating the implementation and maintenance of such applications.

### **5.1 Application Sharing**

A Central Register of Microcomputer Applications is maintained and published on the TSSC BBS to facilitate applications sharing among bureaux and departments.

Based on the information in the Register, departments can select an appropriate application that closely meets their requirements and approach the corresponding contact person for using the programs or source codes.

### **5.2 Information Sharing**

Departments are advised to coordinate with their end users as well as ITSD to facilitate the sharing of operational data after due consideration of the Personal Data (Privacy) Ordinance. For example, the availability of certain data item, the responsible user and any restriction on access control could be announced via electronic notice board.

### **5.3 Inherent Risk and Implication of User-developed Microcomputer Applications**

It is user departments' responsibility to enhance and maintain their user developed microcomputer applications. The most common problem of such applications is that when the developer leaves his/her post, there is no one within the department who can operate or maintain the applications. Departments are therefore strongly advised to stabilize their internal resource for application support by :

- deploying standard tools so that technical skills are aligned with the rest of the civil service;
- deploying at least two officers to work together in developing applications; and
- ensuring that the officers responsible for application development and maintenance have adequate skill in the development tools as well as the development process.

Departments should also ensure that operational procedures as well as technical documents to facilitate subsequent maintenance and enhancement of the application are in place and kept up-to-date.

#### **5.4 Operation and Maintenance of Microcomputer Applications**

Departments should ensure the integrity of their applications and that adequate security measures, back-up and recovery arrangements are in place for these applications. In particular, regular drills should be practised to ensure that operational staff are familiar with the contingency plans and procedures.

Departments should also continuously monitor, review and enhance their user-developed microcomputer applications in order to keep up with the business objectives and the emerging needs under the latest technology.

#### **5.5 Request for Application Development**

Departments should refer to Financial Circular No. 7/97 for the application procedures for the implementation of applications that they cannot develop themselves. Departments may contact their DLOs for further enquiries.

### **6. USEFUL REFERENCE MATERIALS**

The Microcomputer User Guide issued by ITSD contains useful references to hardware/software/services available from the bulk contracts as well as guidelines for anti-virus protection, security, system installation, system design, documentation, conversion, operation, housekeeping and maintenance.

In addition, ITSD has developed various other guidelines for reference by microcomputer users. Please refer to the checklist at Appendix B.

### **7. ENQUIRIES**

Enquiries on the contents of this circular should be directed to our TSSC Helpdesk at 2827-8585.

KHLAU

Director of Information Technology Services

c.c. Judiciary Administrator

SMs and above, ITSD

### **General Guidelines on the Management of Microcomputers**

Many departments are using either standalone or networked microcomputers to increase their productivity and efficiency in delivering their services. In the early days, the use of microcomputers was mostly limited to simple applications like word processing, spreadsheet calculation and single user database application. Since only minimal functions were performed on these microcomputers, the user support requirements were fairly small in scale. With the proliferation of networking technologies and more sophisticated applications, the networked microcomputers have become an effective platform for collaboration and information sharing. The demand for user support in today's networked microcomputer environment has increased substantially. To help departments face this challenge, we have consolidated the existing practices and procedures into a set of general guidelines for ease of reference.

#### **1. ORGANIZATION OF A MICROCOMPUTER USER COMMUNITY**

In order to build up an efficient and effective microcomputer application environment, resources should be allocated to coordinate, support and manage activities such as application development, user support, training and inventory control.

The following table lists the roles in a microcomputer user community. Departments are advised to plan and provide human resources to take up these roles :

<b>Role</b>	<b>Duties</b>	<b>Skill Requirement</b>
Strategic planning and resource allocation	<ul style="list-style-type: none"> <li>● plan and provide human resources to support the management of microcomputers; and</li> <li>● prioritize microcomputer management and development activities based on department's business goal.</li> </ul>	<ul style="list-style-type: none"> <li>● understanding of the department's business goals and requirement; and</li> <li>● preferably with IT knowledge.</li> </ul>

<p>Coordination of user requirements and microcomputer management activities</p>	<ul style="list-style-type: none"> <li>● coordinate with end users and management to identify the information and tools requirement;</li> <li>● coordinate and monitor microcomputer management activities;</li> <li>● formulate departmental procedures and guidelines on the management of microcomputers;</li> <li>● enforce agreed procedures and guidelines on the management of microcomputers; and</li> <li>● feedback users' demand to ITSD and liaise with ITSD.</li> </ul>	<ul style="list-style-type: none"> <li>● IT literate;</li> <li>● understanding of the department's business goals and requirement;</li> <li>● aware of the inherent risk and benefit of end users' developed microcomputer applications; and</li> <li>● good communication skill.</li> </ul>
<p>Local Helpdesk</p>	<ul style="list-style-type: none"> <li>● diagnosis of end users' problems; and</li> <li>● problem solving and coordination with vendors or ITSD for difficult problems.</li> </ul>	<ul style="list-style-type: none"> <li>● general knowledge of the hardware, software and network configuration supported;</li> <li>● good communication skill (with users as well as technical staff);</li> <li>● knowledge of problems encountered in the past and their solutions; and</li> <li>● familiar with the users' applications and work environment.</li> </ul>
<p>LAN / Microcomputer Administration</p>	<ul style="list-style-type: none"> <li>● diagnosis of network related problem;</li> <li>● coordination with vendors and ITSD to get problem solved;</li> <li>● administration of servers and user accounts; and</li> <li>● housekeeping.</li> </ul>	<ul style="list-style-type: none"> <li>● knowledge of LAN administration.</li> </ul>

Procurement Support / Inventory Control	<ul style="list-style-type: none"> <li>● coordinate procurement, installation, acceptance and maintenance of hardware and software;</li> <li>● inventory control; and</li> <li>● redeployment / disposal of old equipment.</li> </ul>	<ul style="list-style-type: none"> <li>● with general IT knowledge; and</li> <li>● administration skill.</li> </ul>
---	---	---

Application Development	<ul style="list-style-type: none"> <li>● develop and maintain applications; and</li> <li>● provide application support to end users.</li> </ul>	<ul style="list-style-type: none"> <li>● application development skill;</li> <li>● familiar with users' business requirement and work environment; and</li> <li>● aware of the inherent risk and implications of end-user developed applications.</li> </ul>
Training Administration	<ul style="list-style-type: none"> <li>● assess users' training needs;</li> <li>● formulate training plans;</li> <li>● keep training records;</li> <li>● coordinate training offered by ITSD/CSTDI/vendors; and</li> <li>● organize training and user group(s) to facilitate experience sharing.</li> </ul>	<ul style="list-style-type: none"> <li>● familiar with the users' applications and work environment as well as training resources available in Government and the private sector; and</li> <li>● preferably with IT knowledge.</li> </ul>
Training	<ul style="list-style-type: none"> <li>● provide job-oriented training, i.e. train users on the application of tools in specific business areas.</li> </ul>	<ul style="list-style-type: none"> <li>● in-depth knowledge on one or more tools;</li> <li>● familiar with the users' applications and work environment; and</li> <li>● with training skill.</li> </ul>

## **2. ACQUISITION OF MICROCOMPUTERS**

### **2.1 Use of Privately Owned Computer in the Office**

Departments are responsible for the provision of computer facilities for office work. The use of privately owned hardware/software for such purpose should generally not be allowed. The main considerations being that these would bring about concerns on compatibility, continuity, skill transfer, security of data stored in privately owned computer, ownership of the developed application/data and risk of infection by computer viruses.

### **2.2 Standardization**

To ensure system compatibility within Government, facilitate information exchange and application sharing, and align the skill among end users as well as support staff, departments should adhere to the prevailing hardware and software standards. Such standard products are available from the microcomputer and network equipment bulk contracts announced via ITSD circulars.

We do not encourage the procurement of non-standard items. Departments should purchase such non-standard IT products only when its operational requirements cannot be met by the standard items available in the bulk contracts. Departments are held accountable for their procurement decisions in such circumstances.

## **2.3 Technical Approval**

### **2.3.1 *Purchase of Standard Computer Equipment***

As stipulated in Financial Circular No. 7/97, departments may acquire standard software packages, standard LANs<sup>1</sup> and standard microcomputers, which do not involve the connection to or linking together of other administrative computer systems, without seeking the technical approval of ITSD. For the procurement of more complicated networks and standard equipment that are connected to other administrative computer systems, prior technical approval from ITSD is required.

### **2.3.2 *Purchase of Non-standard Computer Equipment***

ITSD's prior technical approval is required for the procurement of non-standard computer equipment, regardless of cost, that are connected to other computer systems as well as standalone non-standard computer equipment exceeding \$50,000. Please refer to Financial Circular No. 4/93 for more details.

## **2.4 Coordination**

Departments are advised to appoint procurement coordinators as contact points with ITSD for the dissemination of latest information regarding the procurement of standard microcomputer and standard network equipment. For nomination of procurement coordinators, please send the coordinator's name, designation, telephone, fax no. and address to CPM(T)E2 of ITSD. Alternatively, please complete attachment D of ITSD Circular No. 3/96, 4/96 or 5/96 and return the form to ITSD.

## **2.5 Funding of Computer Systems**

Please refer to Financial Circular No. 7/97 for the funding arrangements for computer systems.

## **3. EQUIPMENT MANAGEMENT**

### **3.1 Inventory**

Departments are responsible for the physical security of their computer equipment and should keep an inventory of their computer hardware and software in order to facilitate upgrade, resource allocation, physical checking, etc.

---

<sup>1</sup> For the definition of standard LAN, please refer to Appendix IX of the Information Summary attached to ITSD Circulars 3/96, 4/96 or 5/96.

To facilitate the compilation of a record of computer facilities in the Government, departments should maintain an inventory and, in response to the relevant ITSD Circular, inform ITSD of all computer and microcomputer items purchased or decommissioned.

The use of illegal software is prohibited. Departments are advised to ensure this by regular spot checks or by the use of software inventory tools available from the microcomputer and network equipment bulk contracts.

### **3.2 Maintenance**

Both on-call maintenance services and regular maintenance services are available in the microcomputer and network equipment bulk contracts. Regular maintenance service in general imposes less administrative overhead.

### **3.3 Replacement of Aged Equipment**

If the total five-year maintenance cost of an existing computer system is in excess of the total five-year cost for a new system inclusive of the initial capital cost and maintenance fees, departments should consider replacing these systems instead of continuing with the maintenance service.

Information Technology Services Department

## Reference Checklist

	Subject	Reference	Notes
<i>Policy Papers</i>			
1.	Computerization	Financial Circular No. 7/97	Note 2
2.	Procurement of “Non-standard” Equipment Items	Financial Circular No. 4/93	Note 2
<i>Service Announcement</i>			
3.	Provision of Microcomputer Related Training Services	CSTDI Circular No. 3/96	
4.	ITSD’s User Guide to Services	N/A	Note 1
5.	Central Register of Microcomputer Applications	ITSD Circular No. 9/95	Note 2
6.	Supply of Standard Microcomputer / Network Equipment and Related Services	ITSD Circular No. 3/96, 4/96, 5/96, 7/97, 8/97, 9/97	Note 2
7.	Technology Services Support Centre (TSSC)	ITSD Circular No. 7/94	Note 2
8.	Bulletin Board System in the Technology Services Support Centre	ITSD Circular No. 10/94	Note 2
9.	LAN Administrator Special Interest Group and Advanced Microcomputer Special Interest Group	ITSD Circular No. 11/94	Note 2
10.	Chinese Office Automation Special Interest Group	ITSD Circular No. 9/96	Note 2
11.	Anti-Virus & Access Control System (AVACS) for Microcomputers	ITSD Circular No. 7/96	Note 2
12.	Anti-Virus & Access Control System (AVACS) for Windows 95	ITSD Circular No. 8/96	Note 2
13.	TSSC Helpdesk Hotline	ITSD Circular No. 10/97	Note 2
<i>Guidelines</i>			
14.	Prohibition on the Use of Illegal Software	ITSD Circular No. 3/90	Note 2
15.	Guidelines on Microcomputer and Local Area Network Security	ITSD Circular No. 1/96	Note 2
16.	Standardisation of Software for Electronic Document Exchange	ITSD Circular No. 2/96	Note 2
17.	Acceptance Plan for Equipment drawn from the Microcomputer and Network Equipment Bulk Contracts	N/A	Note 2
18.	Microcomputer User Guide	N/A	Note 2
19.	LAN Administrator’s Guidelines	N/A	Note 2
20.	cc:Mail Administrator’s Guideline	N/A	Note 2

21.	Implementation Guidelines for Windows 95	N/A	Note 2
22.	Guidelines for Computer Virus Prevention and Detection in a PC Environment	N/A	Note 2
23.	FoxPro Application Development Guide	N/A	Note 2
24.	“The Year 2000 Problem” - Tackling “The Year 2000 Problem” in Micro-computer and Office Network	ITSD Circular No. 12/97	Note 2
25.	Guidelines for Handling Year 2000 Compliance Problems in xBASE Applications	N/A	Note 2
26.	Status of Year 2000 Compliance of microcomputer and network related products	N/A	Note 2
<i>Others</i>			
27.	TSSC News	N/A	Note 2

Notes :

Note 1 Available from ITSD General Registry (tel. : 2582-4520)

Note 2 Downloadable from the TSSC BBS (tel. : 2893-8464)

**MEMO**

Director of Information	Heads of Bureaux and
<i>From</i> <u>Technology Services</u>	<i>To</i> <u>Departments The Ombudsman</u>
<i>Ref.</i> <u>(2) in ITS 11/10 VIII</u>	
<i>Tel. No.</i> <u>2582 4488</u> <i>Fax No.</i> <u>2802 4549</u>	<i>Your Ref.</i> _____ <i>in</i> _____
<i>Date</i> <u>19 March 1999</u>	<i>Dated</i> _____

**ITSD Circular No. 6/99**

**Security of Government Networks Connected to Internet**

This Circular provides guidelines to Bureaux and Departments on security protection of I.T. resources connected to their internal networks (referred to as departmental networks hereafter) which have connections to Internet. This Circular should be read in conjunction with ITSD Circular No. 10/95 on Government Information Centre on the Internet, and ITSD Circular No. 10/96 on Internet Service Acceptable Use Guidelines.

2. Bureaux and Departments are responsible for the security of all I.T. resources within the boundary of their departmental networks. There should be well defined roles and responsibilities for the staff with respect to I.T. security. It should also be ensured that adequate security measures are in place to safeguard the government networks against security risks carried by incoming data traffic. Effective access control should be enforced to prevent unauthorised access to the I.T. resources and services. Access logs are also important for tracing unauthorised attempts to access the departmental networks. Remote access to the departmental networks must be through a remote access server and dial-back modems; PC remote control programs such as PC Anywhere should not be used for this purpose. Remote access equipment and software are available through the Backbone Network Bulk Contract and PC/LAN Term Contracts.

3. There should be continuous management of I.T. security to make sure that the security measures are in effect and that the security procedures are being practised. Bureaux and Departments should designate a security administrator to oversee their I.T. security. The security administrator should have day-to-day responsibility for scrutinising the access logs and reports generated by the security system that is implemented, as well as to report and follow up on security incidents.

## **CONNECTION TO INTERNET**

4. Regarding Internet connection, Bureaux and Departments must implement a secure firewall to safeguard the government network, otherwise connections to the Internet should be restricted to dial-up connection from either standalone PCs or PCs connected to a LAN. This has been stipulated already in ITSD Circular No. 10/96. In addition, the guidelines which are stipulated in the following paragraphs should also be observed by Bureaux and Departments.

5. Bureaux and Departments with the requirement to deploy an Internet gateway for specific purposes should seek technical advice from ITSD first. They should also review their security exposure as a result of introducing an Internet connection to the departmental network. It is strongly recommended that a security risk assessment should be performed to define the departmental security requirements with a view to implementing security measures according to the defined requirements.

6. A security audit is also recommended to be performed regularly to verify whether the security counter-measures and procedures are still sufficient and have been properly set up and practised. Depending on the complexity of the departmental network and the security requirements of the Bureau or Department concerned, security audit should normally be done at least once a year. Bureaux and Departments may seek technical advice from ITSD on security risk assessment and security audit through their Departmental Liaison Officers.

## **USE OF PERSONAL COMPUTERS**

7. PCs are one of the major sources of security threats and therefore great care has to be taken to prevent or detect attacks on a PC, and to minimise the impact to other I.T. resources should there really be an attack on the PC. Bureaux and Departments are responsible for ensuring that their PCs and servers have anti-virus software installed and activated, and that the anti-virus programs are constantly updated for protection against new types of viruses. ITSD's Technology Services Support Centre (TSSC) can provide technical advice on anti-virus issues. Guidelines on the use of PCs and security regarding PCs and LANs are also available in the ITG InfoStation via the URL <http://www.info.gov.hk/itsd/itginfo>. Details about the ITG InfoStation can be found in ITSD Circular No. 3/99.

8. Guidelines on the proper use of PCs should be observed by end users. Some of the recommended good practices are highlighted as follows:

- Treat your password as your personal secret
- Do use a password with a mix of alphabetic and non-alphabetic characters

- Do not include in your password a word contained in English or foreign language dictionaries, spelling lists, or other lists of words
- Perform regular backup of data files on fixed disks
- Do not install or use unlicensed software
- Log off the PC before leaving it unattended, or implement a screen saver which requires a password to re-activate the PC
- For PCs in a LAN environment and with dial-up connection to Internet, the user should first log off from the LAN before making a connection to Internet
- Consider turning off Java and JavaScript in the browser, except when retrieving URLs from well-known and trusted hosts
- Consider turning off ActiveX completely in the browser, or turning on the “High Security” option of ActiveX. The latter will warn the user before downloading and executing any ActiveX code.

9. Enquiries regarding this circular should be addressed to Mr Stanley CY CHAN at 2575 1024.

KHLAU  
Director of Information  
Technology Services

c.c. Judiciary Administrator  
SMs and above of ITSD