

11. IT Security

11.1 Computer Systems Security Policy and Guidelines

Computer viruses, spyware, denial of service (DoS) attacks and other types of malicious attacks have become increasingly powerful, causing loss of critical information as well as interruption of normal business operations. At PolyU, as our daily activities rely heavily on the availability and reliability of the University's IT systems and networks, it is of paramount importance that these IT resources are safeguarded from natural and human hazards.

11.1.1 PolyU Computer Systems Security Policy

To protect the University's IT resources against unauthorized access and intrusion, a Computer Systems Security Policy has been established. The Policy outlines the minimum standards of good practices to be observed in different IT-related areas including computing equipment, operating systems, networks, application systems, personal computers, etc. The Policy has been enforced on all central IT systems provided and maintained by ITS and is also to be observed at departmental and individual user level as appropriate. As the successful implementation of IT security requires the active involvement of all users, you are strongly recommended to read the Policy carefully and observe the security guidelines / procedures.

*The PolyU Computer Systems Security Policy is at **Appendix C**. The up-to-date version can be viewed at https://www2.polyu.edu.hk/PolyU/IT_Security/cssp.html under the PolyU IT Security Web Site (section 11.3).*

11.1.2 Departmental IT Security Guidelines

Based on the Computer Systems Security Policy, a set of Departmental IT Security Guidelines (https://www2.polyu.edu.hk/PolyU/General_Notices/dept_guidelines.pdf) has been formulated. The Guidelines provide guidance and "common-sense" steps for general users as well as recommendations for the departmental IT administrators, to safeguard the University's, the department's and the individual's own IT resources. You are strongly recommended to familiarize yourself with the Departmental IT Security Guidelines and to observe the recommendations and good practices outlined in the document.

The PolyU Computer Systems Security Policy and the Departmental IT Security Guidelines will be regularly reviewed and updated, to take account of the evolving technologies and the practical needs of the University. ITS will provide guidance and advice to users / departments in practising and enhancing IT security. For further information or assistance, please contact our Help Centre at **Ext. 5900**.

11.2 Virus Prevention

Computer viruses pose a major threat to the security of the University's IT environment. As new viruses are found every day, it is important that you have taken effective measures to protect yourself and the University from possible damages. The most effective way to prevent virus infection is to keep your anti-virus software up-to-date and up-and-running at all times.

11.2.1 Site Licence for NOD32 Anti-virus Software

To safeguard the IT resources of the University and to ensure that the most up-to-date anti-virus software is available to staff, a campus-wide site licensing arrangement for the NOD32 anti-virus software has been arranged by ITS. Under the agreement, all staff are licensed to install one copy of the NOD32 anti-virus software on your office PC. Additional licence right is also available for staff to run one copy of the software on a home PC, provided that the 2 copies are not in use at the same time. Please contact the ITS General Office for the media of the NOD32 anti-virus software.

11.2.2 Good Measures against Viruses

To protect yourself against computer viruses, please observe the following good practices:

- Do not open attachment / download files from an unknown source. Be careful even if the attachment is from a friend you know. Some viruses can replicate themselves and spread through e-mail.
- Keep your anti-virus program up-to-date and up-and-running at all times.
- If the anti-virus program warns you of a virus, take it seriously and clean the virus at once.
- Keep your Windows system up-to-date with the patches and fixes from Microsoft. Please refer to the URL: http://www.polyu.edu.hk/its/pub_doc/Windows_Updates.pdf for the procedures of setting up your PC for automatic Windows update.
- Backup your critical and important data files regularly. Make sure to save the backup copy in a separate location, preferably not on the same computer.

11.3 PolyU IT Security Web Site

To facilitate the dissemination and ready access of up-to-date news on IT security, a PolyU IT Security Web Site has been developed to provide a central repository of IT security information. From the web site, you can find important information on security procedures and guidelines, good practices, security alerts and other useful security web site links, etc. You can access the Security Web Site by clicking the "IT Security" button on the ITS web site or directly at: https://www2.polyu.edu.hk/PolyU/IT_Security.



11.4 IT Security Incident Reporting

If you suspect that your computer is infected by viruses, attacked by hackers or is affected by any other types of malicious attacks, please report the incident to the ITS Help Centre at **Ext. 5900**. You may also submit your case online via our HelpCentre Online Tracking Service (HOTS) at <http://www.polyu.edu.hk/hots>.