V1.0 2020/11/25

Notice on Information Security and Personal Information for New Recruits at

National Taiwan Normal University

1. Work email addresses may not be used as accounts to make registrations on non-work related websites, such as social networking and e-commerce sites.
2. Work-related data transmission and work-related communication must be carried out using work e-mail accounts. Private e-mail accounts must not be used to send or discuss work-related information.
3. Automatic downloading of pictures or images in emails should be disabled. E-mails from unknown senders should not be opened to prevent malware attacks.
4. Avoid transmitting sensitive personal information or files via e-mail. If you want to transmit sensitive personal information via e-mail, please encrypt it first.
5. The Ministry of Education conducts social engineering drills twice a year to raise awareness of malicious emails. Please avoid opening e-mails from unknown senders.
6. Do not use LINE or other instant messaging apps to transmit sensitive information or files.
7. Do not download or use software, music, movies or files that lead to violation of intellectual property rights.
8. Do not use non-work related peer-to-peer (P2P) software to download or share files.
9. Please observe authorization rules for software and IT products, such as limited use on specified machines, number of copies used, and time of use.
10. Appropriate protection measures should be taken during personal information exchanges with other on- and off-campus offices. Electronic files should be encrypted and paper-based sensitive personal data should be sealed before transmission to avoid personal information leakage.
11. When leaving their seat, staff members should store sensitive documents and portable information equipment in a lockable cabinet to avoid information leakage.
12. After using a photocopier, printer, fax machine, scanner or multi-function printer, please remove paper-based documents immediately from the machine.
13. Sensitive paper-based documents should be destroyed using a shredder when no longer in use.
14. Computer equipment should not be used to build websites or to serve private or commercial purposes.
15. Viewing of inappropriate content (e.g. violence, pornography, gambling, hacking, malicious websites, phishing scams, botnets, etc.) on the Internet is prohibited during working hours.
16. Personal computers must be protected with a login password that has a minimum length of 6 characters and contains at least a mix of letters and numbers. The password should be updated every six months.
17. Please do not display your password on your computer, monitor or other places where confidential information leakage is likely to occur.

18. When not in use, PCs should be secured by a password-protected screen saver, and the idle time before screen saver activation should be set to 10 minutes or less. Unless required by work, computers should be shut down after work.

19. Computers should be regularly updated to fix vulnerabilities in the operating system and applications by means of update services such as Windows Update, Office Update, Adobe Acrobat updates, etc.

20. Important data kept in PCs should be backed up regularly and stored properly.

21. Anti-virus software should be installed on PCs and virus definitions should be updated regularly to prevent virus attacks and spread.

22. Anti-virus software should be configured to actively perform scans and checks, and such operations should be performed regularly.

23. You should comply with cybersecurity regulations and fully understand corresponding responsibilities when using computers. An act of regulation violation shall be sanctioned with restricted or revoked access to cyber resources in accordance with information security regulations.

24. You shall not steal login IDs and passwords of others by any means when using a computer.

25. You shall not wiretap Internet communications using any device or software when using a computer.

26. You shall not create files containing sexually explicit or indecent content within open cyberspace when using a computer. Spreading sexually explicit messages, pictures, images, sounds or other illegal or inappropriate information on the Internet is prohibited.

27. You shall not send malicious emails to harass others and to cause anxiety and inconvenience when using a computer. You shall not intentionally interfere with or obstruct normal operation of network systems by any means.

28. You should log out and remove temporary files from your browser when you finish using a public computer.

29. When disposing of computers or portable storage devices, please ensure that the data contained is unreadable (which has been destroyed with low-level formatting, degaussing, physical destruction, etc.). The Information Technology Center provides physical destruction services for hard drives.

30. Please ensure your use of personal data complies with legal requirements and confidentiality regulations as stated in the "Personal Data Protection Act."

31. For more information on information security, please visit https://www.itc.ntnu.edu.tw/index.php/promotion/, or visit the official website of NTNU's Information Technology Center and go to Services > Advocacy area > Security.

Office:

New recruit's signature:

Date: