ADVISORY ON DATA PRIVACY WHILE ON WORK-FROM-HOME (WFH)

Help uphold the right to data privacy of individuals whose personal information is processed by UP as well as the confidentiality of University information while working from home.

1. Work in an area of your home where you can secure your computer and other devices as well as the confidentiality of electronic and paper based information. Keep documents in a secure place when not in use.

2. Lock or password-protect your computer and devices. Enable your device's login password and never leave your device unattended without locking it using your password. Log off when not using UP data processing systems.

3. Do not use public unsecured WiFi. Secure your home router by changing the default password when it was first installed. You need to change the router's admin password and add WPA/WPA2-PSK WiFi password. You may Google for instructions that apply to routers provided by PLDT, Globe, Converge, etc.

4. Install verified software updates regularly as these often include patches for security vulnerabilities.

5. When such resources are available to you activate built in fire walls, use antivirus software, VPN and other tools that help secure your access devices. Use the free VPN from protonvpn.com or windscribe.com or for iOS and Android, get the 1.1.1.1 application to protect their traffic. You may refer to the instructions relevant to these VPN tools.

6. If it is necessary to transmit personal information via email you must use your UP Mail account as the mail system uses two-step verification process as required by the National Privacy Commission (NPC). NPC MC 2016-01 also requires that "email attachments containing personal information must be password-protected and such password must be sent on a separate email". In cases when you know the recipient's mobile number, you may send the password via SMS as this will ensure that only such individual would have access to the password.

   See also how to password-protect Office 365 documents at https://support.office.com/en-us/article/protect-a-document-with-a-password-05084cc3-300d-4c1a-8416-38d3e37d6826.

   The following link provides information about how to password-protect Google drive folders that will be shared to those who need to access the same to perform their functions https://websitetipsandtutorials.com/google-drive-password-protect-folder-tutorial/

7. Beware of phishing emails and sites. Be reminded that the University will NEVER ask for your username, password, or any other access credentials. If you encounter any such phishing activities, please immediately contact helpdesk@up.edu.ph

8. DELETE any unsolicited email. If you receive an email from a familiar email address, do not open ANY attachment, and do not click on any link. Send that person a separate email and validate if they really sent the attachment or the link.

9. Report security incidents or personal data breaches involving UP data processing systems. Provide all available information about the nature of the incident or breach including a chronology of events leading to the incident or breach, the information involved (indicate if sensitive personal information eg educational or health records, marital status, age/birthdate, student or employee numbers, or other information that can be used for identity fraud is involved e.g. usernames, passwords) and the number of persons (data subjects) or documents affected. Such report must be made to the unit or office in charge of such system, the relevant IT office, CU data protection officer and the Chancellor's office when CU systems are involved as well as the UP System DPO (dpo@up.edu.ph) and the Office of the UP President (op@up.edu.ph).

For your information and guidance.