THE PRINCE PHILIP DENTAL HOSPITAL

Guidelines on Third Party's Remote Access to Computer Systems and Network of The Prince Philip Dental Hospital

PURPOSE

The purpose of this set of guidelines is to set out procedures on and responsibilities of connecting to The Prince Philip Dental Hospital ("PPDH" or "Hospital") network from external devices via remote access technology by a party other than Hospital staff members, with a view to minimizing the potential exposure to PPDH from unauthorized users and/or malicious attack that could result in information leakage or create possible damage to the PPDH.

2. This Guideline is to be read in conjunction with the following relevant documents:

- Section E6 of Human Resources Manual of the Hospital;
- Service Manual of the IT Office;
- Guidelines on Management of the Administrator Account of an Application System;
- Guideline on the Use of Hospital Windows Accounts, Email Accounts, Access through Personal Electronic Devices and Remote Desktop Connection;
- Guidelines on the Appropriateness to use the Hospital-owned Portable Electronic Storage;
- Guidelines on blocking the websites containing pornography, inappropriate and offensive material;

plus the useful kits of

- Application for the Windows and Email Accounts;
- Application for the Remote Desktop Connection;
- Tips to write an email;

SCOPE

3. These guidelines are applicable to all contractors and other affiliates (vendors, counterparts of the University of Hong Kong and so forth) who utilize their owned devices to remotely access to PPDH's network for performing all work-related activities (hereinafter called "third parties/ party").

4. Hospital staff members should refer to the relevant provisions in the Section E6 of the Human Resources Manual as well as other relevant documents as mentioned in Section 2 herein for the procedures and the relevant guidelines.

5. Remote access is the ability to securely access to PPDH's systems, applications or data that can normally only be accessed within the internal PPDH network, including but not limited to:

(a) Internal administrative/ academic systems
(b) Documents/ files located on internal file servers
(c) Servers

APPLICATION FOR REMOTE ACCESS

6. All third parties requiring remote access to PPDH's systems, applications or data should write to the PPDH Information Technology Office ("ITO") outlining the following information:

(a) name of the PPDH's system, applications or data involved;
(b) justifications for the remote access;
(c) period of the remote access;
(d) name of the personnel accessing to the related system, applications or data (hereinafter called "the responsible personnel");
(e) tile of the responsible personnel;
(f) email address of the responsible personnel;
(g) telephone number of the responsible personnel; and
(h) an indication that "I/ Our company agrees to abide and be bound by the "Guidelines on Third Party's Remote Access to Computer Systems and Network of The Prince Philip Dental Hospital".

7. On receipt of an application, a System Administrator ("SA") of PPDH shall scrutinize the application and assessing its urgency, potential risks and operational needs before making a recommendation to Hospital Administrator 1 ("HA1"), or Senior Hospital Administrator 1 ("SHA1") during his/her absence, who is the approver of such request.

8. After securing the approval from HA1/ SHA1, an officer of the ITO at a rank not lower than ASA should reply the applicant as follows:

(a) informing the application result;
(b) informing the period of remote access;
(c) attaching the "Guidelines on Third Party's Remote Access to Computer Systems and Network of The Prince Philip Dental Hospital";
(d) reminding the applicant to observe and follow these guidelines again;
(e) reminding the applicant that an application for extension is needed if the scheduled works cannot be completed within the approved period.

RESPONSIBILITY OF THE THIRD PARTY

9. It is the responsibility of all third parties who have access to PPDH network in a remote location to ensure that their devices and connection is given the same security considerations as their on-site connection. It is imperative that any remote access device / connection used to conduct PPDH business be utilized appropriately, responsibly, and ethically.

10. The third party/ responsible personnel must deploy a device that contains proper security/ protection measures to access to PPDH network, including but not limited to:

- ✓ Valid and up-to-date virus protection;
- ✓ Malware protection; and
- ✓ Maintaining latest version of operating system and application security patches.

11. The third party/ responsible personal must treat any information/ data viewed or obtained through remote access in the strictest confidence, which should be protected by all practicable steps.

12. The third party/ responsible personal must not duplicate, store, transfer or disclose any information/ data, in any form, as viewed or obtained through remote access without the written agreement of the Hospital.

13. The third party could only assign the responsible personnel as stated in the application to get access to PPDH's network, and should obtain the prior approval of PPDH for any change of responsible personnel.

14. The third party/ responsible personnel must notify ITO of PPDH about any possible infections during the remote access, as well as any incidents or suspected incidents of unauthorized access and/or disclosure of PPDH information.

15. The third party/ responsible personal should note, agree and accept that his or her access and/or connection to PPDH networks may be monitored or recorded in order to identify unusual usage patterns or other suspicious activity.

16. If PPDH finds any suspicious activities/ actions are being/ have been undertaken by the third party or the responsible personnel, PPDH reserves the right to seek assistance from any law-enforcing agent(s) for investigation or even prosecution without seeking clarification from the third party or responsible personnel concerned.

Last updated in September 2021
Edited by IT Office of PPDH