THE PRINCE PHILIP DENTAL HOSPITAL

Guidelines on Management of the Administrator Account of an Application System

PURPOSE

The purpose of these Guidelines is to set out how the system owners should manage the "Administrator" account of an application system.

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

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 apply to all relevant staff members of the Hospital.

MANAGEMENT OF THE ADMINISTRATOR ACCOUNT

4. The "Administrator" account of an application system usually enables the owner of the "Administrator" account to:

(a) have full spectrum of the user account management of the system, including creation or deletion of a user account for a staff member/ student, assignment of roles, functions and permissions to each user account, etc…; and/ or

(b) view, modify, copy or destroy any data/ information in the application system.

Last updated in September 2021
Edited by IT Office of PPDH

5. The owner of the "Administrator" account should comply with the following guidelines when using the "Administrator" account:

(a) Create user accounts to other staff members/ users on a need basis.

(b) Remove or suspend any user accounts as soon as possible when the users leave the Hospital or are transferred to another section/ unit/ clinic/ office.

(c) Assign the appropriate roles, functions and permissions to each user account, with reference to the rules/ guidelines/ regulations/ manuals of the Hospital or the respective section/ unit/ clinic/ office.

(d) Review the roles, functions and permissions of each user account regularly.

(e) Change the password of the "Administrator" account at least once a year. For adoption of strong password, please refer to the relevant clauses in the Section E6 of the Hospital's Human Resources Manual and other relevant document as mentioned in Part 2 stated herein.

(f) Never view, modify, copy or destroy any information or data kept at the system unnecessarily.

(g) Always bear in mind that the owners of the "Administrator" account are placed in a position of trusted and entrusted with certain powers by the Hospital, and that they must manage or use the "Administrator" account responsibly, carefully and for official business only.

6. Staff members misusing the "Administrator" account may not only subject themselves to disciplinary action of the Hospital, but also criminal liability.

OWNERSHIP

7. In view of the sensitivity, the owner of the "Administrator" account should be of appropriate rank. Unless with strong justifications as approved by the Comptroller, system owners should assign the use of the "Administrator" accounts to staff members as follows:

System Owner	Rank
Operating System owned by the Information Technology Office ("ITO")	Assistant System Administrator or above

System owed by section/ unit/ clinic/ office other than ITO	Supervisory Rank at Clerk-in-charge, Senior Certificated Dental Surgery Assistant, or equivalent, or above

MASTER LIST

8. ITO shall keep a master list on the name and post of the owner of the "Administrator" account of each application system. To this effect, ITO shall call a return from all system owners **annually**. That said, system owners should update ITO as soon as possible when there is a change in the ownership of the "Administrator" account.