加強資訊保安

本署謹此提醒 貴公司注意資訊保安及保護個人資料，並確保遵從香港的《個人資料（私隱）條例》。

資訊科技的發達，特別是互聯網的廣泛應用，為社會帶來不少好處，不過，與此同時，網上襲擊的次數日益頻密及多樣化，資訊保安所面對的威脅亦愈來愈大。任何資訊保安事故，例如數據泄漏均足以構成嚴重的影響。

政府資訊科技總監辦公室特別提醒我們資訊保安管理責任的重要性。政府資訊科技總監辦公室的一站式資訊保安入門網站（網址：http://www.infosec.gov.hk）提供了有關這課題的最新消息及參考資料。

貴公司是本署的註冊電業承辦商，本署現誠邀 貴公司撥冗瀏覽上述網站。相信 貴公司定會覺得網站所載的資料十分有用。附錄亦載列了一些重要提示，以供參考。

謹對 貴公司的支持表示謝意。

Enhancement of Information Security

We wish to remind your company to take care of information security and protection of personal data, and to ensure compliance with the Personal Data (Privacy) Ordinance in Hong Kong.

While the society has benefited from advances in information technology and the Internet in particular, the frequency and diversity of cyber attacks and information security threats have also continued to grow. Any information security incidents such as data leakage may have serious impacts.

In this regard, the Office of the Government Chief Information Officer (OGCIO) has drawn our attention to the importance of management responsibility in information security. The one-stop information security portal of the OGCIO http://www.infosec.gov.hk provides latest news and up-to-date reference on the matter.

As an electrical contractor registered in this department, you are cordially invited to spare some time to visit the above website. I trust that you will find the information contained therein useful. Some tips are also provided in Appendix for your reference.

Thank you for your kind support on the matter.

附錄

資訊科技保安政策及指引提示

資訊系統用戶是實際使用資料的人員，他們須為自己在資訊系統進行的一切活動負責。用戶應盡量了解、認識、遵從及運用一切可行及可使用的保安機制，盡量防止他人未獲授權而使用其電腦及工作站。

在傳輸過程中，須將個人資料加密。另外，必須將連接電腦系統或網絡的身份驗証技術（例如：鑰匙、智能卡或密碼等）鎖於安全的地方，或按明確和嚴格執行的保安程序處置。

電腦病毒及惡意程式碼

在使用前，以防毒程式檢查抽取式媒體及附加檔案（特別是不明來歷的檔案）。

如果用戶懷疑電腦已感染病毒，應停止使用該電腦，因? 繼續使用懷疑受感染的電腦可能會令情況迅速變壞。

存取控制

1. 應　動附設密碼的屏幕保護程式。
2. 在未獲授權的情況下，嚴禁複製、竄改或在未獲特許使用權下使用軟件或硬件。
3. 小心放置顯示機密資料的個人電腦、工作站或簡易終端機屏幕，以免被未獲授權的人士窺看。
4. 在辦公時間外，關掉個人電腦。

揀選密碼指引(10 個不應 / 5 個應)：

1. 不應使用任何形式的登入名稱（原形、倒寫、大寫、重複等）。
2. 不應寫下你的密碼，特別是將密碼放在電腦附近或儲存在檔名有「密碼」（password）一詞的檔案內。
3. 不應使用任何形式的本人姓氏或名字作為密碼。
4. 不應使用配偶或子女的姓名作為密碼。
5. 不應使用他人容易取得的其他個人資料作為密碼，包括身份證號碼、車牌號碼、電話號碼、出生年月日、居所街道名稱等。
6. 不應使用完全由數字或由相同字母組成的密碼，例如“123456”或“aaaaaa”。
7. 不應使用能夠在英語或其他外語詞典中查到的詞彙。
8. 不應使用少於六個字符組成的密碼。
9. 不應在任何情況下向任何人士洩露你的密碼，使密碼不受控制。
10. 不應重新採用已使用過的密碼，縱使該密碼已很久沒有使用過。

11. 應使用大小寫不一的字母。
12. 應使用由字母及非字母字符（數字或標點符號）混合組成的密碼。
13. 應使用不容易猜到但方便用戶本人記憶的密碼，以避免將密碼寫下。
14. 應使用無須眼看鍵盤即能快速輸入的密碼。
15. 應每四至六星期更換密碼。

Appendix

Tips on IT Security Policy & Guidelines

Users of Information Systems are persons who actually use the information and they shall be accountable for all their activities on the Information Systems. They should know, understand, follow and apply all possible and available security mechanisms to the maximum extent possible. They have to make their best effort to prevent unauthorized access to their computers and workstations.

Personal data shall be encrypted during transmission. All access keys, cards, passwords, etc. for entry to any of the computer systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures.

Computer Virus and Malicious Code

It is a good practice to check every removable media and attached files (especially those of unknown origin) with a virus scanning program before use.

If a machine is suspected to have been infected by virus, all activities on that machine should be stopped immediately. Continued usage of the machine may cause a serious deterioration of the situation.

Access Control

1. Password protected screen saver should be activated.
2. Unauthorized copying, modification or unlicensed use of the software or hardware are strictly prohibited.
3. The display screen of a personal computer, workstation or dumb terminal on which classified information can be viewed shall be carefully positioned so that unauthorized persons cannot readily view it.
4. Power off personal computer after office hours.

Password Guidelines (10 DON'Ts & 5 DOs)

1. Do not use your login name in any form (as-is, reversed, capitalized, doubled, etc.)
2. Do not write down your password, particularly anywhere near the computer or file it with 'password' marked.
3. Do not use your first, middle, or last name in any form.
4. Do not use your spouse's or child's name.
5. Do not use other information easily obtained about you. This includes license plate numbers, telephone numbers, birth dates, the name of the street you live on, etc.
6. Do not use a password of all digits, or all of the same letter, e.g. "123456" or "aaaaaa".
7. Do not use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
8. Do not use a password with fewer than six characters.
9. Do not tell or give out your passwords even for a very good reason. Out of your hands, out of your control.
10. Do not reuse a password, even if it has not been used for a long time.

11. Do use a password with mixed-case alphabets.
12. Do use a password with a mix of alphabetic and non-alphabetic characters (digits or punctuation).
13. Do use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
14. Do use a password that you can type quickly, without having to look at the keyboard.
15. Do change your password every four to six weeks.