紀錄編號：□□□-□□

1. 系統之使用者應至少每 6 個月更換密碼一次，更換密碼時不可使用相同的密碼。密碼的長度最少應有 8 位長度，且應符合密碼設置原則。
2. 電腦應設定螢幕保護程式與登出時間 10 分鐘並設定密碼保護。
3. 帳號密碼必須妥善保存，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知單位資安窗口與圖書資訊處。
4. 電腦之作業系統漏洞應即時更新修補，開啟電腦自動更新功能。
5. 應定期將重要資料備份存放。
6. 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，不得使用個人私有資訊設備及大陸資通訊廠牌產品，公務設備亦不得連結個人私有手機上網。
7. 若有業務上的需求必須使用大陸資通訊廠牌產品(含硬體、軟體及服務)時，應具體敘明理由，經本校資安長及其上級機關資安長逐級核可，函報主管機關核定後，以專案方式購置，並列冊管理。
8. 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知單位資安窗口與圖書資訊處。
9. 不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。
10. 公務資料傳遞及聯繫必須使用公務電子郵件帳號，不得使用非公務電子郵件傳送或討論公務訊息。
11. 即時通訊軟體使用應注意不得傳送公務敏感與機密資料。
12. 業務所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。
13. 傳送公務資訊應有適當保護，例如加密傳送。
14. 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。
15. 不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本單位敏感等級（含）以上的訊息。
16. 未遵守資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。

17. 有資安疑慮或異常時，應即時通報單位資安窗口與圖書資訊處。

18. 新進人員應填具「保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

19. 應遵守個人資料保護法及資通安全管理法及機關資通安全管理制度。

20. 資安管理制度及相關文件存放位址：國立東華大學資通安全網\ISMS 專區。

入職單位：

新進人員簽名:

中華民國　　　年　　　月　　　日

For referenc

Information security information leaflet for new employees

(此版本為外籍人員對照參考用,無需填寫繳交,簽署仍回到中文紙本簽名)

This version is for reference by foreigners. There is no need to fill in and submit. The signature will still return to the Chinese paper signature.

1.System users should change their passwords at least once every 6 months. The same password cannot be used when changing passwords. The password should be at least 8 characters in length and should comply with the password setting principles.

2.The computer should be set with a screen saver and a logout time of 10 minutes and be password protected.

3.The account password must be properly kept and comply with agency regulations. If there is any concern about leakage, in addition to changing the password as soon as possible, the unit's information security window and library and information office should be notified.

4.Computer operating system vulnerabilities should be updated and patched immediately, and the computer’s automatic update function should be turned on.

5.Important data should be backed up and stored regularly.

6.Information equipment, networks, and required software provided by the agency must be used in the office environment. Personally owned information equipment and products of mainland information and communication brands are not allowed to be used, and official equipment is not allowed to be connected to personal mobile phones for Internet access.

7.If there is a business need to use mainland information and communication brand products (including hardware, software and services), the reasons should be stated in detail and approved step by step by the Chief Information Security Officer of the school and the Chief Information Security

Officer of the superior agency. After reporting to the competent authority for approval, it will be purchased on a special project basis and listed in a register for management.

8.During work hours, you should not link to websites that are not required for official purposes, and avoid linking to malicious websites or phishing websites. If you find any abnormal connections, please notify the unit's information security window and the Library and Information Office.

9.Do not use official email accounts to register as accounts for non-official websites, such as social networking sites, e-commerce services, etc.

10.Official email accounts must be used to transfer and contact official information. Non-official emails are not allowed to be used to send or discuss official information.

11.When using instant messaging software, be careful not to transmit official sensitive and confidential information.

12.All computer software used in business must have legal copyright, and personnel are not allowed to install illegal computer software without permission.

13.The transmission of official information should be appropriately protected, such as encrypted transmission.

14.If paper documents with information of sensitivity level (including) and above are no longer used, the paper should be destroyed with a paper shredder.

15.Do not disclose in any public news groups, forums, or bulletin boards any information related to the unit's sensitivity level (inclusive) or above.

16.Failure to comply with information security regulations will result in a warning for the first time.

If this continues or those who do not listen to the advice will be punished in accordance with the regulations; if an information security incident occurs as a result, the punishment will be increased.

17.If there are any concerns or abnormalities regarding information security, the unit’ s information security window and library information office should be reported immediately.

18.New employees should fill out a "Confidentiality Agreement" and promise that during their tenure, any information they learn from their duties or any data, files, technology, finance or business secrets they hold will not be disclosed to anyone without the authorization of their supervisor. disclosed or misused.

19.The Personal Data Protection Act, the Information Security Management Act, and the agency’ s information security management system must be complied with.

20.The information security management system and related documents are stored at: National Donghua University Information Security Network\ISMS Zone.

Employed unit：

Signature of new employee：

Y M D