The Hong Kong Polytechnic University

Department of Aeronautical and Aviation Engineering

2022-2023 Semester 2

ENG3004 Society and the Engineer

Individual Assignment 1

Name: Choi Hon Lam

SID: 22034805D

Answer:

When handling the confidential document, we can define them into different class of security based on the risk of exposure and the level of sensitivity. Through the classification, we can apply different strategies to protect different types of information. To make a precise management, evaluation should be done on a regular basis.

Complementing access control can be taken place in electronic information. Reduction in the distribution of sensitive information can effectively minimize the risk of leakage and the misuse of sensitive information. Limiting user access to the files by applying the principle of the need-to-know, need-to-do and need-to-use will prevent the distribution of unnecessary sensitive files to unrelated personnel, lowering the risk of leaking and misuse of sensitive information. Additionally, the needed document should be distributed to the individual account with password to ensure the limitation on distribution.

Personal passwords can be used to restrict access to computer information. Passwords should be kept private and changed on a regular basis. Easy-to-guess password such as consecutive numbers 123456 should be avoided. Additionally, multi-factor authentication such as the security question which only known by users can also be complemented to ensure only user themselves are able to access their accounts. Furthermore, when accessing the confidential document, a Virtual Private Network (VPN) can be connected to hide the Internet Protocol (IP), preventing the confidential document from being leaked.

Simultaneously, more can be done on protecting sensitive information in hard copy. The confidential documents should be locked in a designated cabinet located in a restricted access room that only authorized personnel have access. Throwing fully shredded sensitive documents into the confidential waste bin can prevent the reform of destructed sensitive documents when dealing with discarded sensitive documents.

For ensure the safety of sensitive information, audit trail system can be installed into company computers to achieve the access control monitoring. Since the audit trail records all the information about transactions and processes for review in the future, it improves audit security. At the same time, every company's computer should have a monitoring system installed. The monitoring system will be used to monitor suspicious behaviors such as making unusual copies on sensitive information. When suspicious action was alerted by the trail system, investigation will be carried out and disciplinary action will be taken if the misuse of sensitive information is proven. Furthermore, the application should be configured to detect unauthorized access attempts, allowing company to reinforce their security system.

Since employee poses the greatest danger for leaking company’s confidential information, regular security awareness training on how to handle and store sensitive information should be provided. The confidentiality policies should be reviewed on a regular basis to ensure their effectiveness in risk reduction. Employees should be alerted of the serious consequences of disclosing or abusing proprietary information. Aside from education, regularly updating clear guidelines on how to safely keep and handle privilege information should also be issued as a reference. The slogan "Handle sensitive information safely" can be posted in the workplace as reminder.

Likewise, a non-disclosure agreement (NDAs) can be implemented to provide a sufficient deterrent against the misuse of sensitive information. Employees should always be prohibited from leaking or misusing of the sensitive information since the disclosure of sensitive information will be detrimental to a company. The non-disclosure agreement should be in place not only during the employees' employment but also for a specified period after they leave the company。

Reference

Schwegman, Lundberg & Woessner. (2021, November 17). *Protecting & Handling Confidential Information*. Schwegman Lundberg & Woessner. https://www.slwip.com/resources/protecting-handling-confidential-information/

***Chapter 8-Protecting Your System: User Access Security, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics)*. (n.d.).** **https://nces.ed.gov/pubs98/safetech/chapter8.asp**

AuditBoard. (2023, February 17). https://www.auditboard.com/blog/what-is-an-audit-trail/

Chapter 8-Protecting Your System: User Access Security, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics). (n.d.-b). https://nces.ed.gov/pubs98/safetech/chapter8.asp