

ENG 3004 Assignment one

Student Name: Kwok Chun Yin

Student Number: 22019626D

Nowadays, many company involves secret document like bank and law firm. There are a lot of personal data to tackle by them including contact, address, and other information. Internet is very convenient for everyone to share and save anything. It is easy to disclose if it saves to the online drive, then may be of use to competitors or harmful to the client. On above the case that I will suggest how the company can ensure certain that the privileged information. I will assign three part to explain it.

1. New employee

For Company,

Company needs to assess all employee background personal information before joining the company. Company should also make a statement in the contract and provide guidelines for handling confidential information so that employees can clearly understand and sign it. In case of violation, legal proceedings will be initiated.

For employee,

Employees should report all the information related to work before joining the company such as children's stages work or study, related investment projects and past work experience to ensure that there are no conflicts of interest. Employee must understand company rule since you need to follow.

2. On working

For company,

Restrict access to confidential files

Only the responsible employee and supervisor of the work are eligible to view privileged information. There can protect the privacy of customers or the company's property. It cannot cause unnecessary trouble for employees because if there is any problem with the documents, it will not implicate all employees of the company. However, the company will easily investigate and solve it immediately. One of example of DBS bank, the company use high security to tackle the privileged information. The company will provide computer(notebook) for everyone. All the customers documents need to view in that computer. Also, if some customers information documents need to connect company network IP to computer, then it can be watched. In addition, the privileged information do not print it out for record since it have a change to loss and copy. This way can ensure no employee to share

document to public and other platform.

Sign a privileged agreement

In order to protect certain public figures or internal company information. I would recommend that all employees who come into contact with these documents sign this privileged agreement, and once this information is leaked, company may also investigate and exclude unrelated persons. Legal liability is included in the agreement, and the company has the right to require the responsibility of the employee.

Employee training

The company should teach employee that do not see company document in public network because it is easy to hack. Employees who are equipped to recognize risks might help a firm, its stakeholders, and its reputation avoid potentially detrimental circumstances. When a company invests in continual training, its employees understand the importance of appropriately releasing and preserving private information, and information security becomes ingrained in the organization. (n.d.) This way can protect the benefit of every employee because training boosts our safety awareness.

For employee,

Managing files

Employees need to clean important documents on their desks regularly. If they leave their own seats, they need to put privileged files in locker and the computer should be locked to safeguard the privacy of document. All employees cannot bring privileged files to leave company. For example, Gary Cheng, a former legislator, is found guilty in District Court of corruption, false account, theft, and conduct in public office as he obtains privileged information from the leisure and sports development council, and then leaking the documents and making benefit. When the file had finished, all relevant documents should be destroyed or encrypted. Those documents are including many privacies of supplier or company. All data should be deleted to the greatest extent possible. Company can hire professional company to address the privileged information. It can provide a closed document destruction system and control, so that no one will touch the destroyed material during the transportation and destruction process. The entire destruction process can also have video surveillance record. Next, transfer files ensure that there is no other copy. At the same time, finding a program to clean hard disk or memory devices because the general cleanup may be restored by human and the files will be leaked.

3. Quit a job

For company,

Company may confirm the employee to quite the job that do not bring customers information. Then, all electricity information should be delated by IT department. Base on contract detail, employee do not disperse privileged information to everyone. If no, employee may have law trouble. For instance, one of the internal staff of Credit Suisse said that an employee who had left Credit Suisse copied some employee data like ID card sex, address, and bank account to personal devices without Credit Suisse's authorization before leaving. Thus, company need ensure them do not copy company data.

For employee,

Employee must not bring any files to leave company after quitting the job. All the files are company property especially privileged information. They should voluntarily return all documents to the company. If the company discovers that there is a data breach after the employee leaves, company will take all legal action. According to cheater 486 of personal Data (Privacy) ordinance, A data user shall not carry out, whether in whole or in part, a matching procedure—unless and until each individual who is a data subject of the personal data the subject of that procedure has given his prescribed consent to the procedure being carried out. (Hong Kong Government, 1996) if employee leaved company, all document are not from you to handle. Employee have not right to touch and contact the customer or supplier. This way to protect all data in the company.

Reference

How Do You Protect Confidential Information in the Workplace?(n.d.).

Blue-Pencil. <https://www.blue-pencil.ca/how-do-you-protect-confidential-information-in-the-workplace/>

Personal Data (Privacy) Ordinance. (1996, August 1). Hong Kong

Government-Elegislation. https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK?INDEX_CS=N

