

ENG 3004 Individual Assignment 1

Name: Ng Ho Kwan

Student id: 22001021D

Preservation of confidential information entrusted to engineer should be handled in strict compliance with ordinance and with his own moral obligation.

As for professional attitude and ethical rules of their profession, engineer have a duty of loyalty to clients and employers that requires them to preserve confidential information that is or is not proprietary to company.

But to prevent any non-compliance which affects the company's ability to compete in the market, the company should also make certain that the privileged information is handled properly by the employee, by the following measures:

1) Implement proper access control

Classify information into different security groups based on their risk exposure and degree of sensitivity. Classification should be reviewed regularly.

Approve access rights on the basis of a practical application of the need-to-know, need-to-do, and need-to-use principles i.e. only those staff who have genuine need to use the information during the course of duty can have access to the classified information.

Restrict access to computer information by using passwords and the passwords should be changed regularly. Set up an audit trail system for computer systems for identifying persons who have gained access to information in order to facilitate future investigations and access control monitoring.

2) Monitor release of information

Provide clear guidelines on how to safe keep and handle release of classified information and on how to ensure computer security.

Monitor release of information according to the need-to-know, need-to-do, and need-to-use principles.

Obtain the employer's and clients' authorisation before disclosing confidential information relating to them.

3) Exposure proper management controls

Clearly communicate company's policy on preservation of confidentiality to all levels of staff. Such policy should be reviewed regularly to assess its effectiveness in risk minimisation.

Alert staff of the serious consequences of leaking/ abusing proprietary information.
Require staff to sign agreements not to leak or misuse proprietary information during their employment and for a specific period after they have left the company, if necessary.