

OFFICE PRACTICE (DES 1103)

LECTURE : 3

TOPIC : Office Security

AIM : To understand the importance of security in the office

LEARNING OUTCOMES:

After completing this chapter you should be able to understand:

1. What are the security measures to be taken in all situations in the office.

TOPIC OUTLINE

- 3.1 Security at the workplace
- 3.2 Safeguards for maintaining confidentiality
- 3.3 Security of computerized data
- 3.4 Guidelines for the security of valuables
- 3.5 Security of Buildings

NOTES

3.1 Security at the workplace

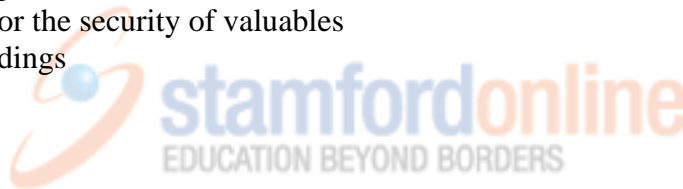
Security has become an increasing problem for offices. Security is focused on:

- The physical security of the property or tangible items from theft, break-ins and vandalism.
- Security of information. This covers such things as breaches of company security and industrial espionage, which might involve anything from the theft of a company's designs, its R&D plant, and its client lists or even its wage rates.

Organizations need to review their security arrangements and undertake what is termed 'risk management'. This is an exercise designed to identify, evaluate and judge potential areas of risk. Security measures need to be introduced to minimize problems. The staff need to be aware of the procedures in operations.

Security risks could be avoided or reduced and the types of things, which are likely to be considered, are:

- Access potential and car parking arrangements
- The roles of the gatehouse, and reception staff
- Alarm systems
- Guard dogs



- Closed-circuit television
- The vetting of staff
- The issue and control of keys, particularly master copies
- Alternative to keys, e.g. the use of code numbers
- The introduction of identity cards and visitor's badges
- Restricted access areas
- Restricted handling of confidential information
- Frequent audits of computer systems and users
- The introduction and frequent changing of computer passwords.

3.2 Safeguards for maintaining confidentiality

- Follow and implement security and confidentiality procedures at all times.
- Never leave confidential records lying around when you leave your office – be sure to lock them away when they are not in use.
- Place confidential records in a folder so that they are not immediately visible to an onlooker.
- Classify and control confidential, private or secret records by marking them accordingly.
- Position your desk in such a way that visitors to your office will not be able to read confidential documents while they are being processed – if this information is displayed on your word processor screen, it may be necessary to scroll it away temporarily when visitors are present.
- Supervise visitors so that they are never left alone at any time in your office or your employer's office.
- If confidential documents have to be reproduced on a copier, it may be desirable for the secretary to do this to ensure that the contents are not disclosed to others.
- If asked for confidential information by an unauthorized person, use tact and diplomacy to evade the question and explain that you have no authority to supply such information and that enquiries should be made elsewhere.
- Take care when supplying confidential information on the telephone that the caller is authorized to receive it.
- Avoid confidential telephone information being overheard by others – this may entail ringing back when you are alone in your office or transferring the call to a more private office.
- Any confidential or secret documents no longer required should not be put in the waste paper bin but destroyed in a shredder or incinerator.
- Take as much care over confidential computerized data and recorded data on dictation machines as you would with documents.
- Inform your manager immediately of any breaches of security you see or which are brought to your attention.

3.3 Security of computerized data

Special precautions must be taken to safeguard computerized data against loss or corruption and this may entail:

- Keeping back-up duplicate copies of disks in a secure place.
- Arranging for personal passwords to be used by the staff authorized to have access to the computer, the passwords being changed at regular intervals.
- Using codes, known only to the users, for document files.
- Using write-protect tags on system disks to prevent data from being altered or added to them.

3.4 Guidelines for the security of valuables

- **Cash**
 - Check sums of money carefully when receiving and paying them
 - Lock any cash held in the office in a cash box and keep it in a safe
 - Never leave the office unattended with the cash box unlocked
 - Ensure that every payment of cash is supported by a voucher or receipt
 - Pay money into the bank as soon as possible after receipt to avoid the security risk of holding money on the premises
 - If large sums of money have to be transported to and from the bank, security agency staff will normally be employed. If the office staff has to undertake this task, two people should go, using a specially designed cash-carrying case and, if regular journeys are made, vary the route taken.
 - Spot checks should be made regularly on any transactions involving the transfer of money and any discrepancies brought to the attention of the Manager.

- **Equipment**
 - Maintain an inventory, i.e. a written record of all equipment held, and include serial numbers and any distinguishing marks.
 - Mark all items of equipment by engraving them or by writing on them with an ultra-violet marking pen so that they are easily identifiable.
 - If any item of equipment has to be borrowed, record the name of the person borrowing it in the inventory.
 - Make a regular 'stock-taking' check of equipment, investigate and report any deficiencies.

3.5 Security of buildings

Security of premises can be controlled by restricting access to authorized personnel and adopting some of the following procedures:

- Issue all employees with photo-identity cards to be worn at all times.
- Use coded electronic cards incorporating pre-programmed number combinations or computerized cards for staff to operate door locks, allowing only those authorized to enter premises – cards may carry an employee photo ID which is photographically or digitally reproduced.
- Issue visitors and contractors with passes to be worn at all times
- Maintain a visitor's book and also keep a record of all permanent and temporary passes issued.
- Arrange for visitors to be met and returned to the reception office by their hosts.
- Employ security officers to control the admission of visitors and contracting staff.
- Use a closed-circuit television for surveillance of buildings – a time-lapse video system offers 24-hour surveillance, and the input from up to 16 video cameras can be recorded on one tape, providing up to seven days' recall.
- Install public address equipment throughout the building to enable emergency announcements to be made to all occupants.
- Use a Central Alarm Monitoring Station with a round-the-clock manned national communications centre, to provide monitoring and management services for controlling both electronic systems and security of premises – a computer system reports and logs all system transactions. Any alarm or default is automatically brought to the attention of the CAMS operators, who ensure a swift and efficient response by the firm's security staff.

REFERENCES:

1. Helen Harding, *Secretarial Procedures – Theory and Applications*, (2nd Edition)
2. John Harrison, *Secretarial Duties*, (10th Edition)

TUTORIAL QUESTIONS – WEEK 3

1. Mr Patrick Moreland, Operations Director of Nestle (M) Bhd, is concerned about the leak of confidential information to which several members of staff may have had access.
 - a) How would you deal with this matter?
 - b) What steps could be taken to try to prevent any further leaks?
2. There has been a spate of thefts from Nestle (M) Bhd recently. Prepare a memorandum to administrative staff setting out preventive measures to be undertaken by themselves and Nestle (M) Bhd.
3. The organization you work for handles top secret information, which could be of use to unscrupulous competitors. Naturally businessmen from other companies must visit your offices but what arrangements could be made to minimize the security risk presented by visitors?