NATIONAL OPEN UNIVERSITY OF NIGERIA

CSS 245

Security Planning, Development & Management

Module 3

CSS 245 (Security Planning, Development and Management) Module 3

Course Developer/Writer
Mr. Darlington Ikpi, National Open University of Nigeria

Course Editor
Dr. U.I Adeyinka Aderinto, National Open University of Nigeria

Course Coordinator
Dr. Niyi Adegoke, National Open University of Nigeria

Programme Leader
Dr. N. Nwabueze, National Open University of Nigeria

Credits of cover-photo: Henry Ude, National Open University of Nigeria

National Open University of Nigeria - University Village, Plot 91, Cadastral Zone, Nnamdi Azikiwe Expressway, Jabi, Abuja-Nigeria.

www.nou.edu.ng centralinfo@nou.edu.ng
oer.nou.edu.ng oerunit@noun.edu.ng OER repository

Published in 2012, 2014, 2021 by the National Open University of Nigeria

Unit 1 Basic Principles of Ethics

1.0 Introduction

Ethic is derived from the Greek word ethos, and this refers to a person's fundamental or basic orientation towards life. The Latin translation of ethics is *Mos* or *Moris*. From Moris we have the word moral. Ever since then, the word has attracted voluminous Literature, but with more universally accepted definition by writers in this field. Often, attempts had been made by a number of writers to draw a distinction between morals (What people do) and ethics (what they think they ought to do).

2.0 Objectives

At the end of this unit, you should be able to:

- define ethic from Ethos and Morals from Moris
- summarize major attributes of ethics
- discuss sources of security ethics
- mention various purposes of professional ethics
- explain the factors of higher ethical Standards
- list many approaches of standing orders for security personnel.

3.0 Main Content

3.1 Meaning of Ethics

Ethics is therefore a mass of moral principles or sets of values about what conduct to be. It may be specified by a written and unwritten set of codes or principles governing a profession (Steiner, 1975).

3.1.1 Attributes of Ethics

There are five major attributes of ethics that constitute the moral approach and consideration to a person's fundamental or basic orientation towards life. They are concept, content judgment, standard and values. However these are summarised as follows.

3.1.2 Concept

The field of ethics can be conceived as a discipline, science, study or evaluation.

3.1.3 Content

The subject matter of ethics is concerned with what is good or bad, right or wrong. Words usually encountered in discussion of ethics are true, fair, just, right and proper etc.

3.1.4 Judgment

Judgment is required to determine whether human action is ethical or not. There are concerns over acts, not the motivation behind it. Behaviour and not its cause is that which is judged.

3.1.5 Standards

Judgment is based upon standards that are of course values.

3.1.6 Values

The final element of ethics is the set of values and criteria used as standards for judging human conduct.

3.2 Security Ethics

Security ethics is therefore directly related to the conduct of security practitioners. It is concerned essentially with the impacts of security decisions on people, within and without the organization individually and collectively, in communities and other groups. Ethical behavior is a conduct that is considered fair or just, measured by ethical rules, and which must be obedient to valid government laws and regulations.

The argument further goes that security practitioners are human beings with ethical values that cannot be separate from their normal organizational lives. Therefore more and more security decisions should cover ethical and moral issues. This is in spite of the basic fact that broad ethical norms are fuzzy, there are rarely detailed rules of conduct; and where they exist, they are found to be contradictory and sometimes confusing. In any case, Nigeria Security practitioners should be more ethical in their conducts and this conforms to the assertion that, a morally responsible security in particular situation that has clear idea of what values hold, ascendance over others in practice.

3.2.1 Sources of Security Ethics

There are five principal repositories of values influencing security practitioners and managers. These are religious, philosophical, cultural, legal and professional codes systems.
Religious System

Most fundamental perception or conception of what is right or wrong in life is rooted in biblical morality. The society believes that moral values are of divine atheistic origin and often rest on atheistic foundation. Most religions in their tenets emphasise that, the social responsibilities of people is to act in such a way as to contribute to the welfare of the society. Alternatively, men should not act to harm it (i.e. society) in any way.

3.2.2 Philosophical System

An important source of ethical conduct come from the views of great thinkers like Plato, Socrates, Aristotle, etc. all these men had a great deal to say about ethics. For example, Aristotle laid down the Golden Rule: "we should behave to friends as we would wish them

to behave to us". Immanuel Kant (1724-1804) tried to find universal Laws of morality to guide men's conduct. Jeremy Bentham (1749-1832) developed a utilitarian system as a guide to ethics. This concept was perfected by John Stuart Mill, David Hume and John Locke in the nineteenth century. These great philosophers did develop standards of ethics, and their beliefs are measures of ethical standards in contemporary society.

3.2.3 Cultural System

The socio-cultural dimension includes the customs, norms, beliefs and values which characterize the environment in which the societal practitioner and organizations operate. These cultural factors have the dominant ethics of preserving the social system. Appropriate standard of security practice/conduct vary across cultures.

3.2.4 Legal System

The law is a confiscation of customs, ideas, beliefs, and ethical standards which society wishes to preserve and enforce. A web of law, regulations and court decisions encircles every security practitioner and manager. Some are designed to protect workers and consumers. Others are designed to make contracts enforceable and to protect property rights. Many are designed to regulate the behaviour of security mangers and their subordinates in organizations. There is relatively little that a security manager can do in any organization that is not in some way concerned with, and often specially controlled by a law or regulation. The law cannot cover all ethical conducts

It has been observed to the dismay of security managers and organizations that the legal and legislative environment is confusing and full of loopholes, when it comes to interpretation, and ambiguous where two or more bodies are directly involved in the enforcement of any law, the internal jurisdictional questions have to be resolved first.

Often this resolution takes time. These legal interpretations, ambiguities and bureaucratic entanglements usually make it very difficult for our security managers to know exactly what course to take or what decision to make. Also, some security practitioners and managers have taken advantage of these loopholes to engage in unethical practices.

3.2.5 Professional Codes System

Professional codes are becoming a major source of ethical norms for security practitioners and managers. Three broad types of these codes have been identified. First are company creeds or philosophies, which are usually short, widely distributed and cover those basic philosophies that presumably govern the organisation. There is usually no standard format for creeds. Some of them are essentially economic statements, but many are basically codes of ethics.

The second types of codes are found in company operational policies, which set up guides to locate what have an ethical content. For instance, specific policy statements concerning such matters as procedure for hiring, promotion and firing employees; making decisions about suppliers and distributors, or handling customer's complaints, or security matters.

Third, security practitioners and managers are members of one association or industrial group or the other. Many of these professional, industrial or trade groups have codes of

ethics which their members are expected to adhere to. Professional security practitioners are required to observe proper standards of professional conduct, whether or not the standards required are written in the rules or are unwritten. They are specifically required to refrain from misconduct, which is difficult to define precisely but which includes any act or default, which is likely to bring discredit on him, his professional body or the profession generally.

Self -Assessment Exercise

Differentiate between Ethos and Moris.

3.3 General Overview of Security Ethics

Several general points can be made which include:

- the professional security practitioner must possess diverse minds, competent abilities, proven achievements, and broad-based experience
- integrity is vital, synonyms for integrity include honesty, trustworthiness, uprightness, probity, rectitude, moral soundness, etc.
- professional security practitioners must not only be people of integrity, they must also be seen to be so
- when a professional security practitioner has ethical difficulties or unsure of what course of conduct to followed, he should consult his professional body or take legal advice. If in doubt always seek advice.

3.4 Purpose of Professional Ethics

The need to have public confide once and promote the profession, has forced professional bodies all over the world to establish the code of Ethics for the members of the profession. In any association, there must be set of rules and regulations that are binding on members of the association. Examples are Nigerian Bar Association (NBA), Nigerian Medical Association (NMA), Institute of Chartered Accountants of Nigeria (ICAN), Institute of Management Consultants (IMC), Nigeria Institute of Industrial Security (NIIS), etc.
These codes of ethics are established to do as follows:

- Guide members in the practice of the profession
- Promote the security profession
- Establish confidence on the work of security practitioners
- Establish standards of practice for all the members.
- Protect the members and the profession in the case of legal action.
- Enforce security practitioners to be competent.

3.5 Ensuring Higher Standards

- One of the major problems of ethical codes is their lack of active support by top management. Top management must make a commitment to think about and improve the ethical conduct of security practitioners and other employees in the company. Part of this commitment is an obvious preparedness to be ahead of others in equitable and just treatment of interest of persons, group.

- Example of better than precept is a popular saying that goes," since employees' behaviour is generally influenced by the actions of the boss, top management must take the lead by setting good example of high ethical conduct." There is no point for top management to ask their subordinates to eschew unethical practices, while they chew them with relic.
- The two most outstanding factors that can bring about higher ethical standards are:
  - Public disclosure and publicity.
  - Increased concern of a better informed employee and public.
- According to Koontz et al (1980) "To make ethical code effective provisions must be made from their enforcement". Unethical security practitioners and managers should be responsible for their actions. This means that privileges and benefits have to be withdrawn and sanctions have to be applied.

3.6 Standing Orders for Security Personnel

It is important to conclude our discussion of ethics with standing orders for security personnel. They are as follows:

- The security practitioners must not neglect, or without any sufficient cause omit to promptly and diligently discharge his required task while at work.
- He must not leave his place of duty without due permission or sufficient cause.
- He must not knowingly make or sign any false description. This is confidential to any employee or client past or present
- He must not without due and sufficient cause, past or present. Employee or client
- He must not without authority, divulge any matter which is confidential to any employee or client past or present.
- He must not corruptly solicit or receive any bribe or other compensations from any persons or fail to account for monies or properties received in connection with employer's company.
- He must not be uncivil to persons encountered in the case of his work or make unnecessary use of authority in connection with the information that will be discharged from the employer's company.
- He must not act in a manner reasonably likely to bring discredit upon the employer, a client or fellow employee.
- He must not feign or exaggerate any sickness or injury with a view to evading work.
- He must not wear the employer's uniform or its equipment for illegal duties.
- He must maintain proper standard of appearance and deportment while at work.
- He must not work while under the influence of alcohol or consume any alcohol while at work.

He must not have been convicted by any criminal offence.

- He must not neglect his hazard hours – from 2 to 4 a.m.
- He must endeavor to be the kind of security practitioner management wants him to be.
- He must not argue or encourage unnecessary argument in the cause of his duty
- He must maintain the uniform provided him by management, unless otherwise directed.
- He must be exposed to fire and first-aid training at agreed intervals.
- He must not unnecessarily familiarize himself with members of the work force

- He must not lose his temper at any time while on duty.
- He must promptly respond to any emergency call in the premises of his employers.
- He must be very observant of criminal activities
- He must understand basic principles of investigation
- He must possess a character that is above board and present himself as a responsible and disciplined officer at all times.

Self-Assessment Exercise

This unit has acknowledge the three broad types of professional code which are becoming a major sources of ethical norms for security practitioners and managers, "Do you agree?".

4.0 Conclusion

This unit highlighted the definitions and concept of security ethics. Sources of the security manager's ethos were identified and briefly discussed. We discussed the general overview of security ethics, basic factors, and purposes of professional ethics. Finally, few ways by which ethical behaviour can be improved were given. Also given were standing orders for security personnel.

5.0 Summary

We are aware that enforcement of ethical codes may not be an easy task, but the mere existence of such codes and the feelings of their enforcement, can increase ethical behaviour.

The employees and public must know how and why the organization's security operates decisions are made, roles of the organization in socio-economic development of the society, and probability of institutionalizing or executing a social point of view.

6.0 Self-Assessment Exercise

1. List only ten standing orders for security personnel
2. Mention six purposes of professional ethics
3. Discuss the major attributes of ethics.

7.0 References/Further Reading

Brown, L. S & Swiznick, P. (1968). *Sociological Paradigms and a Test with Adapted Readings.* Texas: Harper Collins Publishers.

Gilbert, F. & Lilian, G. (1972). *Industrial Psychology.* Cambridge: Harvard University Press.

Koontz, N. (1980). *Enforcement of Ethical Codes.* New York: Paeger Publishers.

Steiner, S. (1975). *Principles of Ethics Governing a Profession.* California: Mayfield Publishers.

Unit 2 Security Policy and Design

1.0 Introduction

It is the aspect of security operation which constantly breads contempt, resentment antagonism and conflict in any, responsibility center. In order to resolve these problems and clear away doubts between the security operatives, proprietors and employees, a clear sighted security policy becomes imperative.

However, despite the increasing waves of crime around businesses today, it is very unfortunate to observe that many organizations operating in sensitive business premises do not have a single security policy to guide the conducts of employees and the rules of security operations.

And because of this neglect, quarreling, mud-slugging, conspiracy and lawlessness will become the order of the day around such organizations, between security operative who are trying to perform their legitimate duty by blocking all avenues of committing crimes, and the disgruntled employees trying to avert such effort and commit crime. Worst of all, some members of the management not only allow such saga to happen but take delight at the unfortunate episode.

2.0 Objectives

At the end of this unit, you should be able to:

- state the role of security operatives in any protected premises
- state the role of the policeman
- explain why criminals do not like police presence.

3.0 Main Content

3.1 Definition of Security Policy

Literally, security means protection and preservation of lives and property in their totality against assaults, 'sabotage, loss, fire, frauds damage or unnecessary wastage in any given premises.

However, security duties cannot be effective and complete without the active participation of the guard force or police force in patrol duties, to access control at gates and other strategic entrance, weight bridge operations searching vehicles and employees, conducting investigations, preventing fire out - break, protection and control of process secrets, financial data, confidential information of vital interest to the company through a uniform and unbiased application of security rules and regulations in offices and the premises in general.

3.2 Policy Formulation

The formulation of security policy is the sole responsibility of management at board level. And such task should be done in an atmosphere of confidence, trust and the general interest of protecting the lives of employees, customers and visitors against all criminal assaults, as well as, the protection of company's properties against all range of crimes. This will be supported by setting parameters within which security operational powers, procedures and conducts of the operatives will look like, with emphasis on the continuous support, good-will and cooperation of all and sundry on the organization, for the success of security operations.

Mechanism of interventions by the management from time to time, to serve the prestige of the security policy or constitution and check mate lawlessness, should be created and reposed in the hand of a competent management staff, This staff must not only render explanations in the event of adverse security breach but will, from time to time, be called to account for the general security and safety of the organization. It is because of these responsibilities that management staff responsible for the formulation of policy, should know the extent and parameters within which policy should operate, to provide cover for the organization.

3.3 Policy on Security

Security is the be-all and end-all of all protection measures. Without security, there is no protection and in the absence of protection, crime lawlessness, and obstructions will prevail. Therefore, policy on security has all the paramount importance in asserting protection. There are the following laid emphases.

- How the security operations should look in general in the organisation.
- How the security department should discharge its functions.
- How security should approach all security matters i.e. searching, investigations arrest, patrol, inspections etc.
- How employees should view security roles and obey the norms guiding their behaviours in relation to daily security operations in the organisation.
- How the security hierarchy will be and the methods of reporting, as well as the accepted channels of communication and sequence of command.
- The limit and extent of powers to be conferred on security managers, supervisors, co-coordinators and the shop floor security operations.
- The colour of uniforms, equipment and other working tools to be used by the security department and operatives.
- The method and yardstick of controlling, auditing and inspecting security operations to improve efficiency.
- The appropriate techniques, methodology and response capability and options to new crime waves and threats to industry and commerce in general, and how such response will be measured in accordance with the available and limited resources.

Self-Assessment Exercise

Policy on security has all the paramount importance in asserting protection "Do you agree?"

3.4 Policy on Recruitment

Among the challenge facing commercial and industrial organizations today is staffing the security department with honest, sincere and hardworking security staff. This has become a source of concern to many organizations because of numerous breaches of security with the covert and overt participation of security staff.

However, despite such incidents, some companies are headless about formulating policy on recruitment, if not ridiculous to employ security staff and wake up one day to discover that the security staff has decisively dealt with the organization. Such incidents do occur whenever careless and disorganized recruitment exercise is carried which leaves so many loopholes, to the advantage of the security staff who may be a person of questionable character. Policy on recruitment is aimed at defeating such lumbers in its totality. The acceptable procedures on policy on recruitment are as follows.

- Define the criteria for recruitment, selection, interview and vetting of security staff before committing them to organizations services.
- Criteria for checking the suitability physique, health condition (medically fits) and moral attachments of the applicants.
- Identifying a reliable source of recruiting corrupting and experienced security force to staff the department.
- Standards and criteria for training induction and deployment of the staff according to accepted operational standards
- Criteria for education, retirees from any of the armed forces and not up to 70 years of age.

3.5 Policy on Employee Dishonesty and Crimes

Certain sections of labour acts and trade unionism have the prerogatives to reverse the dismissal of employees when the circumstances surrounding the punishment are discovered unfair.

In addition to these, grounds for dismissal are carried out and can be challenged by employees in a court of law, which is capable of scandalizing and tarnishing the image of a reputable company.

And it is also capable of destabilizing good industrial relation between the rest of employees and the organizations. Apart from all these, some employees when dismissed may resort to dangerous maneuvers i.e. ARSON Attacks, ASSASINATION PLOT etc. against the company, executive or managers in an attempt to settle an embittered score. It is in a bid to avoid all these unmitigated embarrassments that a clear-cut policy on employee dishonesty and other crimes should be formulated.

Thus will include the following statements:

- The definition of employee dishonesty and the extent to which it can warrant the award of punishments.
- Measures and manner of investigating employee dishonesty and other crimes.
- Appropriate yardstick for awarding punishment commensurate with an alleged offence.
- Compensatory measures for wrong done to wrong victims.
- Extent to which police and regular count will be involved in-awarding punishments.
- The particular department for dealing with employee dishonesty and its extent of Authority in dealing with dishonest employees.
- The powers and extent to which arrest can be instituted by whom and by which department and according to which portion of the company policy.
- The methods with which stolen properties can be recovered and returned to the company.

3.6 Policy on Retrenchment

Retrenchment in any organization is a risky and sensitive exercise which security policy initiatives must pay attention to. Apart from its potentiality to spark off protest, demonstration and violence, retrenchment exercise can produce an atmosphere where deadly conspiracy could be hatched against the company and its executives.
In view of these immense implications, policy on retrenchment should be stipulated with specific instructions to the security department, and the roles the security department will play during such exercise. The policy on retrenchment should clearly define these items.

- What role the security department should play.
- How the security of retrenchment information should be protected against leakage.
- How the management should react to any volatile and hostile situation with direct consequences to security of lives and properties, in the event of information release or leakage of the retrenchment exercise.
- The extent of contingency and emergency preparations against violence and precipitous confusion.
- Who will take charge of security operations in an extraordinary situation?
- To what extent law enforcement agencies will be involved in controlling a volatile situation.

3.7 Policy on Searching

Apart from its legal implications, searching employees in any organization has been the source of frictions, hatred and enmity between the security department and the employees. Dishonest employees will not hesitate to capitalize on this confusion and start paralysis of initiatives to commit crimes. Neglect of search operations naturally creates the temptation among employees to conceal the concealable, and get away with it.

At least, the employee will say it is company's property and it is our sweat, and a company is always a big ocean where everyone, if opportuned, can dip his cup provided he is not caught. It is this misconception of reality which instigates most employees to try to dip their cups into the company's ocean wealth.

In another realm, others may see search operations as an exercise which doubts their sincerity and therefore an insult on their person. They always resent and hate it but how sincere and honest they can be to their conscience and resist the temptations to steal is what cannot be ascertained. In order to avoid all these embarrassments and confusions, it is necessary to institute policy on searching that will be enforced across the organization.

And it will be very effective when management staffs first and foremost surrender themselves to the exercise. However, policy on searching school clearly explains as follows:

- The inclusion or insertion of search clause on the terms and conditions of service so that no employee will view and resent against searching as illegitimate exercise.
- Extending specific powers to security department on the routine need of searching's the extent to which search exercise can be conducted.
- Communicating temporary or permanent notice of search operations through appropriate authority to all employees.
- The specific actions to follow if employee refuses to submit himself to searching.
- The specific actions to follow if employees are found with incriminating property.
- At which points and exits searching can be legitimately conducted.
- The extent to which arrest can be instituted and how police may be invited.

Self-Assessment Exercise

Why is it necessary to institute policy on searching and enforce it?

3.8 Policy Implementation

Formulation of policy is one thing and the implementation of the policy according to policy recommendations and procedures is another. Some companies have the policy formulated adequately covering all aspects of securing affairs, but unfortunately the policy is either not implemented completely or is repeatedly violated and therefore becomes ineffective. This syndromic development has been contributing to the emergence of confusion in policy implementation in many organizations.

And to avoid these, policy implementation should lay the following emphasis:

- It should be clear - cut, incisive and its implementation should not easily be manipulated by someone or others for personal or selfish interest.
- It should not carry an iota of favoritism, insincerity and dubious dealings.
- It should reflect the overall interests of the organization irrespective of who does what.
- It should be enforced across the whole organization
- It should be subjected to review periodically
- It should reflect fairness, justice and aim at balancing security, safety and good industrial relations
- It should be broad - based with the participation and representation of other organs in the organization while undergoing formulation.

4.0 Conclusion

Let us examine these scenarios as a case study. In one episode in October 2002, senior employees collaborated and went away with N700, 000: 00 (Seven hundred thousand naira)

from the vault of a bank, in an attempt to implicate security operations. This happened after series of confrontations between the security operatives and the disgruntled employees who constantly refused the security operatives to search their vehicles, the bank management affably doing nothing to stop the lawlessness.

And when investigations were carried out, the so-called trusted bank staffs capitalized on the no – search opportunity to surreptitiously cart away the money in a phony sports bag. This is one of the dangers to which both the security operations and the businesses are exposed to daily in the absence of a clear-sighted and responsible security policy.

5.0 Summary

It is a pity to also observe that see many so-called professionals and corporate managers of today do not know that they have serious responsibility for security. Whenever their employees misbehave in matters with grievous security implications, they revert to inaction, divide and rule gaming believing that security is not essential to the growth and prosperity of the organization. That their employees are honest, if that assumption is anything to go by, we should not be seeing executives and managers in police cells, facing tribunals with long sentences today. Nobody is perfect and not all consciences are clear.

In any business environment, the direct involvement of every management grand, from the managing director down to junior managers in the policy formulation and control, becomes imperative if business must escape the embarrassments of crimes and crisis. Any act of negligence at the management level, will surely be reflecting in the attitudes of all employees, including the security operatives, to the extent that all security operations will be pointless rabble of confusion and pot of conflicts.

And for any business to be safe and survive, security operatives must be given free hand to operate in accordance with a clear-sighted and responsible security policy, which guides all conducts of employees including the security operations themselves.

6.0 Self-Assessment Exercise

1. Explain the meaning of security policy.
2. State the authority that is responsible for the formulation of security policy.
3. Discuss the legal implications of policy in searching.
4. Compare and contrast destabilizing good industrial relationship between the remaining Employees and the organization.

7.0 References/Further Reading

Osuala, E.C. (1982). *Introduction to Research Methodology.* Onitsha: African Publishers.

Umar, S. (1997). *Achieving Guard force Efficiency.* Lagos: Jo-Sekyson Publishers.

Unit 3 Evaluation of Protection Programmes

1.0 Introduction

Evaluation of protection programme is associated with loss and risk analysis in security operations. However, they are dangers and suffering, harm or losses through unnecessary exposures to risk-bearing.

2.0 Objectives

At the end of this unit, you should be able to:

- establish the possibility of every company being exposed to one kind of risk or another e.g. burglary, fire, fraud, robbery, etc.

3.0 Main Content

3.1 Causes of Industrial Loss

Industrial loses do not just course they are caused. The basis of security is the need to know the loss prevention and reaction in industrial security. Therefore, the loss prevention specialists have analyzed the causes which include unsafe attitude or act, unsafe conditions, and unsafe response respectively.

3.2 Unsafe Attitude or Act

Behavior or actions that expose life and property to danger or security risk due to error, negligence, carelessness etc.; for example, personal protection, equipment or right ,tools provided for a factory worker but he refuses to use those items and gets injured, ignoring casino, etc.

3.3 Unsafe Conditions

State or circumstance or place not providing good protection or not free from danger or security risk e.g. overloading or crack of walls, or any other damages in the factory, which can cause losses to the company.

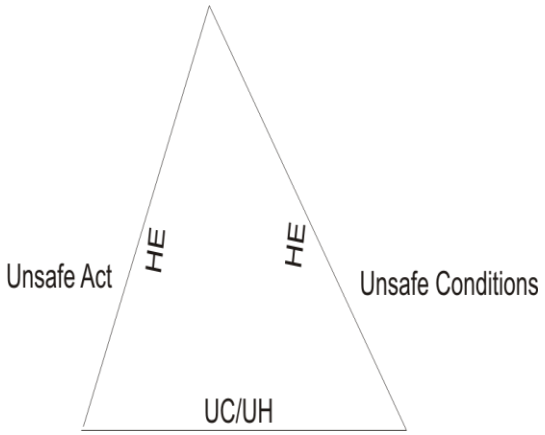
3.4 Unsafe Response

Environment induced actions, events, happenings, etc, that can result in losses to the company, e.g. adverse legislation, riot, war, natural disaster like earthquake etc.

3.5 The Triangular Theory of Industrial Loss

We can now sum that unsafe act resulting to unsafe conditions, or unsafe conditions, resulting from unsafe act, or unsafe response resulting from unsafe conditions or unsafe

conditions resulting to unsafe response which cause unwanted, sometimes unrecoverable losses.



1. HE-Human Error
2. UC-Unavoidable Circumstance
3. UH-Unforseen Happening

Fig. 1: Triangle of Loss

Self-Assessment Exercise

Industrial losses do not just course they are caused "Do you agree?"

3.6 The Industrial Security Environment

The security system does not exist in isolation. It operates within a larger environment, which has physical, economic, political, social, legal, cultural, moral and technological dimensions. The security managers have to operate within the framework established by the environment. Environmental factors can and do affect security operations. These impacts could be favourable or unfavourable.

As such, successful industrial security managers must be aware of their environments, know their possible impact on their activities, and adapt effectively to avoid unwanted or unrecoverable losses.

The diagram below shows the totality of the environment in which the security system operates. The reversible arrow connecting the security system with each of the environmental sub-system portrays the reciprocal nature of the effects which environmental factors have on the security systems and vice-versa.

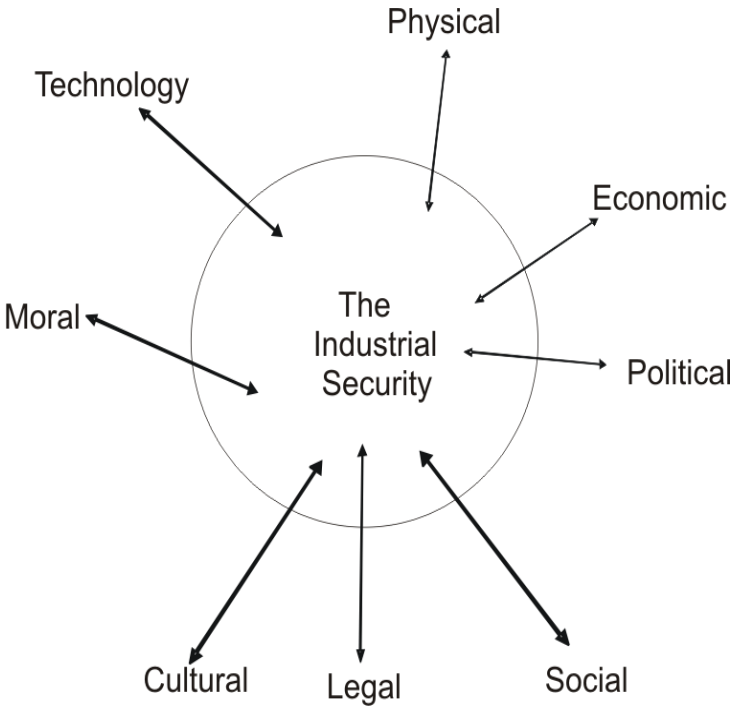


Fig. 2: Industrial Security Environment

4.0 Conclusion

This unit has carefully explained that in view of these dangers, it is very necessary for security operatives whose role is to prevent losses to business, to know what constitutes a risk and how such risk can be analyzed as well as avoided.

5.0 Summary

In this unit we have analyzed the general possibilities of causes of industrial security loss. And apart from these possibilities, buildings and machineries are daily exposed to arson and sabotage which can send a company parking.

6.0 Self-Assessment Exercise

1. Explain the causes of loss in security.
2. Describe the diagram of industrial security environment.

7.0 References/Further Reading

Alla, O. (1997). *Security and Safety. Setting up Industrial Security Business.* Lagos: Spectrum Books Ltd.

Fisher, R.J. & Green, G. (1986). *Introduction to Security Management and Planning*. New York: Paeger Publishers.

Unit 4 Administration and Documentation of Security Records and Reports

1.0 Introduction

Students in this course will apply principles of management to security administration and documentation of records and reports. Despite the anticipation and record of criminal incidents, there are many understandings to the nature of threats posed, which is part of information system and business continuity.

2.0 Objectives

At the end of this unit, you should be able to:

- state the principles and issues in security administration, records and reports of events
- describe and demonstrate the relationship between importance of security records and justified rules of keeping records, in case of eventuality as they relate to private, government and business
- apply research–oriented approaches, case studies and the use of situation analyses as appropriate in the study of security administration and documentation.
-

3.0 Main Content

3.1 Definition of Security Records and Reports

Apart from the anticipation and records of criminal incidents, there are several reasons why security operatives should keep and maintain records of events in their area of responsibility. Accurate and timely account of events provides both hind sight and fore sight to security departments and in the period of uncertainty and confusion, such records will help clear and exonerate doubtful matters.

The discussion in this lesson is to provide vital and necessary information about security record and reports.

3.2 The Importance of Security Records

Keeping and maintenance of security records and reports is as important as the entire force orations as a whole, and in their absence, security duties will not be as credible as it should be in times of serious trial. Some of the importance of security records is listed as follows.

- Records are necessary to keep full information and facts about security incidents, instructions, and performance of the guard force, cases of arrests and other vital facts during security operations.
- Security operatives on duty do not inspire respect and confidence if they could not produce accurately recorded happenings on request, especially when they resort to guessing or had not recorded the incident

- Records are necessary in handing and taking over of duty to clear away doubts during incidents of theft, where lack of records will create confusion as to who lost what and when. Remember it must be physically handing and taking over exercise and not on trust or compromization
- Recording of incidents, if accurately written will help the effort of investigations in identifying and knowing how incidents happen.
- All incidents should be recorded forth with during security operations. And it will be ridiculous, if not funny when a security operative has to start recording incident 24 hours after the incident has taken place.

3.3 Types of Records

Generally, there are four types of records in security practice. It is in these written records that all events of security significance are daily recorded and kept. These records are:-
Register: These are records used to keep a comprehensive register of items or events for the purpose of reference. Under these are numerous registers sub divided as follows:

- Visitor Register
- Key Register
- Lost and found property registers
- Alarm test register
- Borrowed tool register
- Employee search register
- Vehicle search register
- Incoming mail register
- Outgoing mail register
- Attendance registers.

Books: These are records used to record and keep a particular message, instructions, check list or reference for numerous security purposes. They are sub divided into:

- Duty occurrence book
- Security equipments service and repair log book. Telephone
- Message book
- STD code book.

Forms: These are records in security practice used to record, keep or issue out instructions, advice, direction, for various purposes.
These are the following:

- Industrial accident report form
- Fire report form
- Vehicle accident report form
- Lost and found report form
- Visitors pass form
- Way bill and gate pass forms
- First - aid treatment forms.

Cards: These are records used to keep a permanent information and record for easy reference- Cards can be sub-divided into:

- Driver's card
- Visitor card

- Identity card
- Staff access card or card reader.

Self-Assessment Exercise

Is security records a report or an information? Discuss.

3.4 Rules of Keeping Records of Events

There are certain rules to strictly follow by security operative while recording events in the security records. Some of these rules are as follows:

- In the case of arrest, full names of 'the suspect age occupation and his physical descriptions should be recorded. Other information will include the time of the arrest, reasons for the arrest and reference to properties recovered
- There must be no additional writing in between written lines. Written pages must not be removed or torn away in order to make fresh entry.
- If there is error in a recorded incident the correct procedure to follow is to draw a straight line across the erroneous entry and record the correct fact.
- Records should be meticulously kept and all abuses should be avoided.
- Records kept for the purposes of record must be fully utilised and used for such purposes, because it is not predictably possible for the security staff to know when question may arise in respect of a recorded event. The instant provision of such records on request to either the management or the court will inspire confidence, integrity and reliability of the security department and its activities.
- Records should be serially numbered in sequence and all entries by the user should be in chronological order, according to date and time. The accuracy and order of entries will justify its authenticity, in legal proceedings.
- Erasure or fresh insertion of entry will raise implicating suspicion. Tearing of pages or any other alteration of entries should not be allowed to happen; else the entire note book will be seen as a pack of forgery.
- Delayed entry of events or incident normally results in the severe criticism of the security officer in court as to why the entries were made belatedly.
- To crown it all you must ensure that entry should be made as promptly as possible provided the incident is confirmed.

4.0 Conclusion

In this unit we have learned that students will focus on security administration and documentation procedures, and maintenance of records for the safe custody and preservation of information, in case the need arises for easy reference.

5.0 Summary

At the end of this unit, we have been able to provide vital and necessary information about security records and reports.

6.0 Self-Assessment Exercise

1. Explain the meaning of security record and reports.
2. Compare and contrast the importance of security records and the rules of keeping records of events.

7.0 References/Further Reading

Charles, A.S. (1998). *Effective Ssecurity Management.* London: Butterworth Heinemann Books Ltd.

Braimoh, A. (2001). *The Basic of Security Knowledge and Planning.* U.S.A: New world Press.

Unit 5 Samples of Security Procedures for Access Control at the Gate

1.0 Introduction

In order to effectively control and monitor the movements of both visitors and internal staff, physical access control is necessary. The essence of access control in a responsibility area is to create an environment of security consciousness. This is done by establishing guard posts in virtually every strategic entry points to screen, question, watch and direct visitors and employees in the premises. Doorways, gates, lobbies, lifts, staircases, hallways, fire exit etc are vulnerable points where intruders can readily find very easy to access restricted rooms and area in offices.

However, the strategic importance of each access point is determined by security interests. While some accesses are more important, others are not because the penetration of one access point will wreck less security havoc than another. However, all access points are very important and should be taken care of.

2.0 Objectives

At the end of this unit, you should be able to:

- explain what is meant by Samples of Security procedures for Access Control at the gate
- describe the processes and types of Access Control
- state why the words QWQS is very necessary for questioning the visitors as a security officer.

3.0 Main Content

3.1 Physical Access Control

Physical access control is intended to check the following procedures:

- Illegal entry or unauthorized intrusion of persons into protected areas.
- Detect aim less wanderers in the office environment or company premises.
- Interrogate visitors and provide assistance when necessary
- Identify internal staff, for security purposes.
- Detect the deposition of subversive containers or carriages by sneak-in and deception entry criminals.
- Control crowds and visitors during peak business hours.
- Dis-arm visitors carrying offensive objects into office environment or company premises for security reasons.
- Maintain law and order by arresting trouble makers in the building.
- Keep fire exits and escape routes clean of any obstacles in case of emergency.
- Screen deliveries i.e. Parcels, letters, bags, for security purposes.
- Impose company's security policy at access points.
- Control the opening and closure of access doors.
- Ensure the privacy of employees and employers during working hours.

3.2 Types of Access Control

The nature and usage of building or premises determines the type of access control to be effectively used. However, the combinations of all types of access control will pay higher security dividend than one. In this case, there are three types of access control.

1. **Visitors Access Control**

In this type of access control, the problem of security starts with people because problems arises out of interaction, and intermingling of people of various shades and characters at different levels in the company. Visitors in this case can be classified into:

- Contractors
- Subcontractors
- Vendors
- Ex-staffs
- Non-staffs.

It is therefore very vital to control the access of this group of people by the introduction of:

- guard-post at every access-point to check their entry and exit
- visitors card access system to tag and distinguish between visitors and staffs of the company. so that aimless wanderers can be identified and restricted
- visitors-registration system to record such visits according to date, time, name, address and the purpose of such visits, so that investigation effort can be rewarded by referring to records of visitors whenever there is potential penetration or security breaches
- telephone-call system in order to establish instant communication with the persons the visitor claim to come to see especially when there is suspicion about the character seeking for access.

2. **Vehicle Access Control**

Because of the manner of how cars are used to remove valuable properties from premises or how cars are stolen, and how terrorists use vehicles to attack targets with bombs by either driving straight into the premises and leave the bomb inside the car to detonate itself. There is the need for effective car access control measures. This can best be achieved by the introduction of:

Vehicle access card/tally: After access of vehicle is allowed into a premise, card or tally should be issued to the driver, the number-of which should be written against their names and car plate number or the vehicle registration.

Vehicle register: This is to register the number plates of visiting vehicles and the names of the drivers and the time they came and left the premises, in the vehicle register or logbook

Drivers card access system: The drivers should be given visitors tags to hang in the front of their pockets to help distinguish between internal staff and visitors, and they should be directed on what to do according to security policy.

3. **Staff Access Control**

It must be realized that security can best be achieved when all kinds of activities are controlled and monitored, including the activities of staff in a responsible center. Not all staff of the company has access to any office or room in the company.

While some have the right to access one room or office others do not have. It is then necessary to distinguish through access control measure, those who have right to access a particular place and at a particular time and those who are not. For instance, while some staff have right to access computer rooms, warehouses, stores, accounts section etc. others are not allowed to access such areas.

Here, staff access control is necessary. The other aspect of staff access control is the need to identify and distinguish the difference between staff of a company and visitor. Staff can be instantly identified if their identity cards are hanged in front of their clothing. If done appropriately, staff access control is a discretionary way of controlling the access of staff, which will guarantee more security of life and property.

3.3 Quality Words for Quality Service (Procedures)

All access Points should be manned as a matter of necessity, and visitors should be thoroughly scrutinized at the guard post. Those who need assistance should be directed or referred to the reception point for further assistance.

Quarreling, insults and even fighting do occur because of poor or loss of communication between the security staff and visitors. This is because most people, who are ignorant of security operations and the protective roles of security in a particular building, believe that the security staffs are hindrances or obstacles across their path. And because of this negative feeling and belief, they approach security staff in a very aggressive and uncooperative manner.

Self-Assessment Exercise

Explain the acronym QWQS.

3.4 Quality Words for Quality Service (Questions for Visitors)

To avoid quarrel and misunderstanding, the security staff should use the following QWQS questions daily to question visitors before entry is allowed:

- "Welcome Sir, can I help you" (appear confident and look straight into visitor's eyes).
- "Who do you want to see, Sir?"
- "Is there any appointment" or "Is he expecting you"
- "Let me contact him" (If there is any doubt try to confirm)
- "OK, please hang this on" (Give him visitor's card if visit is genuine / approved and direct him to book down his presence in the visitor's book)
- "Do you know how to get to his office?" (Escort or direct him where necessary)
- "Our visitors' tag, Sir" (Remind visitors, and collect the tags when they are leaving)
- "Good-bye, thank you, Sir".

4.0 Conclusion

In this unit, you have examined in detail the term "Sample of Security Procedures for Access control at the gate. You have learnt the processes of physical Access control, and examined

what the functions at the gate applies, before using quality words for quality service (QWQS).

The unit also looked at the various administrative procedures and behavioural approach beginning from the basic knowledge of security theories, and the need to know the basis of Access protection and effective control, to the behavioural School of Business and organizational security management thoughts.

5.0 Summary

In this unit, we have acquired the experiences about the overview of principles and issues in physical security, Access Control Business and organisational security management.

We also examined the challenges embodied in the various aspects of security Access, such as visitors, staff and vehicles for easy operations.

6.0 Self-Assessment Exercise

1. What do you understand by the term "Access control procedures"?
2. What are the three major types of Access
3. Enumerate the functions of QWQS.

7.0 References/Further Reading

Momodu , B. (2001). *The Basic of Security knowledge and Planning.* Lagos: Olucity Press Ltd.

Umar, S. (1997). *Security Operations guard Force.* Lagos: Jo-Sekyson, K Publishers.