SECURITY OF INFORMATION SYSTEM AND RECORD MANAGEMENT

(A CASE STUDY OF NIGERITE LTD)

BY

KADIRI OLUWAKEMI RITA
PGD/MSC/98/99/751

A PROJECT SUBMITTED TO THE DEPARTMENT OF MATHS/COMPUTER SCIENCE, FEDERAL UNIVERSITY OF TECHNOLOGY MINNA.
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A POST GRADUATE DIPLOMA (PGD) IN COMPUTER SCIENCE OF THE FEDERAL UNIVERSITY OF TECHNOLOGY MINNA.

SEPTEMBER, 2000

CERTIFICATION

This is to certify that this project "SECURITY OF INFORMATION AND RECORD MANGEMENT" has been presented by Kadiri Oluwakemi Rita. PGD/MSC/99/751 of the Department of Maths Computer, School of Science and Science Education, Federal University of Technology Minna Niger State.

Approved by:

______________________ ______________________

Prof. K.R Adeboye. Date.

Project supervisor

______________________ ______________________

Dr. S.A Reju. Date.

Head of Department.

______________________ ______________________

External Examiner Date

DEDICATION

To Jehovah, my heavenly Father who made the words of Psalms 37:25.

("A young man I used to be, I have also grown old, and I have not seen the righteous forsaken, nor His offspring looking for bread") true for me.

ACKNOWLEDGEMENT

My profound thanks goes to my project supervisor Professor K.R Adeboye for his diligence in seeing to the timely completion of this project.

My invaluable thanks goes to my parents for their care, perseverance and encouragement, who have expended time and money in helping me see to it that this project work is completed.

My profound gratitude goes to my dear, Fred Balogun for his love, support, advice and encouragement all through the course of this program.

I would not forget to mention my lecturers who had been very helpful to me Dr. S.A Reju, Mallam Audu Isah, Mr Hakimi Danladi, Prince R.O Badmus, Dr. Y.M Ayesimi, Mrs. O. Agbachi and Mr. L.N Ezeakor.

My wonderful friends also are Ogechi Ugwu, Eti Mbuk Ekperikpe, Kemi Ologunagba, Asa Joseph, Mark Adamu and a host of others.

My greatest thanks however goes, to JEHOVAH. My Father in heaven, who has made me what I am today. In Him I live, in Him I move, in Him I have my being. I thank Him for the love he has shown me through his Son, our Lord and Saviour Jesus Christ.

ABSTRACT

This project work looks at the issue of data security in record management. It is aimed at protecting the records in an organization against intruders, where there is need for security of some vital information on the computer system.

After discussing the various ways that data files can be secured through the use of data access controls, encryption and password, we go on to show how these suggestions can be implemented by developing a program that uses them in protecting the personal records of employees in the organisation, Nigerite Limited.

TABLE OF CONTENTS

TITLE PAGE

CHAPTER ONE

HISTORICAL BACKGROUND AND IMPORTANCE OF THE STUDY

CHAPTER TWO

THE PROCESSING OF INFORMATION AND RECORD MANAGEMENT

CHAPTER THREE

DATA GENERATION AND ANALYSIS OF SECURITY SYSTEMS.

CHAPTER FOUR

PROGRAM DEVELOPMENT AND IMPLEMENTATION.

CHAPTER FIVE.

SYSTEM RECOMMENDATION AND USERS MANUAL.

CHAPTER ONE

HISTORICAL BACKGROUND AND IMPORTANCE OF THE STUDY

1.1 INTRODUCTION TO INFORMATION SYSTEM

The record of information is the life wire of every organisation, regardless of the type of the organisation; and also the size of that organisation.

The importance of information otherwise known as record management cannot be over emphasized. The purpose of information is mainly concerned with the processing of data about the operation of an organisation in order provide accurate, current information to the management and whosoever might need it for use.

The historical background of information management or the processing of information started right from when man came into existence. However, raw data are of limited importance; they become useful only when they are examined, analyzed, summarized and classified. Then they become useful information for management to use. Over two hundred million papers are sometimes found in files, nearly one million file drawers are generated annually by some nations or organizations.

The other problems are:

a) Papers occupied too much space, which can be used for other purposes.

b) Cost of the papers that are in use is much.

c) Storage method of such papers is faulty.

d) Retrieval of such information sometimes become difficult.

e) Security of such information is doubtful.

f) The accuracy of such information is not certain.

Going by the advantages attached to computerizing the existing methods, the researcher decided to focus on the personnel department of Nigerite Limited, situated in Lagos. The area of focus on the security of employee's personal records in the organisation. Also, measures to ensure privacy and security of information made available for management use in relation to the;

1) Size of information

2) Security

3) Accuracy

4) Correctness

5) Access to information

1.2 NEED FOR COMPUTERISATION AND SECURITY OF RECORD MANAGEMENT

The researcher carried out feasibility studies of the existing methods to see how feasible it is going to be and a description of the existing method was also given and the disadvantages are spelt out.

The identified solution is not only to computerise the existing methods but also to regulate its activities by designing a system of checks and control principles in order to: -

(a) Safe guard

(b) Follow stated policies instituted by management

(c) Maintain reliable records.

(d) Carry on business activities in an efficient manner.

These will in turn.

(1) Reduce cost

(2) Provide security of information

(3) Retrieval of information will be made easy

(4) Processing power of information will be faster

(5) Large volume of information can easily be stored

Bearing in mind all these, there are certain characteristics that are expected with any good computerised information system.

They are:

a. Recording of information

b. Classification of information

c. Sorting of information

d. Calculation of information

e. Summarizing of information

f. Reporting of information

Programs were designed and written, which will be aimed at taking care of:

- Adding more information
- Deleting a records
- Sorting of records
- Updating of records
- Viewing of records

1.3 OBJECTIVES OF THE STUDY

The objective is to computerize employees personal records of the personnel department, and the organization as a whole. The area of focus is on the personnel department of the Nigerite Limited.

This project is aimed at discovering new techniques for ensuring the security and privacy of information (data) of employees and records of great importance on the computer system. Computerized manner of protecting accident or intentional harm, distraction of computer hardware, physical loss of data and the deliberate invasion of databases by unauthorized individuals.

1.31. PROCEDURES FOR ACHIEVING THE OBJECTIVES

(A) The study of the existing situation method

(B) A feasible study

(C) Programs were designed, written, tested and run successfully.

1.4 SCOPE AND LIMITATION OF STUDY

The scope of this study is limited to the personnell, Department of Nigerite limited to the personal records of employees in the department.

The researcher would have included other departments, but due to time constraint the focus will remain on the personnel department.

1.5 DEFINITION OF TERMS

COMPUTER SECURITY

Techniques developed to protect single computers and network linked computers systems from accidental or intentional damage, including destruction of computer hardware and deception of computer users.

SERVERS

These are special computers, which provide connections between networked computers and outside system such as database storage and printing facilities.

ENCRYPTION

One technique used to protect confidentiality is encryption. Information can be scrambled and unscrambled using mathematical equations and a secret code called a key. Two keys are usually employed, one to encode the data, called the private key, (this is possessed by the sender). The other is to decode information called the public key, this is possessed by several receivers.

APPROVED USERS.

This is another technique to prevent computer crime. It is used to limit access to computer data files to approved users. Access control software verifies computer users and limits their privileges to view and alter files.

PASSWORD

Passwords are confidential sequences of character that gives approved users access to computer. To be effective, password contains a mixture of characters and symbols that are not real words.

TOKENS

Tokens are tamper-resistant plastic cards with micro-processor chips that contain a stored password that automatically and frequently changes when a computer is accessed using a token. The computer reads the token password as well as another password entered by the user, and matches to a identical token password generated by the computer and the user password which is stored on a confidential list.

FIRE WALLS

Computer networks, multiple computers linked together, are particularly vulnerable to computer crimes. Information on network can be protected by a firewall. A computer placed between the networked computers and the network. The firewall prevents unauthorised users from gaining access to the computers on a network.

CHAPTER TWO

THE PROCESSING OF INFORMATION AND RECORD MANAGEMENT

2.1 HISTORICAL BACKGROUND OF THE ORGANIZATION

Nigerite limited was established in 1959 and it started operation in 1961. Diversification was done in 1987. It started as Bestors Cement Products then diversified into the production of the floor flex tiles.

The products profile of the Company includes roofing sheets of different types, ceiling sheets and vinyl floor tiles.

The Company is located on a fifty acre site a long Oba Akran Avenue Ikeja in Lagos State.

It is a joint venture between Odua Investment Corporation Limited and Etex Group of Belgium.main Products include;

(a) Ceiling sheets.

(b) Roofing sheets.

(c) Garden items.

DISTRIBUTION.

The main factory is in Lagos. There are depots in Ibadan and Ilorin. The main marketing outlet is through distributors who are all over the federation.

The staff strength of the organisation presently is about 800 employees.

Categories of staff include the.

(i) Junior staff

(ii) Senior staff

The affair of the senior and junior staff is handled by the personnel department of the organisation.

(iii) Managers

(iv) Directors

(v) Expatriates

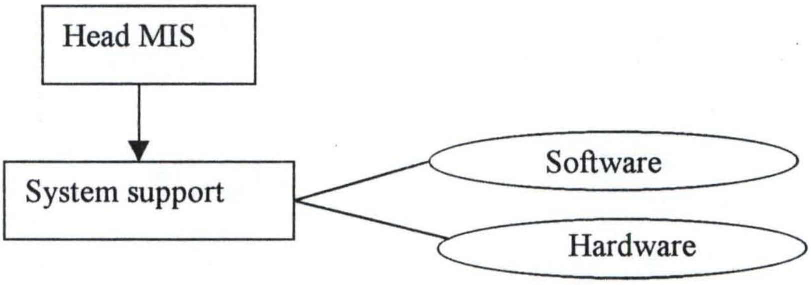
The corporate affairs department of the organisation handles the affair of these categories of staff.

2.2 FEASIBILITY STUDY OF THE PRESENT SYSTEM.

The present system of operation is computerised. The local area network system (LAN) is being used here. Formerly the system was centralised where by every job coming from all departments need to come to MIS (Management Information System) for data processing.

The file server network here is a process where one system unit called, file server is linked with other PCs. The central PC is where information is stored thereby enabling everyone to have access to it. Here different departments use different information on the same server. Security comes in by file sharing.

For now the system of operation is decentralized whereby each department processes its data. The MIS then coordinates the activities of the organisation as a whole. Under the decentralized system we have



For confidentiality of each file, there is a password that protects the opening of the documents. Our focus however, is on the security of the information system and record management in relation to employee's personal record. It was found that employees personal records are mainly kept in files, recorded and stored both manually and with the PC.

The personnel department handles only the personal records of the junior and senior staff of the organization. While the corporate affairs department handles the personal records of the managers and the directors of the organisation.

The computer in the personnel department is mainly used to store data information that has to do with job description, payroll records, because payment of salary of the junior and senior staff is made through the personnel department and also internal audit. Only information that is considered to be of importance on employees is stored in the computer.

Another method of searing information_in this organisation is the backup storage in form of data bank. This is a fireproof cabinet to ensure security.

2.3 PROBLEMS ASSOCIATED WITH THE PRESENT SYSTEM

Though the organization's system of operation is computerised, there is need for improvement of its security measures. Regulation of activities at all levels should be done by designing a system of checks and control principles in order to maintain reliable record on employees and data as a whole.

The hardest kind of computer to protect is the one with multiple users, some who are connected to the main frame from remote stations. The typical multi-user is vulnerable to many points.

Through discovery two major categories of dangers face this system.

(1) **Environmental hazards:-** This has to do with electricity. There is problem of stable electric power supply to the system. For any system operation to run smoothly and effectively, there is need for regular power supply. Maintain a temperate climate for the system. Even the Air-Conditioner,

when it's too much can even filter the surfaces of tapes making an entire disk unreadable.

(2) **Human Hazards:** - (Danger caused by people).

It was also discovered that security of information can be tampered with by intruders. They do not have the necessary security devices to prevent illegal access.

The intruder who seeks to alter stored data will hope to do this without discovery by the legitimate owner or user. Alteration of stored data may take place either through misuse of normal access to channel or by re-writing data on exchangeable storage media. Where an intruder has illegal access to data recording media, deletion of data cannot be prevented clearly. This is very serious matter and demands the creation of a secured physical environment for storage of tapes, disks, together with backup copies at a different location.

A major way of ensuring data security in this organisation is the password method of choice used for verifying the identity of individuals logging onto computer network linked by telephones. The effectiveness of password hinges on the challenging task of keeping them secret, obstacle of secrecy are abound. Passwords are said to effective only if they are secret; and users are notoriously indiscreet as we see in our organizations today.

2.4 SECURITY OF RECORDS ON COMPUTER FILES AGAINST ILLEGAL ACCESS

Security of information under the computer department is in the form file sharing among the various departments in the organisation.

A measure against illegal access also used is the password. A password (code) is attached to each user level for each department. Each department is grouped as a user. There is file attached to each departmental job. Here it is the boss who gives a go-ahead to supply information that is of relevance to each department. Also there is the data bank, for backup storage facilities.

A simple method also used for information or file security is the Access Control List (ACL). This method is used to regulate the security of electronic files. An ACL names those authorized to use a file and specifies what kind of access each person is permitted.

Though this method hasn't been adopted by the organisation, the researcher believes that it will be of great help for file security.

Read-access allows the individual to use a program or look at the contents of the file, but doesn't grant the right to alter the program or file in any way; To make additions, deletions or other changes, a user must also have write access, request for a file. It must first bring the relevant ACL into temporary memory, to check for user name, only if the name is found will the file be brought into memory.

2.5 DESIGN OF DATA SECURITY AND INFORMATION PRINCIPLES

USER ACCEPTABILITY

The security system must be acceptable to the users. The human Interface must be simple, natural and easy to use or user will by pass it, thus rendering the system ineffective.

COMPLETE MODERATION

All access to every object must be checked for authority. This principle requires that if a change in authority occurs, future access cannot use remembered result of authority checks, but must be reduced.

NON SECRET DESIGN.

Exposing the facilities of a design to a number of bright people during planning stages which will facilitate corrections before other systems are implemented. And before other systems come to rely on it's faulty design. One could attempt to keep secret the security provision, but in the long run, bugs will be found. It is better to have discoveries early by invited commentators than later by intruders.

ECONOMY OF MACHANISM

Keep the design as small as possible and it must be flexible. It must be adaptive to changes when and where necessary.

SEPARATION OF PRIVILEDGE.

Requiring two keys to unlock any protection mechanism is more flexible and robust than allowing access to the presenter of only a single key. Which can be physically separated. Also distinct programs, organization or individuals can be made responsible for them.

LEASE COMMON MECHANISM.

Every shared mechanism represents a potential information path between user; therefore these should be minimized.

LEAST PRIVILEDGES.

Every user, program, terminal and other human resources should use only the priviledges necessary to complete the job.

Adhering to these security principles will reduce both the number and seriousness of flaws that appear in computer systems.

CHAPTER THREE

DATA GENERATION AND ANALYSIS OF SECURITY SYSTEM.

3.1 DATA GENERATION

Generation of data used for this research work was done through two must effective methods of data collection. They are, through the personal discussion or interview and observation.

However, it was discovered that the personal data of employees in the personal department were not well protected against illegal access, due to the nature of system used to keep records (manual filing system). It is only information considered to be of uttermost importance that is sent in to the PC for record purposes. It is also found that even the personal computer in the department and the MIS as a whole do not have good and tight security measures to prevent intruders from having illegal claim to any kind of data whatsoever. Inadequate number or kinds of physical protectors both within and outside the computer mainframe.

In this chapter we shall present a complete program we have designed and written to.

(i) Add new records.

(ii) Update new sorting of records.

(iii) Indexing or sorting of records.

(iv) Viewing of records.

(v) Deletion of records

(i) ADD NEW RECORD

Program allows a person to add new data to the already derived one.

(ii) UPDATE NEW RECORD.

Allows one to make changes on particular record where need be.

(iii) SORTING OF RECORDS (INDEXING)

Allows one to make changes on a particular key the organisation might decide to arrange to it's record, based on the department each employee represents.

(iv) VIEWING OF RECORDS.

Just to show the personal data of each employee when needed.

(v) DELETION OF RECORDS.

This will help the department to delete data or Name that are no longer of relevance to the organisation e.g. Names and data of employees who have left the organisation.

The program is designed not only for record management but written to provide effective security measures needed to counteract the likely attack of data or invasion of the information stored. The effect or alteration or wrong deletion of data can make the organisation loose so much. As we know it is a high price to pay. So security measures need not to be overlooked.

3.2 ANALYSIS OF SECURITY SYSTEMS

Here we analyse the measures used to implement the data security system used for the program.

(A) PASSWORDS

Turning away an attack with a word. This is a matter of choice for verifying the identity of an individual logging onto computer networks. Passwords have been recognized to be the most widely used data access control technique today.

A good password must satisfy the following conditions:

(a) It should not be guessable.

(b) It should be easily remembered

(c) It should not be in dictionary

(d) It should not be changed regularly

(e) It should be protected.

We can divide password into several categories.

(i) Grouped password: which are common to all users on a system

(ii) Passwords which are unique to individual users.

(iii) Passwords, which are not unique to individual users but serve to confirm, claimed identity.

(iv) Passwords which change any time a system is accessed

Each of these passwords have been used in our context for the purpose of the security system. The best type however is the (ii) type. By allowing each user to have a unique password, which cannot be known by another user except he/she wishes. Also password is unique to each user potentially because it provides a much higher level of security.

(B) DATA ENCRYPTION

In most cases, transmission of information from one computer to another travels via the telephone system. In the short time required for the data to travel from the sender to the receiver the system affords eavesdroppers opportunities to intercept the information and sometimes alter it.

Encryption renders their effort fruitless by re-arranging the data into codes that makes no sense to anyone who does not posses the secrete key needed to decipher it. (decode).

Encryption is the scrambling of data or messages with a cipher or code so that they are unreadable without a secret key.

Encryption procedure or methods can be classified according to:

(1) THE NATURE OF ALGORITHM.

(a) Transposition or permutation e.g. Nilhist cipher.

(b) Substitution, either mono-alphabetic or poly-alphabetic e.g. Caeser and Vigenere ciphers.

(c) Product, combining, permutation and substitution ciphers e.g. the US data encryption standard (DES)

(2) THE NATURE OF THE KEY

(a) Private key: - This includes the transposition and substitution ciphers. It uses the same key for encryption and decryption.

(b) Public key: - A dual system. It uses one key to encrypt and another key to decrypt. The encryption key can be made public. Data encryption can be embedded or inscribed on the article or material.

1a. Transposition: - They are techniques aimed at hiding the content of a file by taking the individual character or bits and rearranging their orders. The simplest possible transposition takes successive letter group and rearranges each in a regular fashion.

For example the letters can be taken in groups (block) of five and arranged in order.

41532

The sequence of 41532 constitute the encipherment key e.g. we want to encrypt the plain text.

MATHEMETICS b DEPARTMENT

Using the key "41532" where 'b' represent blank

plain text: MATHE/MATIC/S b DEP/ARTME/NT bbb
12345/12345/12345/12345/12345

KEY:

4	1	5	3	2
H	M	E	T	A
I	M	L	T	A
E	S	P	D	b
M	A	E	T	R
B	N	b	b	T

Cipher text: HMETAIMLTTAESPDbMAETRBNbbT

This form of transposition is called the NILHIIST CIPHER.

1b. **Substitution:** - These techniques retain the relative position of the characters in the original plain text. But hide their identity in the cipher text. A simple example of the substitution is the ceaser cipher which substitute the nth letter away from the plain text character in the alphabet. This applied modulo 27 (the 26th letter in the English alphabet and blank). n is the key indicating the alphabet shift.

A general mono-alphabetic substitution cipher replaces characters in the plain text with characters from some other alphabet, called a cipher alphabet which becomes a key e.g. the following transformation.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G R D N F S F A E O T M B H P C Y J X V Z K I Q U L

Transforms the plain text: DATA

Into Cipher text: : NGVG

1c. Polyalphabetic Substitution:- Uses multiple alphabets cyclically from a different cipher text alphabet thereby obsuring the frequency characteristics of the character in the plain text alphabet.

SECURITY OF ENCRYPTED FILE.

The security of the encrypted data depends on a variety of factors among which are:

(1) The Secrecy of the key

(2) The difficulty of guessing the key or trying out all the possible keys. (key search).

(3) The Difficulty of inverting the algorithm with knowing the encryption key (breaking the algorithm).

3.22. ACCESS PRIVILEDGE AND AUDIT TRAIL

This means assigning access privileges to users based on the action they are authorized to perform on the database. When an authorized user logs into the system, his access privilege is checked in the user profile and he is not allowed to take an action he has no authority to perform. Four levels of access priviledges are used in the program.

(i) Granting Priviledges (00)

This priviledge is given to the database administrator to assign priviledges to other users (and to revoke). A user with a granting priviledge is also allowed to add new records, edit existing records, delete records and to display records. This access priviledge is given the record "00"

(ii) Append Priviledge (01).

This is the priviledge given to the data entry clerk_to add new records into the database. They are not allowed alter or read previously stored data. It is given the code "01".

(iii) Update Priviledge (11)

This is the authorization given to certain user to update (edit and delete) the database, they can also be read and add new records to the database. But unlike the database administrator, they cannot grant access priviledge to other users. It has the code (11).

(iv) Read only Priviledge "10"

This is the priviledge granted certain users to only read (i.e. display) records in the database e.g. for statistical purposes or issuing of results. It is given the code "10"

Login File

Logging is one of the most important an defective method of increasing security in computer system. Without an accurate 'log' it is impossible to look at what has happened in the past, to plug leaks where they occurred. The log produced can be examined periodically or in the real time by the computer installation manager to determine if violation of access rules are been attempted.

The log file will open at any point, a user is denied access to the system. Display of welcome greeting for the user, the identification and authentication of the user follows. If access is denied a complete log of all the request made by a user along with the time submitted, date, users name and the type of transaction made by the user will be stored in the log file. The figure below shows layout of the purposed file.

Date used	Time in	Time out	User	Transaction
15/5/2000	10.14	12.06	Amen A.O	Update of payroll of dbf.
16/5/2000	11.30	14.04	Okon E.O	Denied access to delete command.
17/5/2000	15.12	17.09	Ajose J.A	Creation of file payroll dbf.

3.3 USER IDENTIFICATION AND AUTHENTIFICATION

Identifying and authenticating users identity is a form of data access control.

Identification is a unique name or number assigned to an object. In this system there are three identification which are:- users name, password and terminal code. Identification is necessary for accounting or to keep record of the user on objects being used and authorization purposes. But it cannot be used without additional authentication. If some degree of security is designed in a system. Identification is given to each user in form of password. A group of users with different passwords are allocated to a given terminal by a known terminal code (i.e. workstation).

Now to deal with authentication:- This verifies that a person is who he/she claims to be. There are several types of information which may be required before identification could be accepted as valid.

Passwords,_question and answer methods are used by the computer to authenticate users. If the user is unable to provide the right piece of information, the computer accepts the user since authentication method in this system is only invoked once, space and time requirements have title importance relative to other considerations

From the users point of view, the typing, the thinking and the way of handling typing errors all are more important. After users name, password and terminal code are being checked by the system. The user will be linked to the question and answer method.

LOGIN

Login: Oyelola S.U

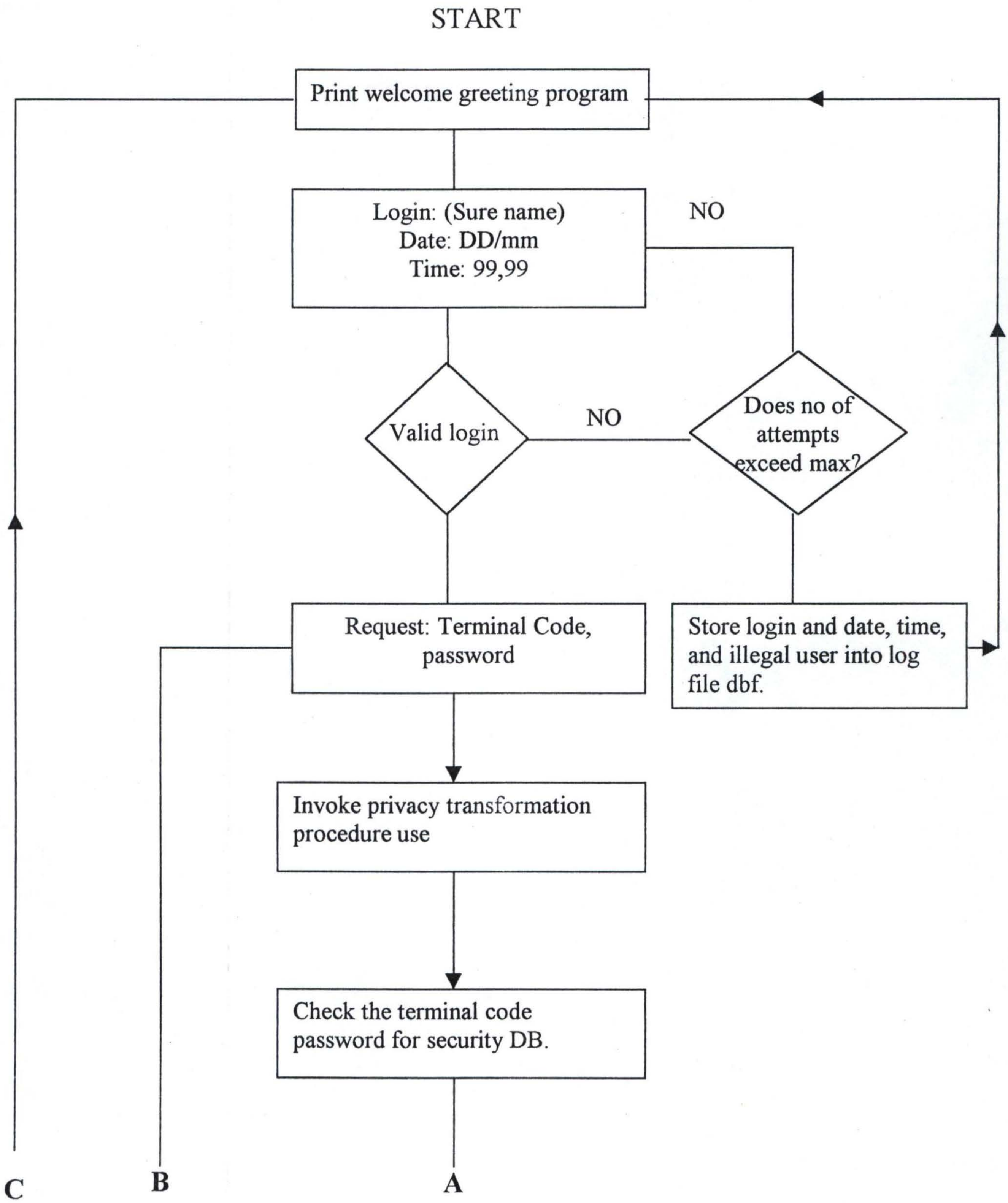
How long have you been in this organization?

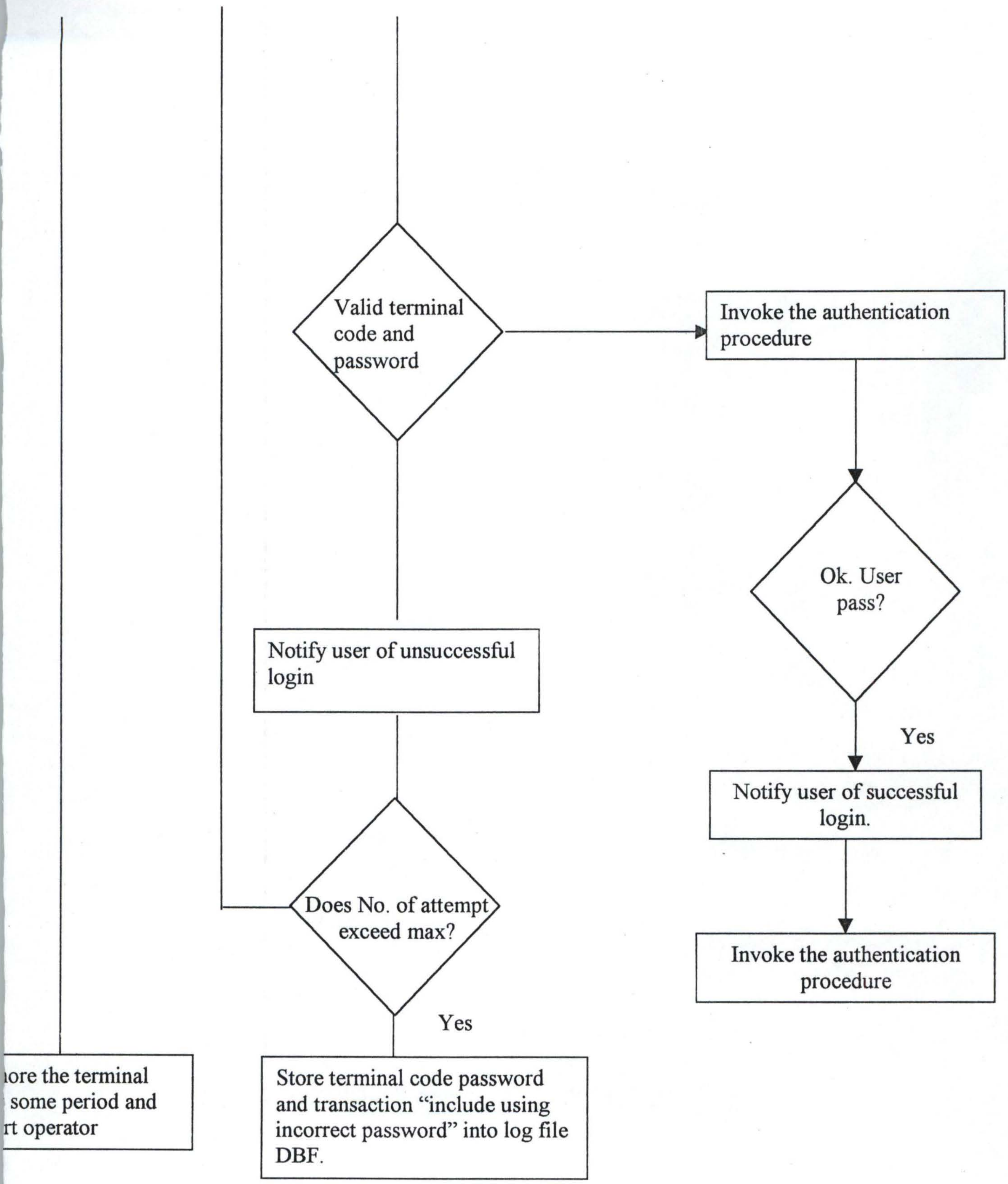
How old are you?

Authentication granted ....

Press any key to link you to the authorized menu.

FLOW CHART FOR IDENTIFICATION AND AUTHENTICATION


START
Print welcome greeting program
Login: (Sure name)
Date: DD/mm
Time: 99,99
NO
Valid login
NO
Does no of attempts exceed max?
Request: Terminal Code, password
Store login and date, time, and illegal user into log file dbf.
Invoke privacy transformation procedure use
Check the terminal code password for security DB.
C
B
A


Valid terminal code and password
Invoke the authentication procedure
Ok. User pass?
Yes
Notify user of successful login.
Invoke the authentication procedure
Notify user of unsuccessful login
Does No. of attempt exceed max?
Yes
ıore the terminal
some period and
ırt operator
Store terminal code password and transaction “include using incorrect password” into log file DBF.

3.4 AUTHORIZATION OF CONTROL SYSTEM.

Once authentication is carried out and granted, the authorization of a given user or other result would be checked against incoming request. So if desired operation is permitted, it means that the requestor is authorized to a given database file.

The data item may be a file, a record or field of a record, whether or not access is granted on.

(1) The access priviledge of the user.

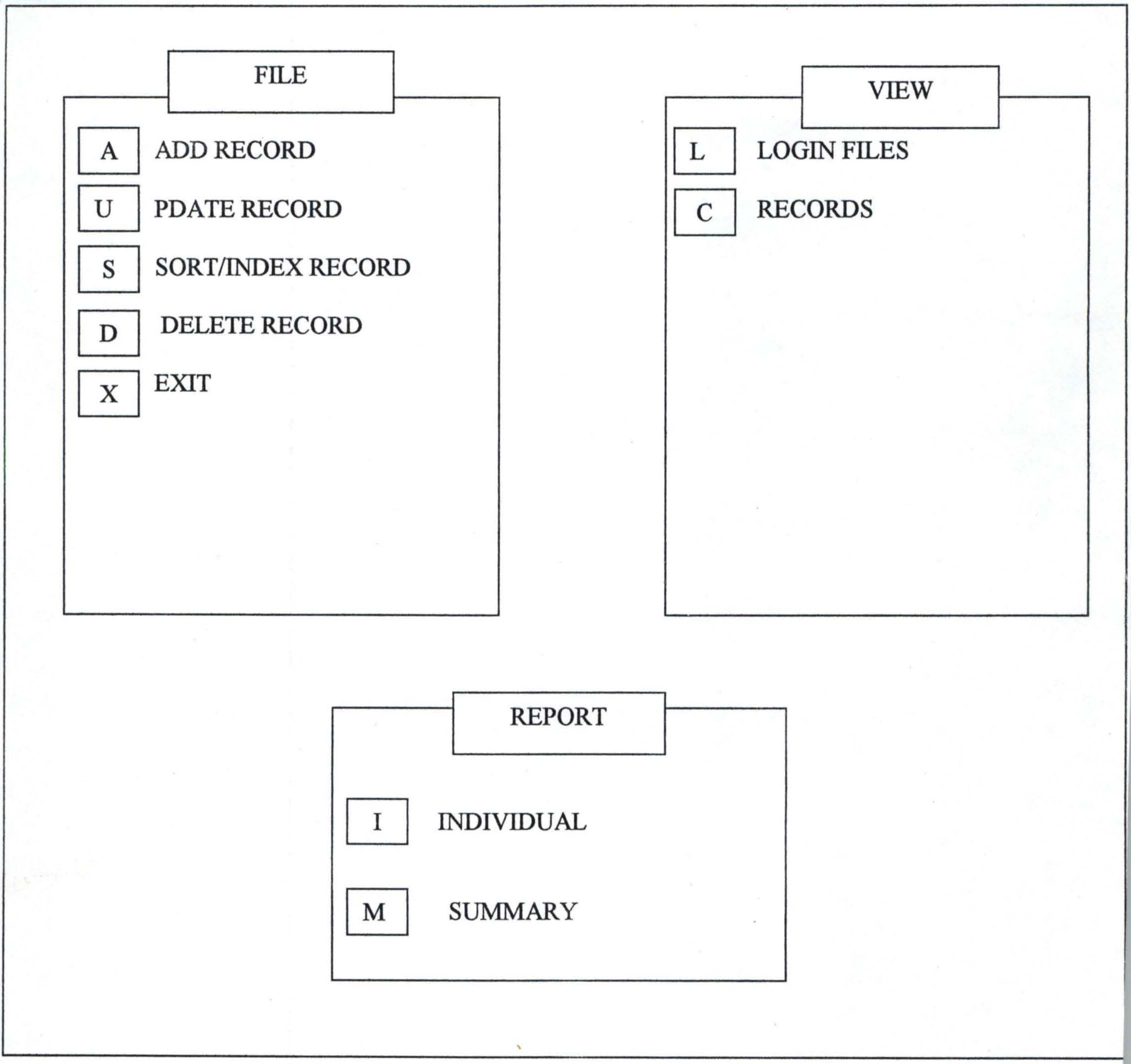
(2) The operation request.

(3) The value of datum.

The program makes use of the user password which will be checked for in the title called priority database file. This contains the user file status and his/her password.

Diagram shows the purposed menu for authorization section of the system. If access is not granted to a particular user, he/she would not be allowed to perform the pre-selected operation.

AUTHORIZATION OF CONTROL SYSTEM



3.5 PHYSICAL SECURITY DIMENSION

Physical security dictates that a system must posses the ability to distinguish among authorized persons, unauthorized visitors and other unauthorized persons. This discrimination should be exercised by automatic access control system or by guards. The following are physical security precautions which must be taken in any computer installation: -

(i) Security starts by limiting access to the computer room only to those who have a specific need to be there. To ensure this, admission badges should be worn conspicuously by those who are entitled to be there for any business.

(ii) Where computer room personnel for some reasons stop having business with the computer room, entrance card should be collected from them and destroyed so that access is denied them.

(iii) In cases of known security violation from any other threat from any source, changes in access rule and requirement should be affected immediately.

(iv) Where an employee is disengaged by violation, the rule of instant termination should be invoked to ensure that the employee leaves the premises immediately without returning to the place of work. Cases have been reported in the past of employees who have damaged their terminals or corrupted software learning programs on learning of their termination

(v) Security is a matter of attitude. Employees of the computer room should be encouraged to challenge all strangers who come around the operating environment of the computer.

(vi) Tours of the computer room, whether guided should be discouraged. The fewer the people that enter the room, the lesser the risk of security breach.]

(vii) There should be a careful and deliberate location of the computer room in part of the premises which is somehow obscure to all but to those with the need to know. The fewer the people that are aware of where the computer room is located the better for everyone concerned with security.

CHAPTER FOUR

PROGRAM DEVELOPMENT AND IMPLEMENTATION

4.1 PROGRAM LANGUAGES

Program language are referred to as languages which one can use to communicate with a computer with the aim of solving a particular problem or to perform a specific task.

There are different types of programming languages. We have the machine language, the low-level language and the high level languages.

The machine language is directly understood and decoded by the computer. It is a language that is clearly understood by the computer without the use of a translator. The machine language is written in 'Is and Os'. Most machines work with binary digits, hexadecimal etc. For instance 4 in binary form will be 100.

The low level language are closer to machine language. They are normally written in form of mnemonics i.e.. Java scripts.

The high level languages are written in English, while the computer translates or compiles the codes into machine language before execution and vice-versa to output the results.

These are achieved through translators (i.e. basic) and the compilers (i.e. Pascal, FoxPro etc.)

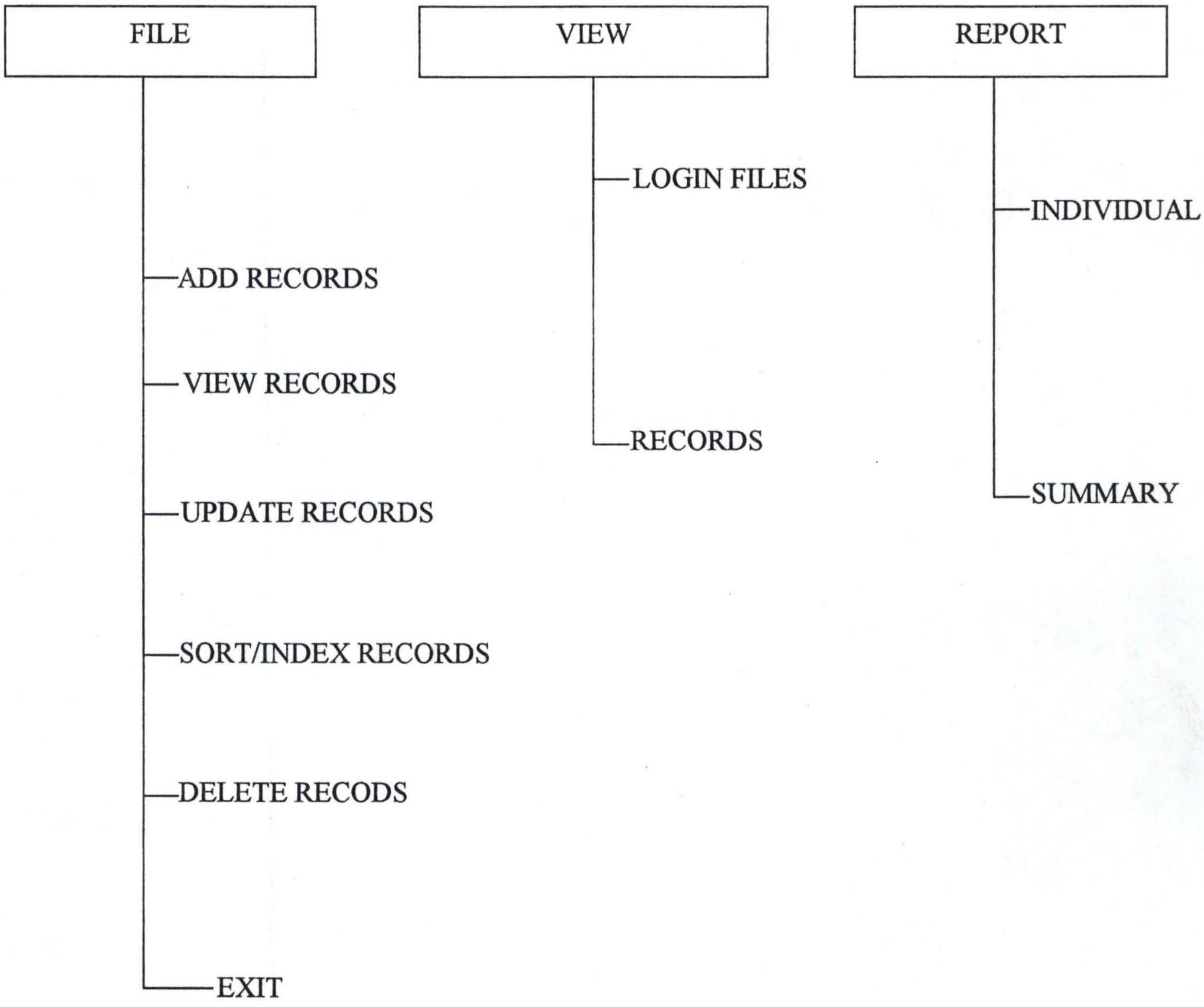
4.2 CHOICE OF PROGRAM LANGUAGE

The choice of program language depends on what exactly the programmer wants to do. Each language has the best area it's most suitable for. High level languages are suitable for specific purposes depending on what the programmer intends to achieve and how he intends to solve a given problem. For instance, for scientific purposes or calculations, one can use C++, Q Basic, Pascal, Fortran etc.

The program used for the purpose of this project is FoxPro for windows. This windows base has facilities support system for data and record management. It also provides room for the security of the database structural programs.

4.3 MAIN MENU

The main menu for this system is described below.



To see the sub menus under file, the user can click file or ALT + F keys.

To see the sub menus under report, one can click report or press ALT + R keys.

Each of the sub menus can be accessed by clicking on each of them or press ALT + underlined letter.

4.31 PROGRAM TO SORT DATA

This aspect of the program sorts or indexes the record serially according to the employees number. The employees number is a unique key for each of the employees and is given to them sequentially during their employment.

As soon as the user click on sort/index records, the computer prompts the user to hold on while it sorts the records. And when this is done the user is also prompted to return to the main menu.

4.32 PROGRAM TO ADD DATA.

In order to add additional information to the data file, this sub-program makes provision for that. However, only an authorized user can add records to the database file. This is protected by the transposition code of encryption which is '1234'. Any unauthorized will be denied access.

4.33 PROGRAM TO VIEW RECORDS

This part of the program allows the user to look at each record without changes or unnecessary diversion to other entries. Before the user can see the records, the key field has to known which is the employee number.

The user can click on record under the main menu view before having access to this program. The user could decide to view many records before returning back to the main menu.

4.34 PROGRAM TO DELETE RECORD

Deleting records is a very sensitive matter. Records can be deleted if such employee is no more in the organisation, so as not to pay him or her.

However, not all users can delete records. This part of the program is encrypted so as not to give access to every user. It can only be accessed by the manager or boss who has the encryption code. The essence of this is to guide against invasion of stored information and alteration or wrong deletion of data. This sub-program has been encrypted so that only the authorized user can delete staff records. The substitution code under the encryption key is 'TFBE'.

4.35 PROGRAM TO UP DATE RECORD

To update a record refers to making changes in the previous entries, This is in case of mistakes, promotion or dismissal. To get access to this part of the program, the user need to click on update records under the main menu file.

The unique key, which is the employee number is use to access each of the employee record. Before making changes the previous record is displayed for the user. This sub-program is encrypted so that only the authorized user can make changes to staff records. The encryption code is '1234' any unauthorized user will be denied access to this sub-program.

4.4 SYSTEM SPECIFICATION

System specification provides a detailed documentation of the entire system. The content of system specification includes: -

(a) Preliminary information contents, names of those who can change in files, program etc.

(b) Objectives of the system depth involved

(c) System description-detailed procedures both clerical and consulting using flow charts when necessary.

(d) Detailed specification of input files, source document and output document.

(e) Time scale for getting the system working.

(f) Plans to enable smooth changeover from the old to the new system

The system specification has to do with the requirement (i.e. minimum requirement) in which the system can be used. There are the software and hardware specification which are discussed below.

4.41 SOFTWARE SPECIFICATION

For the system to be able to run smoothly it requires a minimum of windows 95. This is as a result of the program written with FoxPro windows. Windows 95 is the minimum operating system that is required.

4.42 HARD WARE SPECIFICATION

The hardware specification is given below:

* Pentium 133 MHz

* Hard Disk 2.0 GB

* 14" Monitor

* Mini-tower case or Desktop case

* Keyboard, mouse and mouse pad windows compatible

* CD ROM 48x

* 3½ floppy disk drive

* UPS backup 650w.

CHAPTER FIVE

5.0 SYSTEM RECOMMENDATION AND USERS MANUAL

5.1 DOCUMENTATION

This refers to proper keeping of program codes for maintenance. This can be achieved by making comments in the program to explain steps, procedures and functions.

Whenever the needs arises for modification in the program, perhaps based on the operations of the organization, it will be easier for any programmer to go through the original codes to make or effect those changes. It also guides against remembrance of steps, procedures and function names used in the program.

5.2 INSTALLATION

Installation involves the site preparation, installation of the gadgets, fluctuation (that is non interference with wiring system) and climate. (That is air condition).

Putting in place computers in an organisation for the purpose of security of some vital information. A separate room (computer room) with all the requirements for the smooth operation of those computers is necessary for the durability of such computer systems.

5.3 CONCLUSION

Having gone through this project work, any organisation should ensure that the appropriate security measures should be taken to forestall destruction of personal data and against accidental loss.

In conclusion the field of data security is still open to many new ideas and it is hoped that courses in this field would be included in the course of study in the computer training of employees in organisations as well as students in the universities.

RECOMMENDATION

Having looked at the need for an effective means (mechanism) for storing and processing data and having come to the conclusion that computer offers us the best possible choice for fast retrieval, storage and processing. It is imperative in cases where data stored are sensitive and liable to fraudulent modification and usage; that adequate security measure should be taken to prevent unauthorised access.

Various methods of data access control had been looked into, and for the sample program attached, use of password and encryption had been implemented. It is important that in assigning password and encryption keys, that the following points be remembered.

(i) They should be easy for users to remember

(ii) They should be difficult for an intruder to guess.

(iii) Password should be changed frequently.

(iv) They should be well protected (not written down)

(v) The longer the password/key the more desirable it is.

(vi) They cannot be found in a dictionary.

As new security methods are introduced, attack becomes igenious, thus for many organisations, the emphasis should be on backups, recovery and procedures.

To computer users:

(a) Managers should: -

Define responsibilities of those involved in system design, in systems use and in auditing. Develop a 'computer code of conduct and watch out for violators.

Ensure adequate training is given at all levels.

Become personally computer literate.

Allow realistic time and budget schedules for developing security in computer systems.

(b) Auditors to companies should:-

Lias with computer staffs in development of systems. Ensure provision of adequate audit trails. Become personally computer literate.

(c) Computer room employees should: -

Be aware of the need for security. Ensure that programmers and analyst posses general business skills, as well as technical expertise.

Allow sufficient time to develop secured systems during program development.

(d) Those concerned with security

Become computer literate.

Analyse risk associated with using the computer .

Always interrogate (whenever necessary) the computer staff, auditors or others users of the system. Only authorised users should be given the passwords and encryption code.

(e) The government should: -

Enact computer specific laws to deal with computer related crimes. Set up a computer crime unit in the Nigerian Police Force to monitor and persecute computer crime.

REFERENCES

(1) Anderson R.G. "Data processing principles and practice. Longman Group U. K

(2) Andrew L. Freindman (1989) "Computer systems Development history, Oganisation, Implementation Publisher, Wiley Series.

(3) Badmus R.O "System Analysis and Design" Lecture note.

(4) Caroll J.M "Computer security" Butterworth Publishers U.S.A 1987.

(5) Everest C. Gordon "Database management objectives" System function administration. Mc. Graw Hill book company, New York 1986. Pg. 519.

(6) Harry Garlard (1979) Introduction to Microprocesser system design. Publisher Mc. Graw Hill.

(7) John A. Adam "Threats and Counter Measures". I.E.E.E spectrum August 1992 pp.21

(8) Mathew Rapaporti (1991) Computer medicated communication John Wiley.

(9) Management of B-S computer services. "Managing Computer viruses" pp.4.

(10) Vijay Ahuja (1982) Design and Analysis of computer communication network.

```
***ACTIPOP.PRG ***

*** Name this program ACTIPOP.PRG ***
SET TALK OFF
SET ECHO OFF
SET STATUS OFF
SET SCOREBOARD OFF
CLEAR

SET SYSMENU SAVE
SET SYSMENU TO
DEFINE PAD filepad OF _MSYSMENU PROMPT '\<File' COLOR SCHEME 3 ;
        KEY ALT+F, ''
DEFINE PAD viewdpad OF _MSYSMENU PROMPT '\<View' COLOR SCHEME 3 ;
        KEY ALT+V, ''
DEFINE PAD reportpad OF _MSYSMENU PROMPT '\<Report' COLOR SCHEME 3;
   KEY ALT+R, ''
ON PAD filepad OF _MSYSMENU ACTIVATE POPUP file
ON PAD viewdpad OF _MSYSMENU ACTIVATE POPUP view
ON PAD reportpad OF _MSYSMENU ACTIVATE POPUP report
DEFINE POPUP file MARGIN RELATIVE SHADOW COLOR SCHEME 4
DEFINE BAR 1 OF file PROMPT '\<Add New Records' KEY CTRL+A, '^A'
DEFINE BAR 2 OF file PROMPT '\<Sort/Index Records' ;
        KEY CTRL+S, '^S'
DEFINE BAR 3 OF file PROMPT '\<Update Records' ;
        KEY CTRL+U, '^U'
DEFINE BAR 4 OF file PROMPT '\<Delete Records' ;
        KEY CTRL+D, '^D'
DEFINE BAR 5 OF file PROMPT 'E\<xit' ;
        KEY CTRL+X, '^X'
ON SELECTION POPUP file;
        DO choice IN actipop WITH PROMPT( ), POPUP( )
DEFINE POPUP view MARGIN RELATIVE SHADOW COLOR SCHEME 4
DEFINE BAR 1 OF view PROMPT '\<Login Files' ;
        KEY ALT+L, ''
DEFINE BAR 2 OF view PROMPT 'Re\<cords' ;
        KEY ALT+C, ''
ON SELECTION POPUP view;
        DO choice IN actipop WITH PROMPT( ), POPUP( )
DEFINE POPUP report MARGIN RELATIVE SHADOW COLOR SCHEME 4
DEFINE BAR 1 OF report PROMPT '\<Individual' ;
   KEY ALT+I, ''
DEFINE BAR 2 OF report PROMPT 'Sum\<mary' ;
   KEY ALT+M, ''
ON SELECTION POPUP report;
   DO choice IN actipop WITH PROMPT( ), POPUP( )
PROCEDURE choice
PARAMETERS mprompt, mpopup
WAIT WINDOW 'You chose ' + mprompt + ;
```

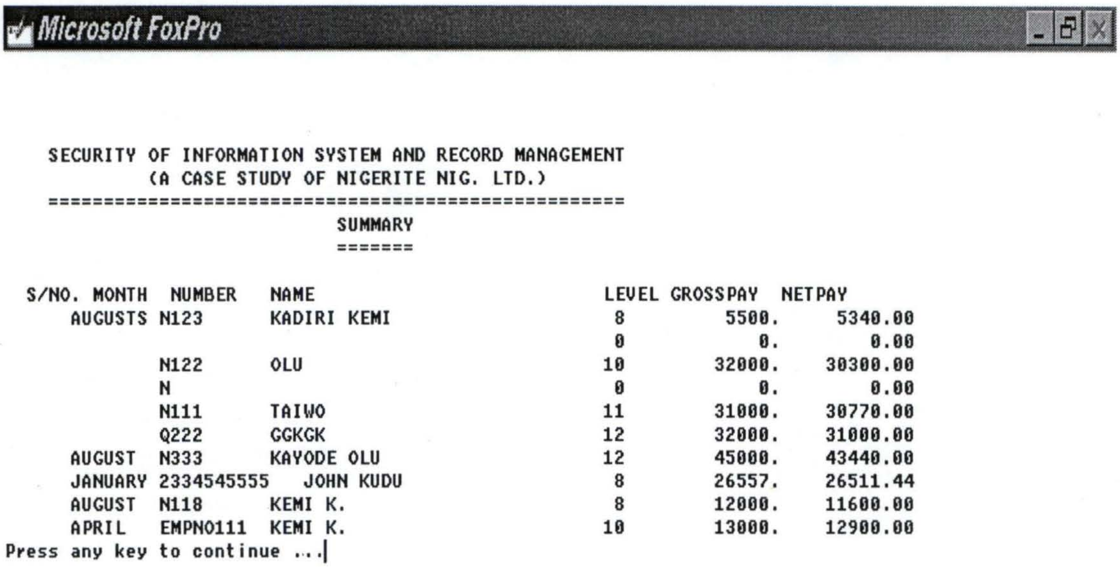
```
      ' from popup ' + mpopup NOWAIT
IF mprompt = 'Exit'
  USE LOGIN
  STORE TIME() TO MTIMEOUT
  REPLACE TIMEOUT WITH MTIMEOUT
  USE
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
      SET SYSMENU TO DEFAULT
ENDIF

IF mprompt = 'Add New Records'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO ADD
ENDIF

IF mprompt = 'Sort/Index Records'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO ARRANGEREC
ENDIF

IF mprompt = 'Update Records'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO MODIF
ENDIF

IF mprompt = 'Delete Records'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO DELREC
ENDIF

IF mprompt = 'Summary'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO REPREC
ENDIF

IF mprompt = 'Login Files'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO VIEWLOGIN
ENDIF

IF mprompt = 'Records'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO VIEWREC
ENDIF

IF mprompt = 'Individual'
  SET SYSMENU NOSAVE
  SET SYSMENU OFF
  DEACTIVATE WINDOW ALL
  DO VIEWREC
ENDIF

PROCEDURE GETDATA
@9,40 SAY "MONTH: " GET MCMONTH
@10,8 SAY "EMPLOYEES' NAME: " GET MNAME
@11,8 SAY "GRADE LEVEL: " GET MLEVEL PICT "99" RANGE 1,16
@12,8 SAY "BASIC SALARY: " GET MBASIC PICT "9999999.99"
@13,8 SAY "TRANSPORT ALLOWANCE: " GET MTRALLOW PICT "99999.99"
@14,8 SAY "HEALTH ALLOWANCE: " GET MHEALLOW PICT "99999.99"
@15,8 SAY "TAX : " GET MTAX PICT "99999.99"
RETURN

PROCEDURE HEAD
CLEAR
@4,4 SAY "SECURITY OF INFORMATION SYSTEM AND RECORD
MANAGEMENT"
@5,4 SAY "        (A CASE STUDY OF NIGERITE NIG. LTD.)"
@6,4 SAY "========================================================="
RETURN


PROCEDURE ADD
ANS="Y"
DO WHILE ANS="Y"
USE PAYROLL
DO HEAD
@7,30 SAY "ADD RECORD"
STORE SPACE(12) TO MEMPNUM
@9,8 SAY "EMPLOYEE NUMBER: " GET MEMPNUM PICT "@!"
READ
LOCATE FOR EMPNUM=MEMPNUM
IF FOUND()
   @14,10 SAY "RECORD ALREADY EXIST IN THE DATABASE"
  @15,10 SAY "PRESS ENTER KEY..."
ELSE
  STORE SPACE(12) TO MCMONTH
  STORE SPACE(30) TO MNAME
  STORE 0 TO MLEVEL
  STORE 0.0 TO
MBASIC,MTRALLOW,MHEALLOW,MTAX,MGROSSPAY,MNETPAY
  DO GETDATA
  READ
  MGROSSPAY=MBASIC+MTRALLOW+MHEALLOW
  MNETPAY=MGROSSPAY-MTAX
  @16,8 SAY "GROSSPAY = "
  @16,30 SAY MGROSSPAY
  @17,8 SAY "NETPAY = "
  @17,30 SAY MNETPAY
  APPEND BLANK
  REPLACE EMPNUM WITH MEMPNUM,NAME WITH MNAME,CMONTH WITH
MCMONTH,LEVEL WITH MLEVEL
  REPLACE BASIC WITH MBASIC,TRALLOW WITH MTRALLOW,HEALLOW
WITH MHEALLOW
  REPLACE TAX WITH MTAX,GROSSPAY WITH MGROSSPAY,NETPAY WITH
MNETPAY
ENDIF
@20,10 SAY "DO YOU WANT TO ADD MORE? (Y/N) " GET ANS PICT "!"
READ
ENDDO
DO ACTIPOP
CLOSE DATABASE
RETURN

PROCEDURE ARRANGEREC
DO HEAD
@8,30 SAY "SORT/INDEX RECORDS"
@9,30 SAY "=================="
@14,10 SAY "WAIT WHILE THE COMPUTER SORTS THE RECORDS"
USE PAYROLL
INDEX ON empnum TAG empnum
@18,10 SAY "RECORDS SUCCESSFULLY SORTED"
@20,10 SAY "PRESS ENTER KEY"
WAIT ""
DO ACTIPOP
RETURN

PROCEDURE MODIF
ANS="Y"
DO WHILE ANS="Y"
USE PAYROLL
DO HEAD
@7,30 SAY "UPDATE RECORDS"
```

```
STORE SPACE(12) TO MEMPNUM
@9,8 SAY "EMPLOYEE NUMBER: " GET MEMPNUM PICT "@!"
READ
LOCATE ALL FOR EMPNUM=MEMPNUM
IF .NOT. FOUND()
   @14,10 SAY "RECORD DOES EXIST IN THE DATABASE"
   @15,10 SAY "PRESS ENTER KEY..."
ELSE
  STORE CMONTH TO MCMONTH
  STORE NAME TO MNAME
  STORE LEVEL TO MLEVEL
  STORE BASIC TO MBASIC
  STORE TRALLOW TO MTRALLOW
  STORE HEALLOW TO MHEALLOW
  STORE TAX TO MTAX
  DO GETDATA
  READ
  MGROSSPAY=MBASIC+MTRALLOW+MHEALLOW
  MNETPAY=MGROSSPAY-MTAX
  @16,8 SAY "GROSSPAY = "
  @16,30 SAY MGROSSPAY
  @17,8 SAY "NETPAY = "
  @17,30 SAY MNETPAY

  REPLACE EMPNUM WITH MEMPNUM,NAME WITH MNAME,CMONTH WITH
MCMONTH
  REPLACE BASIC WITH MBASIC,TRALLOW WITH MTRALLOW,LEVEL WITH
MLEVEL,HEALLOW WITH MHEALLOW
  REPLACE TAX WITH MTAX,GROSSPAY WITH MGROSSPAY,NETPAY WITH
MNETPAY
ENDIF
@20,10 SAY "DO YOU WANT TO ADD MORE? (Y/N) " GET ANS PICT "!"
READ
ENDDO
DO ACTIPOP
CLOSE DATABASE
RETURN

PROCEDURE DELREC
STORE SPACE(4) TO MENCRIPT
DO HEAD
@10,20 SAY "ENCRIPTION VERIFICATION"
@12,15 SAY "ENTER CODE: " GET MENCRIPT PICT "!!!!"
READ
IF MENCRIPT="TFBE"
@15,15 SAY "AUTHENTICATED"
WAIT
ANS="Y"
DO WHILE ANS="Y"
```

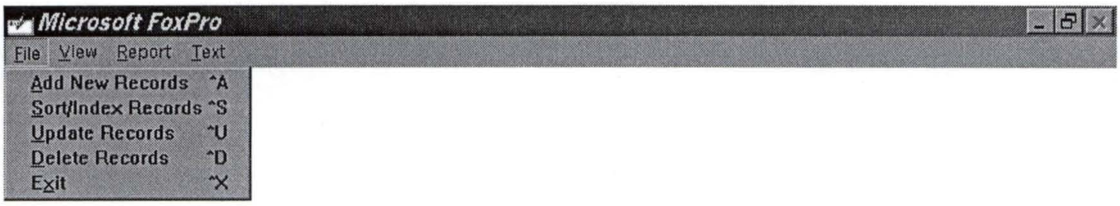
```
USE PAYROLL
DO HEAD
@7,30 SAY "DELETE RECORDS"
STORE SPACE(12) TO MEMPNUM
@9,8 SAY "EMPLOYEE NUMBER: " GET MEMPNUM PICT "@!"
READ
LOCATE FOR EMPNUM=MEMPNUM
IF .NOT. FOUND()
   @14,10 SAY "RECORD DOES EXIST IN THE DATABASE"
   @15,10 SAY "PRESS ENTER KEY..."
ELSE
  STORE CMONTH TO MCMONTH
  STORE NAME TO MNAME
  STORE LEVEL TO MLEVEL
  STORE BASIC TO MBASIC
  STORE TRALLOW TO MTRALLOW
  STORE HEALLOW TO MHEALLOW
  STORE TAX TO MTAX
  STORE GROSSPAY TO MGROSSPAY
  STORE NETPAY TO MNETPAY
  DO GETDATA
  @16,8 SAY "GROSSPAY = "
  @16,30 SAY MGROSSPAY
  @17,8 SAY "NETPAY = "
  @17,30 SAY MNETPAY
  STORE "N" TO REQ
  CLEAR GETS
  @22,10 SAY "Are you really sure? (Y/N)" GET REQ PICT "!"
  READ
  IF REQ="Y"
   DELETE
   PACK
  ENDIF
  @20,10 CLEAR TO 22,79
ENDIF
@20,10 SAY "DELETE  MORE? (Y/N) " GET ANS PICT "!"
READ
ENDDO
DO ACTIPOP
CLOSE DATABASE
ELSE
 @15,15 SAY "ACCESS DENIED"
 WAIT
 DO ACTIPOP
ENDIF
RETURN

PROCEDURE VIEWLOGIN
ANS="Y"
```

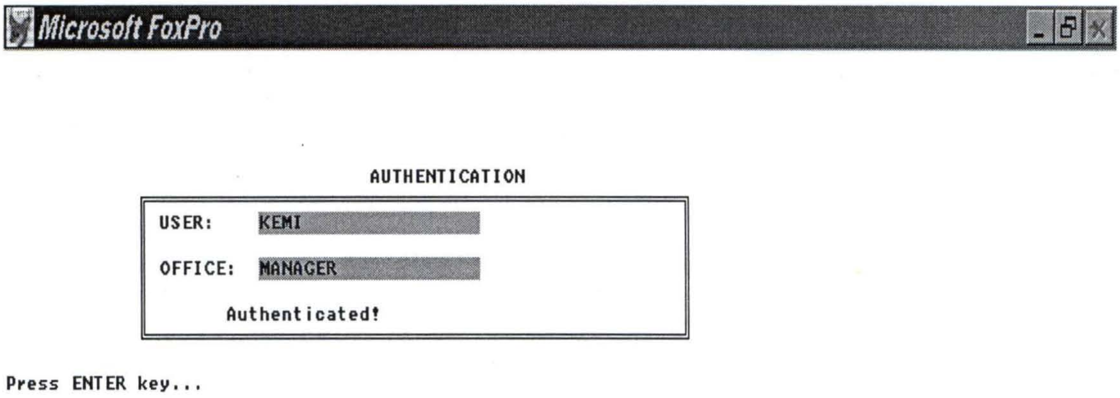
```
DO WHILE ANS="Y"
USE LOGIN
DO HEAD
@7,30 SAY "VIEW LOGIN RECORDS"
STORE SPACE(20) TO MUSER
@9,8 SAY "USER NAME : " GET MUSER PICT "@!"
READ
LOCATE FOR USER=MUSER
IF .NOT. FOUND()
   @14,10 SAY "USER NAME NOT FOUND IN THE FILE"
   @15,10 SAY "PRESS ENTER KEY..."
ELSE
  STORE TIMEIN TO MTIMEIN
  STORE TIMEOUT TO MTIMEOUT
  STORE OFFICE TO MOFFICE
  @12,10 SAY "TIME LOGIN: "
  @12,40 SAY MTIMEIN
  @14,10 SAY "TIME LOGOUT: "
  @14,40 SAY MTIMEOUT
ENDIF
@20,10 SAY "VEIW  MORE? (Y/N) " GET ANS PICT "!"
READ
ENDDO
DO ACTIPOP
CLOSE DATABASE
RETURN


PROCEDURE VIEWREC
ANS1="Y"
DO WHILE ANS1="Y"
 USE PAYROLL
 DO HEAD
 @7,30 SAY "VIEW RECORDS"
 STORE SPACE(12) TO MEMPNUM
 @9,8 SAY "EMPLOYEE NUMBER: " GET MEMPNUM PICT "@!"
 READ
 LOCATE FOR EMPNUM=MEMPNUM
 IF .NOT. FOUND()
    @14,10 SAY "RECORD DOES EXIST IN THE DATABASE"
    @15,10 SAY "PRESS ENTER KEY..."
 ELSE
   STORE CMONTH TO MCMONTH
   STORE NAME TO MNAME
   STORE LEVEL TO MLEVEL
   STORE BASIC TO MBASIC
   STORE TRALLOW TO MTRALLOW
   STORE HEALLOW TO MHEALLOW
   STORE TAX TO MTAX
   STORE GROSSPAY TO MGROSSPAY
   STORE NETPAY TO MNETPAY
   DO GETDATA
   @16,8 SAY "GROSSPAY = "
   @16,30 SAY MGROSSPAY
   @17,8 SAY "NETPAY = "
   @17,30 SAY MNETPAY
   CLEAR GETS
  ENDIF
   @20,10 SAY "VIEW MORE? (Y/N) " GET ANS1 PICT "!"
   READ

ENDDO
DO ACTIPOP
CLOSE DATABASE
RETURN


PROCEDURE REPREC
ANS="Y"
DO WHILE ANS="Y"
USE PAYROLL
DO HEAD
@7,30 SAY "SUMMARY"
@8,30 SAY "======="
@10,2 SAY "S/NO."
@10,8 SAY "MONTH"
@10,15 SAY "NUMBER"
@10,24 SAY "NAME"
@10,54 SAY "LEVEL"
@10,60 SAY "GROSSPAY"
@10,70 SAY "NETPAY"
GO TOP
I=11
K=1
DO WHILE .NOT. EOF()
 @I,3 SAY K
 @I,6 SAY CMONTH
 @I,14 SAY EMPNUM
 @I,24 SAY NAME
 @I,54 SAY LEVEL
 @I,60 SAY GROSSPAY
 @I,70 SAY NETPAY
 I=I+1
 SKIP
ENDDO
WAIT
STORE "N" TO ANS
ENDDO
```

```
CLOSE DATABASE
DO ACTIPOP
RETURN


********PASS1.PRG*****
SET TALK OFF
SET ECHO OFF
SET STATUS OFF
SET SCOREBOARD OFF
SET SYSMENU NOSAVE
SET SYSMENU OFF

CLEAR
DEFINE WINDOW mruka FROM 10,10 TO 22,75 DOUBLE
        ACTIVATE WINDOW mruka
? 'SECURITY OF INFORMATION SYSTEM AND RECORD MANAGEMENRT'
?
? '(A CASE STUDY OF NIGERITE LTD.)'
?
? 'A PROJECT SUBMITTED BY KADIRI RITA OLUWAKEMI
(PGD/MCS/98/99/751)'
?
? 'TO THE DEPT. OF MATHS/COMPUTER SCIENCE F.U.T, MINNA.'
?
WAIT WINDOW 'PRESS ANY KEY TO CON...'
DEACTIVATE WINDOW mruka
USE LOGIN
CLEA
STORE SPACE(20) TO MUSER
STORE SPACE(20) TO MOFFICE
STORE SPACE(6) TO KEMI
TRIAL = 0
STORE SPACE(4) TO PWORD
  @6,12 TO 12,61 DOUBLE
  @7,14 SAY "USER:   " GET MUSER PICT "@!"
  @9,14 SAY "OFFICE: " GET MOFFICE PICT "@!"
  READ
  MUSER=LTRIM(MUSER)
  MUSER=RTRIM(MUSER)
 DO WHILE TRIAL <= 3
  @5,33 SAY "AUTHENTICATION"
  @11,13 SAY " Enter your Password"
  @11,37 CLEAR TO 11,41
  STORE 0 TO K, COUNTER
  PWORD = SPACE(0)
  P = 37
  @11,37 SAY SPAC(24)
  DO WHILE COUNTER < 6 .AND. K <> 13
  P = P + 1
  K = 0
  DO WHILE K = 0
       K = INKEY()
  ENDDO
  IF K <> 13
       @11,P SAY "*"
       PWORD = PWORD + CHR(K)
  ENDIF
 ENDDO
 IF PWORD <> "KEMI"
   TRIAL = TRIAL + 1
   @11,14 SAY SPACE(40)
   @11,14 SAY "Invalid Password!"
   WAIT ""
   IF TRIAL > 3
       @18,10 TO 20,60
       @19,20 SAY "Unauthorized user is not allowed! O.K"
       @21,10 SAY ""
       WAIT "Press ENTER key..."
       SET COLOR TO
       CLEAR
  ENDIF
  LOOP
 ENDIF
 IF PWORD = "KEMI"
   @11,14 SAY SPACE(30)
   @11,20 SAY "Authenticated!"
   @13,10 SAY ""
   WAIT "Press ENTER key..."
   STORE DATE() TO MDATEUSED
   APPEND BLANK
   REPLACE TIMEIN WITH TIME(),USER WITH MUSER,OFFICE WITH
MOFFICE
   REPLACE DATEUSED WITH MDATEUSED
   USE

   DO ACTIPOP
   RETURN
 ELSE
  SET COLOR TO
  CLEAR
  QUIT
 ENDIF
ENDDO
RETURN
*********END OF PASS1.PRG****
```

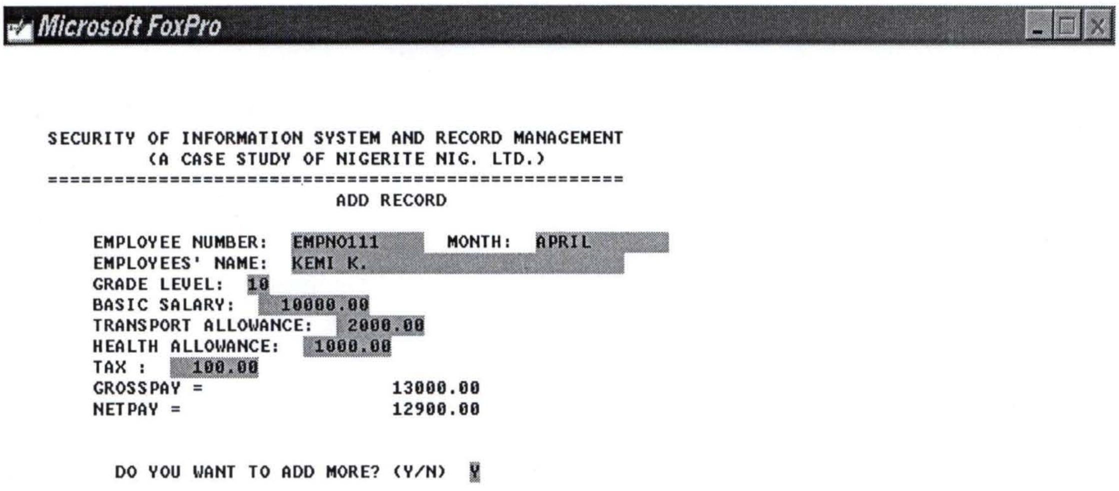


```
    SECURITY OF INFORMATION SYSTEM AND RECORD MANAGEMENT
             (A CASE STUDY OF NIGERITE NIG. LTD.)
    ====================================================
                                  SUMMARY
                                  =======

  S/NO. MONTH   NUMBER    NAME                       LEVEL GROSSPAY  NETPAY
      AUGUSTS N123      KADIRI KEMI                   8       5500.      5340.00
                                                      0         0.         0.00
              N122      OLU                           10     32000.     30300.00
              N                                       0         0.         0.00
              N111      TAIWO                         11     31000.     30770.00
              Q222      GGKGK                         12     32000.     31000.00
      AUGUST  N333      KAYODE OLU                    12     45000.     43440.00
      JANUARY 2334545555   JOHN KUDU                  8      26557.     26511.44
      AUGUST  N118      KEMI K.                       8      12000.     11600.00
      APRIL   EMPNO111  KEMI K.                       10     13000.     12900.00
Press any key to continue ...
```

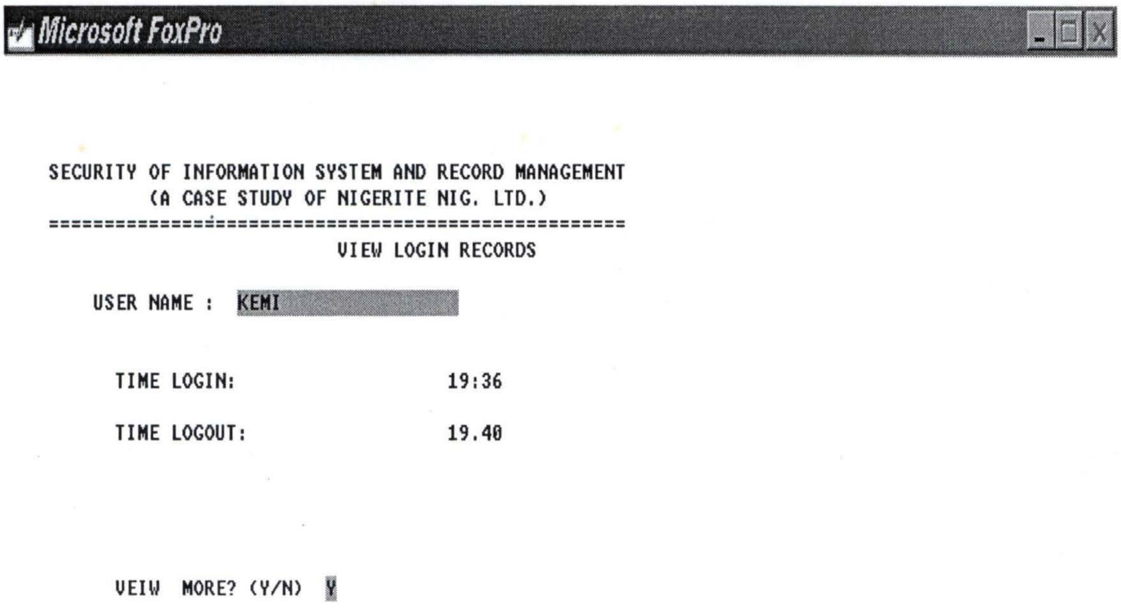

Microsoft FoxPro
File
View
Report
Text
Add New Records ^A
Sort/Index Records ^S
Update Records ^U
Delete Records ^D
Exit ^X



```
                         AUTHENTICATION
       USER:     KEMI

       OFFICE:   MANAGER

              Authenticated!

Press ENTER key...
```



```
SECURITY OF INFORMATION SYSTEM AND RECORD MANAGEMENT
        (A CASE STUDY OF NIGERITE NIG. LTD.)
====================================================
                        ADD RECORD

    EMPLOYEE NUMBER:  EMPNO111     MONTH:  APRIL
    EMPLOYEES' NAME:  KEMI K.
    GRADE LEVEL:  10
    BASIC SALARY:   10000.00
    TRANSPORT ALLOWANCE:   2000.00
    HEALTH ALLOWANCE:  1000.00
    TAX :   100.00
    GROSSPAY =                 13000.00
    NETPAY =                   12900.00

      DO YOU WANT TO ADD MORE? (Y/N)  Y
```



```
SECURITY OF INFORMATION SYSTEM AND RECORD MANAGEMENT
        (A CASE STUDY OF NIGERITE NIG. LTD.)
====================================================
                         VIEW LOGIN RECORDS

    USER NAME :  KEMI

      TIME LOGIN:                 19:36

      TIME LOGOUT:                19.40



      VEIW  MORE? (Y/N)  Y
```