INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

POLICIES AND PROCEDURES MANUAL

VERSION CONTROL			
VERSION	**DATE**	**CHANGE DESCRIPTION**	**SIGN-OFF**
AIK v1.0		**Version 1.0** of AAR procedures	
AIK v1.1	24/04/2018	**Version 1.1** Security update	

Table of Contents

APPROVAL

The **Board** has approved this ICT Policies and Procedures Manual.

Signed on behalf of the **Board** Date:

Date of last update: ……

GENERAL PRINCIPALS GOVERNING COMPANY INFORMATION

The following fundamental principles apply for all company information;

The company has absolute ownership of all information processed using its information hardware hence can access all information without seeking for the affected parties' authorization.

Company staff will access company data only for delivery of services to the company.

Each department is ultimately responsible for its own data. ICT department only supports their functions.

Any government, department, agency or other regulatory body that requires company data can be allowed access only if the data will be used to develop, promote and protect the company or to manage company resources at a macro Level. Any outsourced service shall be subject to rules and regulations in this manual.

The policies apply to all computing platforms and any technology used to process, maintain, retain, destroy or store company data.

The policies also apply to traditional paper based company data too.

The company has designated the IT Network and Security Administrator to develop, implement,monitor and evaluate the company's IT network and compliance policy.

Computer systems which process and store company data will be subject to a periodic independent inspection and audit of security and privacy safeguards review.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to andincluding termination of employment.

INFORMATIONSYSTEMS ACQUISITION, DEVELOPMENT,IMPLEMENTATION AND MAINTENANCE

Policy : All Information systems acquired by AAR Insurance Company shall be governed by preset guidelines.

Purpose: The purpose of this policy is to provide a framework via which information systems are acquired, developed, implemented and maintained.

Scope: The policy will apply to ICT department

Responsibilities: ICT Manager

Definitions:

Procedures:

(a) Acquisition

A business case report justifying the acquisition of the software has to be written and approved bythe ICT manager before the process of acquiring or developing the software begins.

After this the following is done

i). A feasibility study is done and documentation for the same done. The feasibility report shouldamong other issues outline the viability and expected benefits of undertaking the project.Where possible the expected payback period and return on investments should be included inthe report.

ii). A user requirements specification is done. The actual users of this system develop the userrequirements and are required to sign this off.

iii). The selection process begins and will involve developing a request for information (RFI) afterwhich a Request for Proposal (RFP) is done and forwarded to the vendors via the procurementsection of the group.

System demonstrations or site visits or both are then done and should focus on reliability ofvendor's solution, commitment to service, training and documentation.

Possible alternate solutions are evaluated.

IT vendor valuation is done and a report produced.

Final selection, contract negotiation and signing are done.

(b) Development

There are cases where software will be developed in-house. In this case the following procedures willbe followed;

A business case for development of the system is formulated.

A decision on the programming standard to be used is made. This could either be objectorientated, visual based, web-based, prototyping or re-engineering.

A design of the system is then done and documented using the standard flow chart symbols byGane and Sarson.

Security considerations for the software are evaluated and documented.

Development process begins

A test plan is developed and documented. Test environment must be secured away from theproduction environment.

A report on the test results is done.

Outstanding issues and re-test where errors have been located.

(c) Implementation

An implementation plan is formulated. The plan should contain the staff responsible, the tasksinvolved and the process of verifying the tasks.

Back-out procedures are laid down

Data conversion procedures are laid out.

Acceptance testing is done and is signed off by users.

Test environment must be secured from the production environment.

Certification and accreditation is then done

A post implementation review is then done and completed to verify that the system was designed and developed properly including the security guards.

Findings and conclusions/recommendations are then documented.

(d) Maintenance

In-house developed software will be reviewed yearly

For outsourced software, maintenance contracts must be maintained with the supplying vendor

A yearly review of the vendor will be done and will include vendor review too.

For new requirements on existing systems, the user department should present their case in writing vividly outlining their new requirements.

Forms:

Information systems acquisition checklist

ICT SYSTEMS SECURITY

Policy: All ICT systems at AAR Insurance Company shall be secured.

Purpose: The purpose of this policy is to provide guidelines that will ensure that information at AAR Insurance Company satisfies the three pillars of information security which is confidentiality, Integrity and availability (CIA).

Scope: This policy covers all employees of AAR Insurance Company.

Responsibilities: Board OF Governors

Definitions:

Procedures:

Authentication and Authorization

Authentication is the process whereby individuals confirm their identity on a system. Authorization isa process of deciding whether a user is allowed to access a certain resource within the network.

All use of computing systems must be authorized

All users will be accountable to the use of their own username and password.

All users joining the organization will be created in the system and provided with a login name and an initial password which must be changed by the user on first logon.

Login names will follow the syntax; [InitialFirstLetterFirstName][Surname] e.g. for a user Frank Woods, the user name will be FWoods.

Do not leave your computer open. Always lock it if you happen to step out.

The system should lock out a user ID after 5 Consecutive failed login attempts.

No access will be permitted to system and data resources without the user being identified. The identifier should uniquely identify the individual.

Single login to applications via active directory will be encouraged.

Where the authentication process uses unique authentication codes or passwords, the following conditions will apply:

a) Individual users will have the ability to set their own passwords.

b) All system password files must be stored in an encrypted file that cannot be read by any other user.

c) Passwords must contain a minimum of 8 characters, must contain a number and the first character must be in UPPER-CASE. The rest can be in lower case and can contain symbols.

d) Passwords should not be displayed in clear text at sign-on, on reports or be trapped in transaction logs.

e) The security system must force users to set a new password after a password has been reset by the IT Network and Security Administrator.

f) The security system should lock-out a user ID after 3 consecutive failed sign-on attempts.

g) The ability to reset passwords will be restricted to domain administrators.

h) Passwords should not be hard coded into any system file or routine.

i) Passwords should be changed after every 30 days.

Passwords

Passwords will have the following characteristics

i). First letter of the password will be in UPPER CASE (Capital Letters) while the rest of the characters will be in lower case (Small letters).

ii). The password shall not be less than eight characters.

iii). The password must contain a numeric value.

iv). Passwords will be in such a way that it will not be easy to guess it. Avoid using common names associated with you e.g. relatives name, pet names e t c

An Example of a valid password is **Password1**.

Passwords must never be shared or communicated to anybody.

There will be a group policy that forces all passwords to expire within 30 days.

Upon request and approval by GM ICT and immediate supervisor one can be exempted from password change every 30 days based on the nature of their job.

All system password files must be stored in an encrypted file that cannot be read by any other user.

Passwords for any system should never be displayed in clear text.

The ability to reset passwords will only be by administrators.

Sharing of Information, Files and Folders

Sharing of access rights jeopardizes information security and is therefore not allowed.

Users are not allowed to share passwords.

Audit trails must be setup for all systems.

Should an audit trail show that your account was used to perform an irregularity then you will be held accountable.

Input and Output Controls

All data being input to a system either locally or remotely must be accounted for:

Data should be checked for accuracy prior to entry.

All data input into the system must have integrity. They must be correct to its nature and

must not be altered without due authorization.

Logs recording all details of transactions together with supporting authorizations should be maintained and safeguarded. The System Administrator will be the custodian of these records.

Where output is provided on hardcopy or in electronic form:

a) only the number of copies of output specified by the person requesting the output should be produced;

b) distribution of all output should be logged;

c) the appropriate security classification or designation should be marked on all output;

d) output should be delivered only to the owner or to a person who has been authorized to receive it; and

e) receipts should be obtained when output is delivered.

When data is copied for backup purposes, the copy should be verified to ensure the process was successful.

Sufficient generations of backup data should be maintained to ensure that data can be recovered. (Consideration must be given to the length of time an error could remain un detected to ensure a backup will recover valid data.)

Access Logs review

The system logs will be checked on a bi-weekly period to verify that all processing was

authorized.

A report on the type and frequency of system, security and application errors will be kept and reviewed. The information in this report will be reviewed for security connotations by the Network & Security Administrator.

Where feasible, usage meters/recordings on information technology equipment will be regularly read, logged and reviewed for maintenance purposes and to assist in the detection ofunauthorized use of the system.

The Network & Security Administrator must periodically verify that all work is authorized

Virus Protection

Virus scanning software must be installed on both the personal computers and the LAN serverwhich will automatically push updates to the clients.

All media received from external sources, including licensed or copyright software, must bescanned for the existence of viruses.

All original master copies of software must be stored on media with the write-protect securityfeature activated.

Computer systems should be scanned for the existence of viruses after an upgrade or change ofsoftware and after each instance of hardware maintenance.

Use of removable media e.g. Flash disks is not allowed

Security Incident Reporting and Management

A security incident reporting shall follow the following procedure;

i) . Record the security activity and event(s) to be monitored,

ii) . Outline the method of determining how the activities and events are to be monitored,

iii) . Record the type of records to be kept, and how and when the security information is to bereported.

iv). Once the incident has been solved, communication will be done by the GICT Manager.

ICT Security incidents will be investigated by the Network & Security Administrator andrecords maintained on each case.

If these security incidents constitute a possible breach, they should be reported to the CEO ofthecompany, generally through the IT Business Partner.

State and national legislation, as well as company policy, require some types of incidents to bereported to the police.

Inventory of Assets and disposal procedures

The company must maintain a detailed inventory of company information assets. The inventoryshould include:

i) All hardware components, such as computers, printers, disk drives and other data storageequipment, telecommunications equipment, environmental control equipment, etc.;

ii) All software components, such as office automation programs, financial and clinical

application programs, database management programs, communications programs, engineeringand scientific programs, design and drawing programs, compilers, etc.;

iii) All databases;

iv) All communication networks, including local area networks, wide area networks, wirelessnetworks, etc.

Hardware inventory records should include:

i) Description;

ii) Manufacturer/supplier;

iii) Model number;

iv) Serial or license number;

v) Warranty or maintenance conditions;

vi) License conditions;

vii) Location;

viii) Number and identity of authorized users.

Software and database inventory records should include:

i) individual applications,

ii) individual programs,

iii) database and files (libraries),

iv) software procedures (e.g. command or script files),

v) software utilities,

vi) security-relevant software components,

vii) systems software,

viii) software under development or test,

ix) warranty/maintenance conditions (e.g. period covered), and

x) number and identity of valid/licensed users.

Software and database inventory records for each item should include the following information:

i) the number of copies and their locations (e.g. Server room, off-site storage);

ii) identification of owner, custodian, authorized user and maintainer, and

iii) date created or modified, version/level number and any special modifications.

Computers will be considered disposable material after they have been used for a period of atleast three Years. This could be donated in line with the company's corporate social responsibilityprogram.

Any IT system disposed must be signed off by the IT Business Partner and handed over to procurement for further disposal.

Problem Reporting and the helpdesk

Procedures must be developed, documented and implemented for reporting, recording, tracking and resolving system problems.

Records of problems and their resolutions should be retained for a period of at least one year.

System problems affecting security should be immediately reported to the IT Business Partner.

Change Control

All control procedures for any change to the system hardware, software, database or communications network must be documented. The procedures should include the mechanism for requesting changes, recording and tracking outstanding requests,

approval of requests, testing and documentation of changes and incorporation of the changes.

All system modifications, maintenance activities and physical or logical re-configurations shouldbe authorized by the IT Business Partner.

Additions, deletions or alterations should not compromise the intended security profile of thesystem.

All changes to the system should be centrally controlled and documented.

Forms

Change control forms

PHYSICAL AND ENVIRONMENTAL SECURITY

Policy: All ICT systems and equipment at AAR Insurance Company shall be physically secured and kept in a secure environment that must conform to the manufacturers environmental conditions

Purpose: The purpose of this policy is to provide guidelines that will ensure that all systems and ICT equipment shall be kept in a physically safe and environmentally secure location.

Scope: This policy covers the entire group

Responsibilities: Board of Governors

Definitions:

Procedures:

(a) Location, Construction and Protection of Equipment

Information processing facilities and equipment should be located within the building and where there is no exposure to:

i) fire, water, corrosive agents and smoke from adjacent areas;

ii) flooding;

iii) explosion or shock;

iii) unauthorized access;

iv) undesirable, externally-generated electromagnetic radiations; and

v) potential hazards from physically adjacent areas.

Where site selection cannot compensate for identified risks, reasonable precautions should be taken.

Buildings housing company information facilities, equipment and data must conform to relevant statutory codes and standards (e.g. fire, building and electricity).

Entrances to areas containing company data, hardware or software must be protected with secure doors and locking hardware.

Where feasible, utility service lines providing support to company equipment and storage areas should enter the building from underground.

The number of openings to areas housing company data or related hardware and software should be kept to a minimum, consistent only with fire regulations.

There must be power backup facilities in all buildings housing our information systems

equipment.

(b) Access Control to Secure Places

All areas where data is processed and/or stored, and areas housing utilities or service facilities supporting information equipment, including air conditioning, telephone terminal, and electrical distribution rooms, should be designated as secure areas.

Access privileges to secure areas should be authorized and controlled.

Unauthorized personnel and visitors who require access to secure areas should be escorted by authorized personnel at all times.

Signs indicating "authorized personnel only" or a similar message should be prominently posted at all entrances to secure areas.

Unauthorized access to secure areas when the area is unattended and unoccupied is prohibited.

Access control methods should be provided for all secure areas e.g. card swipe mechanisms

Surveillance methods, such as motion detectors and alarms, should be installed in all secure areas.

Authorization lists should be maintained for:

a) Access to secure areas, sensitive documents and

b) All access control items, including keys, codes, combinations and badges.

Records, in the form of an access control log should be kept of access to secure areas for:

i) Visitors

ii) External maintenance and support personnel and

iii) Authorized personnel outside of normal business hours or assigned hours of work.

The access control log should record the following information:

i) Identification of the person entering;

ii) Employer or affiliation;

iii) Identification of the individual authorizing entry;

iv) Restricted area to be entered;

v) Date and time of entry; and

vi) Date and time of departure.

All persons admitted to a secure area should wear an approved access badge or identificationcard.

All security logs should be reviewed periodically including CCTV logs if available.

c) Utilities and Services Support

Installation, monitoring and maintenance of environmental support equipment, communications wiring and equipment, electrical wiring and equipment, plumbing and other utilities and services shall be consistent with the manufacturers' specifications.

Uninterruptible power supply (UPS) or Generator service for essential information processingequipment shall be installed.

Air conditioning for all information system equipment and storage areas must conform to theequipment manufacturer's specifications.

Where there is a possibility of water damage, protection should include:

i). Adequate drainage to remove excess water; and

ii). Water detection equipment.

Flammable and caustic materials should not be stored in areas housing information equipmentand data.

The use of materials known to produce static electricity or magnetic forces should be prohibitedin equipment and data storage areas.

(d) Fire Protection

Fire protection for all information systems and data storage areas must conform to all fireregulations governing the location.

(e) Waste Disposal

Records, orders and other documents and recording media containing company data or securitycontrol records should be destroyed in an appropriate manner (For example: burning,shredding, disintegration).

Media containing company data awaiting destruction should be stored in a secure manner.

(f) Offsite Facilities

Physical and environmental security provisions for off-site storage should conform to the samestandards as primary facilities.

Plans for backup facilities should ensure that physical and environmental security at the backupsite can be made commensurate with the primary site.

The location for off-site storage should not be subject to the same exposure to a specific threatas the primary site.

(g) Storage Media

Where removable media, such as floppy diskettes, magnetic tape, optical disk, or hardcopy, areused to store company data:

i) the media should be stored in a secure container when not in use;

ii) where confidentiality is a concern, the data should be encrypted; and

ii) the media should be tracked or controlled whenever it is stored or moved outside of a securearea.

All company data, whether it is on magnetic media, optical storage media or hardcopydocument should be secured whenever the system or secure area is left unattended.

Forms

HUMAN RESOURCES AND SECURITY

Policy: People play an important role in information systems use and security. All employees of AAR Insurance Company are required to be familiar with policies relating to information use and security.

Purpose: The purpose of this policy is to provide guidelines that will ensure that all employees of the group are familiar with information use and security

Scope: This policy covers the entire group

Responsibilities: Board of Governors

Definitions:

Procedures:

a) Recruitment

Upon recruitment the prospective staff should confirm that they are bound by a professional code of ethics/conduct.

As a condition of employment, each employee should sign a witnessed and dated "Pledge ofConfidentiality and Privacy" indicating that they have been made aware of the companies ITsystems security and privacy policy and the consequences of breaching itBefore commencement of duties, the company should formally advise employees of:

i) Levels of security access

ii) Their responsibilities with respect to the security and privacy of company data.

(b) Security awareness and training

The company will provide orientation and training to all employees, professional staff, contractstaff and volunteers concerning the policies and procedures for ensuring the privacy andsecurity of company data. Orientation and training programs should include:

i) security and privacy policy,

ii) security procedures,

iii) employee responsibilities,

iv) reporting security and privacy violations.

A certificate of attendance at a security awareness or training program will be placed on theemployee's personnel file.

Security awareness and training programs will be provided to employees, professional staff,contract staff and volunteers on a periodic basis annually to maintain awareness and provideinformation about new policies or procedures.

(c) Personnel Security

A record will be maintained and be readily available documenting:

i) The issue and retrieval of security-related items such as keys, codes, combinations, badgesand system passwords;

ii) The custody and use of all information system assets such as loan or issue of computer

hardware (eg. laptop), computer software, and specialized equipment.

On termination or transfer of employment, or when the employee's duties no longer requireaccess to company data, the company will:

i) revoke access privileges (eg. user-ID's and passwords) to system and data resources, andsecure areas,

ii) retrieve sensitive material including access control items (eg. keys and badges), and

iii) retrieve all hardware, software and documentation issued or loaned to the employee.

The company will institute corrective and disciplinary procedures to address any breach ofsecurity or privacy.

Staff performance reviews should assess performance related to the handling of company data.

In the case of contracted personnel and services, it should be a condition of the contract thatsuch personnel be bound by all policies and procedures of the company concerning the securityand privacy of company data including the completion of the Pledge of Confidentiality andPrivacy form.

(d) Separation of duties

IT department must have an organization structure and job descriptions designed to ensure anappropriate separation of duties.

Forms

Matrix on segregation of duties

COMMUNICATIONS SYSTEMS SECURITY

Policy: All communication systems must have controls surrounding their use

Purpose: The purpose of this policy is to provide guidelines that will ensure that adequate controls are placed around all communication systems.

Scope: This policy covers the entire group

Responsibilities: Board of Governors

Definitions:

Procedures:

Security Features

Communications facilities logs will be monitored for discrepancies e.g. protocol errors,

inconsistent communications identification data as related to hardware identification, and polling responses, sequence errors, status and error alarms, data inconsistencies, communications access control errors, nodes (e.g. workstations, etc.) appearing and disappearing on the network, errors in network applications, e.g. E-mail, file-transfer, proxy accounts, routing e.t.c.

Surveillance tests will be conducted periodically to ensure communications controls have not been compromised or misused. Results of these surveillance tests will be recorded for audit and quality assurance purposes.

All unsuccessful system access attempts must be recorded and reviewed.

Company data, passwords and other company or security related information, if communicated over an uncontrolled network, should be encrypted.

Maintenance and Support of communication systems

Where access to company data is possible, contract personnel performing maintenance should be supervised by a knowledgeable employee or other person responsible to the company who understands the implications of actions taken.

The use of communications test equipment, communications software utilities, network monitoring tools and diagnostics for monitoring the network should be authorized and controlled.

Communications Equipment Control

Communications equipment, excluding user workstations, terminals or other peripheral input/output devices, should be operated only by authorized personnel.

All communications components (e.g. gateways, routers, etc.) should be located in secure physical facilities as outlined in the physical security section.

Remote Access

Information systems that access the company's system and data resources from a remote location should conform to the general guidelines outlined in this policy.

[Examples: employees working from home, employees with laptops working from remote locations]

Where company data is communicated to remote locations across public telephone lines, radio frequencies, or by means of electronic mail or electronic data interchange (EDI), the data should be encrypted.

Where the company has local area networks or other information system resources that are connected to public networks such as the Internet and there is a risk of unauthorized access, the company systems should be protected by means of a firewall.

Internet Use

Internet is available for productive use only.

There are three groupings for use of internet namely; AAR Internet Users and AAR Managers and AAR night shift users.

i).AAR internet users- Have access to internet every day before 8.00 am and after 5.00pm.

ii). AAR Managers- Have access to the internet throughout

iii). AAR Night Shift users- Have access of internet from 6.00 pm up to 6.00am

Access to unauthorized sites; betting, gaming, pornography and entertainment is prohibited. Downloading/uploading and/or installing files are strictly prohibited.

Facsimile Communications

Company data should be transmitted by facsimile only when required for urgent or emergent service.

The sender of the data should be responsible for ensuring the security of company data

transmitted.

The facsimile device (fax machine, fax modem, etc.) should be located in a secure area where it can be monitored and used by authorized persons only.

The following steps should be taken when transmitting company related data:

a) The receiver should be notified by telephone that the data is being transmitted.

b) The receiver should stand by to receive the data.

c) The sender must take utmost care to assure the accuracy of the fax numbers dialed.

d) The sender should transmit a covering letter to accompany the company related data. The letter should contain the following:

i) name, address and phone number of the sender;

ii) name, address and fax number of the receiver;

iii) number of pages transmitted;

iv) a notice that the data is confidential and is not to be copied or released without the prior written approval of the sender;

v) the purpose for which the data is provided.

Where there is doubt about the security of the receiving fax machine or the ability of the receiver to ensure privacy and confidentiality, communication by fax should be denied and other methods of transmitting the data employed.

Where there is frequent transmission between two points, or where faxes are sent to a fax mail-box, transmissions should be encrypted.

Cellular and Radio Frequency Communications

Cellular telephones and other radio frequency communications should not be used for voice,facsimile or transmission of company data unless the information is required urgently and noother alternative is available.

Data transmitted over analogue cellular and other radio frequencies should be encrypted.

APPLICATION ACCESS CONTROL

Policy: All applications must have controls that surround their use in order to maintain data integrity.

Purpose: The purpose of this policy is to provide guidelines that will ensure that adequate controls are put around all applications.

Scope: This policy covers all users in the Company.

Responsibilities: Board of Governors

Definitions:

Procedures:

Access to software

If a user recognizes that an unauthorized access attempt has been made using their user ID or password, the user (or user's supervisor) must report the incident to the Network & Systems Administrator officer.

Access to directories and/or data within a system should be based on user identity and only be granted based on pre-defined authorization.

When access to system and data resources is denied, no indication of the reason for denial should be provided. The user should be directed to contact the IT Business Partner.

Application Security Features

Passwords or similar authenticators should be obscured by one-way encryption.

All changes to systems must be authorized

The following privileges must be restricted and monitored:

i) changing computer system privileges or controls;

ii) changing protective features or parameters affecting another user;

iii) allocating resources;

iv) halting the computing system; and

v) controlling the allocation and sharing of system and data resources (eg. memory, file space, CPU cycles, etc.).

The system should automatically terminate or re-authenticate an interactive user's session when a predefined period of inactivity has been exceeded.

User authentication information should not be included on computer output.

All transactions should be logged automatically, making it possible to re-create the chain of events leading to any addition, deletion or modification of such software or data without recourse to the input source documents.

Controls should be implemented to ensure that the integrity is maintained while the data is stored or processed on the system. Examples of such controls include batch totals, file record counts, file release dates and version numbers, block counts, check sums, hash totals, data edit routines, and file and message authentication coding.

Where 100% availability of the system is required:

i) redundant hardware, communications and software should be used to process the

transactions simultaneously,

ii) hardware and/or software techniques should be used to detect hardware/software failures in the primary and backup systems,

iii) in case of failure of the primary system, the backup system should automatically switch the required hardware, software and communications equipment to primary status, and Systems should record security-relevant events. Such events include:

i) job entry, initiation, completion, deletion, restart, abort

ii) terminal connects, disconnects, configuration changes

iii) user log-on and log-off

d) file, volume, and/or database creation, deletion, access, close, rename, backup and restore

iv) network-related status messages

v) computer operator(s) commands and responses

vi) system and sub-system start-up, shutdown, dump, generated messages or requests, volume mounts and dismounts, configuration changes

vii) use of functions affecting logs (eg. printing, deleting, renaming, altering)

viii) overflow of logging system

ix) changes to access control information

x) changes to lists of authorized users

xi) detected security incidents

Note: Security-relevant information whose confidentiality must be protected, i.e. changes to access control information and lists of authorized users, should not be recorded; only the fact that a change has been made should be recorded.

For each security event, the following information, if applicable, should be recorded:

i) event, name or type,

ii) date and time,

iii) user identification,

iv) terminal identification,

v) job identification,

vi) file identification,

vii) file owner,

viii) account number,

ix) mode of access,

x) volume identification,

xi) configuration details, and

x) nature of incident.

xi). Where log records are machine readable and of sufficient volume to make manual recognition of security-relevant incidents impractical, software routines should be utilized to highlight security-relevant incidents.

xii). When a security-related incident is detected, an alarm should be activated.

Note: Alarms should include a message to a console or printer to be utilized for further analysis, or appropriate notification of the Network & Systems Administrator Officer.

Data and Database administration

Responsibilities for data administration and/or database administration should be established and include:

i) access control,

ii) definition and creation,

ii) data dictionary,

iii) integrity,

iv) backup, and

v) recovery.

Database audit checks should be conducted at regular intervals to verify the logical and physicalconsistency of the database and identify discrepancies such as lost records, open chains andincomplete sets.

A data dictionary should be used to document, standardize and control the naming and use ofdata.Database maintenance utilities that bypass controls should be restricted and monitored.

Following a system or application software failure, the system should be capable of automatically recovering the database. –

Where 100% availability of the system is essential, duplicate databases should be maintained onseparate physical devices and all database maintenance transactions should be performedsimultaneously on both databases.

Automated or manual controls should be implemented to protect against unauthorized disclosure by means of inference search techniques.

Scripts or any routines run on databases should be tested and authorized.

Data integrity verification techniques such as message (record) authentication coding or hashtotal techniques should be implemented.

To facilitate the auditability and authorization of data records stored on the database thefollowing measures should be implemented:

i) The user identification and authentication process should positively identify the authorizer.

ii) The user identification of the authorizer should be retained on the transaction record.

iii) The user identification of the data entry person should be retained on the transaction record.

iv) All critical data elements, including transaction date and time, data entry and authorizer useridentifiers, should be included in the data integrity verification process.

Database Linkage

Databases should be designed to inhibit the linking of data between databases, except asexpressly authorized by the. Steps to inhibit linking may include:

i) Separation of databases that contain client identifying data and service/diagnostic data.

ii) Encryption of patient and provider identifiers in databases containing service or diagnosticdata.

iii) Encryption of extremely sensitive patient service/diagnostic data.

Where company data from a database is downloaded into PCs or laptop computers, the datashould be encrypted, with security mechanisms built into the portable or stand-alone device.

Company data should be erased from the device when it is no longer required.

BUSINESS CONTINUITY PLANNING

Policy: There shall exist a business continuity plan for the company

Purpose: The purpose of this policy is to provide guidelines that will ensure that the organization canrecover from catastrophic events

Scope: This policy covers the entire group

Responsibilities: Board of Governors

Definitions:

Procedures:

Contingency Planning

Back up plans must be present, documented and maintained to ensure the essential level of service will be provided following any loss of processing capability. Plans should cover on-site and off-site recovery. The following issues will be considered as a minimum:

i) recovery from any failure to the system and information resources;

ii) re-establishment of the information system services, following destruction of the facility

providing those services;

iii) forced evacuation of the facility;

iv) strikes and other labor disputes;

v) bankruptcy of critical suppliers; and

vi) loss of critical support systems.

Plans will include the identification of essential systems, information resources, and personnel. Planned responses to contingencies should not compromise confidentiality or integrity requirements.

Copies of all contingency plans, procedures and agreements must be maintained in at least two geographically separate locations.

Contingency plans should be tested annually to the extent that is practical.

Employees required to support an essential level of service will be identified and the up-to-date list should form part of the contingency plans.

Employees identified to take an active role in contingency situations should receive training and practice in their assigned duties.

Backup copies of the essential information should be taken at regular intervals and stored at an off-site location.

Current copies of the critical operational data and material and a sufficient supply of the critical media resources to ensure the continued provision of the minimum essential level of service, as defined in the organizations contingency plan, should be stored at an off-site location. These items should include:

i) operating system software,

ii) utilities,

iii) applications system software,

iv) data,

v) documentation,

vi) encryption keys,

vii) access control information (e.g. passwords), and

viii) forms.

An index of the resources which are stored off-site must also be stored at the off-site location and should contain:

i) Identification of the resources and data

ii) names of the owners of the data, and

iii) the classification or designation of the data.

In the event of a virus attack, the infected machine(s) will immediately be isolated from the network. The machine will then have to be cleaned first before being restored back to the network.

COMPLIANCE

Policy: All staff are required to adhere to legislated requirements for ICT use.

Purpose: The purpose of this policy is to provide guidelines that will ensure that all users are aware oflegislated laws for ICT use.

Scope: This policy covers the entire group

Responsibilities: Board of Governors

Definitions:

Procedures:

Awareness of Legal obligations

All new employees must be made aware of the legal responsibilities with respect to their use ofcomputer based information systems and data. Such responsibilities will be

included in key staffdocumentation such as terms and conditions for employment and the organization code ofconduct.

All employees are required to fully comply with the organizations Information Security policies.

The monitoring of such compliance will be the responsibility of management.

Compliance with the data protection act or equivalent

The organization intends to fully comply with the requirements of data protection policy in sofar as it directly affects the organization.

Data may only be used for the specific purposes for which it was collected.

Data must not be disclosed to other parties without the consent of the individual whom it isabout, unless there is legislation or other overriding legitimate reason to share the information(for example, the prevention or detection of crime).

Personal information should not be kept for no longer than is necessary.

Personal information may not be transmitted outside an area unless the individual whom it isabout has consented or adequate protection is in place, for example by the use of a prescribedform of contract to govern the transmission of the data.

Entities holding personal information are required to have adequate security measures in place.Those include technical measures (such as firewalls) and organizational measures (such as stafftraining).

Complying with copyright and licensing legislation

All employees must be made aware of key aspects of software copyright and licensing in so faras this affects their activities and their duties.

a). Copying and distribution of unlicensed software is not allowed in the organization

b). Contractors or consultants working within the organization are not allowed to use unlicensedsoftware.

c). Individuals using software within the company must be ready to produce the license forinspection.

d). All legitimate software license must be properly kept.

Legal Safeguards against Computer misuse

Unauthorized access to computer system which covers anything from harmless exploration, tohacking for access to specific data is prohibited.

Unauthorized access to computer systems with the intent of using the information accessed fora further offence e.g. extortion is not allowed.

Unauthorized access to computer system with the intent of modifying the contents of thecomputer system is also prohibited.

Defamation, Libel & Slander

Do not create material which might be defamatory (i.e. which falsely states or implies somethingabout an individual that will result in that individual being held in lower esteem by others as aresult).

Libel is a civil offence and may incur substantial financial penalties. Facts concerning individualsor organizations must be accurate and verifiable and views or opinions must not portray theirsubjects in any way which could damage their reputation.

Intellectual Property rights

Intellectual rights refer to the legal protection afforded to owners of "intellectual capital/rights'rights. All company employees should adhere to the intellectual rights law which covers

- Creativity (Individual Capital) - which implies rights to benefit from ones free expression
- Invention (Instructional capital) - which implies rights to benefit from having created some moreefficient device or progress.
- Reputation (Social Capital) - which implies rights not to have one's name or specificdistinguishing tagline or ethic sullied by imitators or rivals.

THREAT RISK ASSESSMENT

Policy: The Company will conduct regular security and privacy threat risk assessments.

Purpose: The purpose of this policy is to provide guidelines that will ensure that the group conductsregular security and privacy threat risk assessments.

Scope: This policy covers the entire group

Responsibilities: Board of Governors

Definitions:

Procedures:

The company will conduct regular security and privacy threat risk assessments. The guidelines will bebased on the following four parts.

1. Definition of assets
2. Threat Assessment
3. Risk Assessment
4. Recommendations

(a) Definition of Assets

The company must identify all assets that may be subject to risk. These assets include:

1. Data/Information

Examples:

- Data bases

- Data files

- Company records

- Hardcopy files and printouts

- Reference and educational material

- Billing records

2. Software

Examples:

- Commercial software products

- Custom developed application software

- Database management software

- Operating systems

- Network software

3. Hardware

Examples:

- Servers and Microcomputers

- Disk and tape drives

- Printers

- Fax machines

- Power Supplies

- Communications devices (routers, controller, etc.)

(b). Threat Assessment

1. Agent or Event

The potential agent or events that could place the asset at risk will be identified.

- Examples:

- Theft

- Vandalism

- Fire

- Flood

- Power Loss

- Unauthorized access

- Viruses

- Corruption of data

2. Class of Threat

For each agent or event, the classification will be by the following types of threat:

- Disclosure

- Interruption

- Modification

- Removal

- Destruction

3. Likelihood

The likelihood of the agent or event occurring will then be classified as:

- Low - meaning there is no history and the threat is unlikely to occur

- Medium – meaning that there is some history and an assessment that the threat may occur

- High – meaning that there is significant history and an assessment that the threat is quite likelyto occur

4. Impact

The impact of each possible event will be rated as follows:

- Very serious (e.g. may compromise clients),

- Serious (e.g. may disrupt normal operations, cause significant inconvenience to clients, or becostly to rectify),

- Less serious (e.g. may disrupt non-critical operations or may cause limited inconvenience toemployees).

5. Consequences

The potential consequences will be identified as follows:

- Loss of privacy

- Loss of trust

- Loss of asset

- Loss of service

(c). Risk Assessment

Assess the adequacy of existing safeguards to protect against potential threats.

1. Existing Safeguards

All the existing safeguards to protect against the potential event should be listed. For example,the company may have after hour's security and surveillance cameras installed at all entrancesto the facility to protect against theft or vandalism, or access security already built into thepresent system to protect against computer hackers.

2. Vulnerability

Describe the vulnerability (ie. How can a threat/threat agent get at the asset being protected).

3. Risk

The potential risk will be classified as:

- Low - requires some attention and consideration for safeguard implementation as goodbusiness practice.

- Moderate - requires attention and safeguard attention in the near future.

- High - requires immediate attention and safeguard implementation.

(d). Recommendations

1. Proposed Safeguards

In consideration of the potential vulnerability and risk, additional safeguards recommended to

lower the risk to an acceptable level should be described including alternative safeguards

providing different levels of protection..

2. Projected Risk

The projected risk of the proposed safeguards should also be rated as:

- Low

- Moderate

- High

I being an employee of AAR Insurance Company hereby give my undertaking as follows:

1. That I will keep confidential all information that may come into my knowledge during or in the courseof my employment and that I shall not discuss and or divulge such information to third parties eitherinternally or externally to the company.

2. Further, whilst working on any documents, I shall ensure that they are securely kept and are dealtwith in such a way as to avoid any third party having access to them.

3. This confidential agreement applies to any form of information of the company and its clientswhether of a financial, personal and/or professional nature, company records, documents, data anyother information which may come into my knowledge during the course of my work.

4. I hereby acknowledge that any breach of the terms of this undertaking may lead to my dismissall agree to abide by the above terms.

Name: ……Signature: ……Date: ……