IT Security Policy Handbook

SIC Group of Companies

State Investment Corporation Ltd

July 2005

Version 1.2

Table of contents

1 Introduction

Communication and Information Technology security, as well as Network systems Security, are becoming extremely important nowadays as we strive to promote the country as a Cyber-Island.

The State Investment Corporation Ltd is very closely linked to major national endeavours in the making of Mauritius-The Cyber-Island. In line with our commitment to ensure security of information to the maximum possible, we are implementing this policy to detail the major aspects of security consideration for the State Investment Corporation Ltd and for the SIC Group of Companies. We are confident that this document will prove very useful for all concerned.

This policy forms an integral part of our search for best practices in all areas of management. We are convinced that it will be instrumental in leading us to attain a high level of information security of information according to agreed guidelines.

Managing Director.

2 Background

With the State Investment Corporation embarking on "Good Governance Principles" and the "Total Quality Management" concept, it is but a sine qua non factor to have established procedures and principles especially to ensure security of information to a maximum possible.

This document is intended for use as a reference document by managers and employees who are responsible for initiating, implementing and maintaining IT security within the State Investment Corporation Ltd (SIC) and the SIC Group of Companies.

The document though intended to be as comprehensive as possible would need to be updated regularly with the advent of new technologies in this particularly ever changing field.

Notice

The codes of practice/policies in this document are to be considered as guidelines. SIC, at this option, may change, delete, suspend or discontinue any part or parts of the policies in this document at any time without prior notice.

3 Objectives

The objective of this document is to attain a high level of information security throughout the SIC Group so as to ensure business continuity and also to allow information to be shared while protecting the integrity of the information and computing assets.

4 Security Policies

4.1 Availability of IT facilities

Each installation should have a written request either through a request form or through e-mail from the manager of that department authorising its purpose and use.

4.2 Inventory of Assets

The IT assets of the company should be accounted so as to ensure protection, conformance to established policies and security. The Fixed Assets Register needs to be updated as soon as an asset is acquired, transferred or disposed.

An annual audit of IT assets include:

- Databases and data files
- Systems documentation
- User Manuals
- Training/Operational manuals
- Applications software (Office productivity tools, business applications software, workgroup productivity tools, development tools, utilities, shareware, groupware…)
- Systems software (operating systems, RDBMS)
- Computer equipment (PC's, servers, printers, scanners, …)
- Data communications & Network equipment (routers, modems, switch, hubs, UPS ..)

4.3 Work-sites

All workstations dealing with sensitive data should be protected and branched on the UPS.

All workstations should be protected from the following hazards:

- Fire
- Smoke
- Water
- Dust
- Vibration
- Electrical supply interference
- Electromagnetic Radiation

Smoking, eating and drinking is prohibited in the IT server room and also while working on the work-stations.

Workstations handling sensitive data should be positioned to reduce the risk of overlooking.

4.4 Recruitment of Personnel

The conditions of employment, especially in the IT dept., should include the signing a confidentiality (non-disclosure) clause. Any application for a job should include at least 2 character references that can be easily verified.

4.5 Third Party Access

Where there is a need for third party access (IT services provider e.g. GSI ltd., Harel Mallac, SIL etc.), the following needs to be spelled out in the contract:

- The IT facilities to be made available in terms of Network Access,
- Files/Directories Access, Database Access should be spelt out in the contract with the third party.
- A list of individuals authorised to use the IT facilities
- The right to monitor and revoke user activity
- The right to audit responsibilities spelt out in the contract
- Restrictions on copying and disclosing information
- Validation/restriction for installation of software
- Authorisation to use media implying that all media should be virus free/free of malicious software
- Date and time of entry as well as departure to be noted
- A third-party staff should always be supervised by a staff of the SIC Group both for safety and to prevent opportunities for malicious operations

4.6 Equipment, data and software off-premises

No IT equipment/data/software owned by the SIC Group can be taken off-premises without prior authorisation from senior management.

While traveling, equipment and media should not be left unattended in public places. Portable computers should be carried as hand luggage when traveling.

Portable computers are more vulnerable to theft, loss and unauthorised access when traveling. All portable computers should have a password either at boot level or operating system level to prevent unauthorised access to their contents.

4.7 Non-SIC Group equipment on premises

Non-SIC equipment should only be allowed on the premises of SIC prior to authorisation from senior management.

4.8 Incident Management

All potential types of security incident including:

- System failures and loss of service
- Errors resulting from inaccurate or incomplete data
- Breaches of confidentiality

should be reported to the IT Department.

In the case of malicious software e.g. a virus, particular consideration should be given to the following:

- Note the symptoms and any messages appearing on the screen.
- Stop using the computer and isolate it from the network, if possible.
- Inform the IT dept. immediately. If a transferable media (e.g. floppy disk, pen drive…) was being used, then it should not be used on other computers.
- Users should not attempt to remove the suspected software.

4.9 Segregation of duties

To minimise the risk of negligence or deliberate system misuse, it is recommended that the following functions be carried out by different employees:

- Business system use
- Computer Operation
- Network Management
- System Administration
- Systems development and maintenance
- Security audit

Note: This control is difficult to achieve owing that the IT department **has got a small team.**

4.10 IT Server Room security

- Hazardous and combustible materials should be stored securely at a safe distance from the IT Room. Computer supplies such as stationery should not be stored in the IT Room until required.
- Appropriate safety equipment should be installed such as heat and smoke detectors, fire alarms and fire extinguishing equipment.
- Papers and diskettes should be stored in cabinets when not in use, especially outside working hours.
- Personal computers/workstations should be protected by screen savers passwords when not in use.
- Doors should be locked when unattended.

- Only authorised people should have access to the IT Server Room.
- A log book should be maintained detailing access to the IT Server Room.

Note: It is recommended to identify an isolated area (external to the IT Room) for delivery and loading of supplies and equipment.

4.11 Equipment Maintenance

The IT equipment should be properly maintained to ensure a high level of availability and integrity.

- All computer equipment should have a maximum 3 months servicing interval.
- Repairs and servicing of equipment should be carried by authorised maintenance personnel.
- A record of all faults per equipment should be kept.

4.12 Environmental Monitoring

Computer environments, including temperature, humidity and power supply quality and dust removal should be monitored so that the computers equipment is not affected adversely.

4.13 User registration

There should be a formal user registration and de-registration procedure for access to all multi-user IT services.

Access to multi-user IT services should be controlled through a formal user registration process which should, for example:

- Maintain a formal record of all persons registered to use the service.
- Immediately remove the access rights of users who have changed jobs or left the organisation.
- Periodically check for, and remove, redundant user Ids and accounts that are no longer required.
- Ensure that redundant user Ids are not re-issued to another user.
- All departments are to provide the IT dept with the necessary information whenever new access is required (e.g. new employee) or access is to be denied (e.g. employee has resigned).

4.14 User password management

The allocation of passwords should be controlled by a formal management process, the requirements of which should be as follows:

- Require users to sign an undertaking to keep personal passwords confidential and work group passwords solely within the members of the group.

4.15 Review of user access rights

To maintain effective control over access to data and IT services, the IT dept. should at regular intervals review users' access rights. This process should ensure that:

- Users' access capabilities are reviewed at regular intervals; a period of 6 months is recommended.

4.16 Password Use

All users are strongly advised to follow these guidelines for maintaining passwords:

- Allocate individual passwords to maintain accountability
- Keep passwords confidential
- Avoid keeping a paper record of passwords, unless this can be stored securely
- Select passwords with a minimum length of 8 characters
- Avoid basing passwords on any of the following :
    - Months of the year, days of the week or any other aspect of the date
    - Family names, initials or car registration numbers
    - Company names, identifiers or references
    - Telephone numbers or similar all-numeric groups
    - User ID, user name, group ID or other system identifier
    - More than two consecutive identical characters
    - All-numeric or all-alphabetic groups
- Change passwords at regular intervals of about 30 days and avoid re-using or 'cycling' old passwords
- Change temporary passwords at the first logon
- Do not include passwords in any automated logon process, e.g. stored in a macro or function key. (E.g. in Microsoft Outlook etc.)
- Alter default vendor passwords following installation of software
- Store passwords in encrypted form, using a one-way encryption algorithm

4.17 Unattended user equipment

- Terminate active sessions when finished, unless they can be secured by an appropriate lock, e.g. screen saver password
- Log off sessions when over. Do not just switch off the PC

4.18 Terminal logon procedures

Any application software implemented at the SIC Group should have the following logon procedures:

- It should not display application identifiers any time till the logon process has been successfully completed
- Display a general notice warning that the computer must only be accessed by authorized users
- Limit the number of unsuccessful logon attempts (maximum of 5)

4.19 Internet Access and e-mail

Company communications systems and equipment, including electronic mail and Internet systems, along with their associated hardware and software, are for official and authorized purposes only. Managers may authorize incidental use which:

- does not interfere with the performance or professional duties,
- is of reasonable duration and frequency,
- serves a legitimate company interest, such as enhancing professional interests or education,

- and does not overburden the system or create any additional expense to the company.

- Employees may not use the Internet for personal commercial purposes, may not access any obscene or pornographic sites, and may not access or use information that would be considered harassing. Employees abusing such privileges will be subject to monitoring of their computer system activity and disciplinary action.

- Access to the Internet and Mail services should strictly be done through the company's proxy server and e-mail server and not through dial-up facilities. Unless the proxy server is temporarily unavailable, the user should contact the IT department to be advised whether to use dial-up facilities.

- Access to the Internet from a company-owned home computer/laptop or through company-owned connections must adhere to all the same policies that apply to use from within company facilities.

- Employees should not allow family members or other non-employees to access company computer systems.

- Users posting to Usenet newsgroups, Internet mailing lists, etc. must include a company disclaimer as part of each message.

- All employees are expected to conduct their use of these systems with the same integrity as in face-to-face or telephonic business operations. Any use perceived

to be illegal, harassing, and offensive or in violation of other company policies can be the basis for disciplinary action.

- Use of SIC's email to participate in chain letters is not acceptable.

- SIC provides electronic mail to employees for business purposes. Limited personal use is acceptable as long as it does not negatively affect the business of SIC.

- The use of email in any way to facilitate the conduct of a private commercial purpose is forbidden.

- If SIC provides access to electronic mail to external users such as consultants, temporary employees, or partners, they must read and sign the email policy statement.

- Only Microsoft Outlook e-mail software is authorized.

- Users must not allow anyone else to send email using their accounts. This includes their supervisors, secretaries, assistants and any other subordinates.

- SIC reserves the right to review all employee email communications. Email messages may be retrieved by the SIC even though they have been deleted by the sender and the reader. Such messages may be used in disciplinary actions.

- Incoming messages will be scanned for viruses and other malign content.

- Software for browsing the Internet such as WWW, Gopher, WAIS, etc. is provided to employees primarily for business use. The authorized browser software is Internet Explorer.

- SIC's Internet users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening, or racially or sexually harassing.

- Users of the WWW are reminded that Web browsers leave "footprints" providing a trail of all site visits.

- All WEB browsers shall be configured to use the firewall http proxy.

- Users may browse the Internet using World Wide Web (WWW), Gopher, WAIS, etc., for the sole purpose of their research or job function.

- No sites known to contain offensive material may be visited.

- Any user suspected of misuse may have all transactions and material logged for further action.

- All sites visited are logged.

- Web browsers shall be configured with the following rules:
    - They will only access the Internet through the firewall HTTP proxy.

- They will scan every file downloaded for viruses or other malign content.

- Web pages often include forms. As with e-mail, data sent from a Web browser to a Web server passes through many interconnecting computers and networks before reaching its final destination. Any personal or valuable information sent using a Web page entry may be eavesdropped on.

4.20 Data back-up

All users are strongly advised to regularly back-up the important data on the local hard disks using tools like MS-backup on the network directories allocated to them. To ensure maximum security, while performing back-up, the users can password their back-ups.

- The drives of the servers as well as the databases on the servers will be backed-up on a daily basis.
- On a weekly basis, back-up tapes of the server drives and the databases are to be sent to the some off-site location (e.g. banks) for safe-keeping
- After major processing like yearly valuations of portfolios, end-of-year processing, proper back-up of databases and master-files should be sent to off-site secure locations for safe keeping and retained for auditing purposes if need be.
- At least 3 generations of back-up data should be retained for important business applications.

- Back-up data should be regularly tested, where practicable to ensure that they can be relied upon as part of contingency planning.
- A log of the back-ups should be maintained to ensure back-up strategy management.

4.21 Virus controls

- Only licensed software should be installed on the company's computing assets. Installation has to be authorised by the IT dept.
- Unauthorised software installation is prohibited and will be subject to disciplinary action
- Anti-virus software should be installed on all computers
- Virus-specific detection software (which should be regularly updated and used as directed by the supplier) should be used to scan computers and media for known viruses, either as a precautionary measure or on a routine basis. This will be automated by the anti-virus software.
- Any diskettes of uncertain or unauthorized origin should be checked for viruses before use.
- Users should never run executable program from an unknown source

4.22 Control of proprietary software copying

- Users are advised not to contravene this policy by copying software from one machine to another without the owner's documented authority.
- Where it is necessary to use a software product on additional machines, licenses should be extended or additional copies purchased.

Regular audits of software use should be taken and software registers maintained.

4.23 Information access restriction

Application of the following controls should be considered in order to support access policy requirements:

- Providing menus to control access to application system function.
- Controlling the access capabilities of users e.g. read, write, delete, execute.

4.24 Clock synchronization

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

4.25 Diskette/Data handling procedures (especially for subsidiaries like EOI)

- All authorised recipients should be formally recorded.
- The diskettes should be first scanned using the latest virus scan software available before use.
- Upon receipt of diskettes the recipients should inform the senders.
- There should be regular review of distribution lists and lists of authorised recipients.

- All diskettes should be sent/received through sealed envelopes. (tamperproof packaging).
- Reliable couriers should be used. Delivery by hand is preferred.
- Files on diskettes should be password protected if possible.

4.26 Separation of development and operational facilities

- Development and operational software should, where possible, run on different processors, or in different domains or directories.
- Development and test work should be separated as far as possible

4.27 Capacity Planning

Capacity requirements should be monitored to avoid failures due to inadequate capacity.

The IT dept Database Administrator and the Network Administrator should monitor the utilisation of key system resources, including processors, main storage, file storage, printers and other output devices, and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system (MIS) tools.

4.28 Management of removable computer media

Removable computer media (tapes, diskettes, CD's etc.) should be managed as follows:

- Use a data storage system that avoids the use of descriptive labels, that is the data stored should not be identifiable from its label
- If no longer required, erase the previous contents of any re-usable media that are to be removed from the organization.
- Require a written authorisation for all media removed from the organisation and keep a record of all such removals to maintain an audit trail.

4.29 Security of system documentation

- System documentation should be physically locked in sturdy cabinets
- The distribution list for system documentation should be kept to a minimum and authorised by the IT dept.

4.30 Documented access control policy

Each business application owner should have, as part of user requirements and sign-off procedures, a clearly defined access policy statement, which defines the access rights of each user or group of users. The policy should take account of the following:

- The security requirements of individual business applications.
- Policies for information dissemination and entitlement, e.g. the 'need to know' principle

4.31 Protection of system test data

Test data should be protected and controlled.

The following controls should be applied to protect live data, when used for testing purposes:

- There should be separate authorization each time live data are copied to a test application system
- Live data should be erased from a test application system immediately after the testing is complete
- The copying of live data should be logged to provide an audit trail

4.32 Disciplinary process

There would be a disciplinary process for employees who have allegedly violated the policies and procedures.

4.33 Measures for Cyclonic Conditions

In event of a cyclone warning class 2 with potential risk of a class 3, the IT dept. should be on standby to switch off all servers. As soon as a cyclone warning class 3 is emitted, IT dept. staff should perform the following:

- Shutdown all applications
- Shutdown all servers
- Remove power cords from power outlet
- Remove telephone line from all modems

IT Staff should make sure that they have the latest update on cyclone bulletins when cyclonic conditions are prevailing.

It is the responsibility of each employee to put at safe every component which can be affected by humidity of the flooring. The following should be carried out by each and every employee:

- Shutdown PC
- Remove PC power cord from power outlets
- Keep PC, modem, etc on tables to avoid damage by humidity of the flooring. The tables should be away from windows so as to avoid water leakage from windows.
- Remove telephone line from all modems

IT Staff should ensure that the above have been completed.

Upon resumption of work, IT staff should perform the following:

- Check the stability of power supply (no fluctuation in power supply and continuous supply of electricity for 30 minutes or so)
- Check for dryness of all equipment. If there is any sign of humidity or water leakage, use the dryer to dry up the equipment.
- Plug in power cords.
- Plug in telephone lines to modems
- Start PC/Servers and applications

Each and every employee should check his/her pc and inform the IT dept. immediately in case there is water leakage or humidity.