Industrial Investment Trust Limited

INFORMATION SECURITY POLICY

March 10, 2021

1 Introduction

1.1 Information Security

Information Security Policies are the cornerstone of information security effectiveness. The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. The overall objective is to control or guide human behavior in an attempt to reduce the risk to information assets by accidental or deliberate actions.

Information security policies underpin the security and well-being of information resources. They are the foundation, the bottom line, of information security within an organization.

We all practice elements of data security. At home, for example, we make sure that deeds and insurance documents are kept safely so that they are available when we need them. All office information deserves to be treated in the same way. In an office, having the right information at the right time can make the difference between success and failure. Data Security will help the user to control and secure information from inadvertent or malicious changes and deletions or unauthorized disclosure.

The basic levels of data security are:

Confidentiality: Protecting information from unauthorized disclosure like to the press, or through improper disposal techniques, or those who are not entitled to have the same.

Integrity: Protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

Availability: Ensuring information is available when it is required.

Authenticity: Ensuring the data, communications or documents (electronic or physical) are genuine.

Data can be held in many different areas, some of these are:

- Network Servers
- Personal Computers and Workstations
- Laptop PCs
- Removable Storage Media (External HDD, CD-ROMS, Flash Drive etc.)

1.2 Data Loss Prevention

Leading Causes of Data Loss:

- Natural Disasters
- Viruses
- Human Errors
- Software Malfunction
- Hardware & System Malfunction

A. Policy For General Users

2 Policies for General Users

2.1 Using Floppies/ CD/ Flash Drives

- External Flash drives, HDDs should be used in consultation with system administrator and should be scanned before use.
- Unofficial CDs or Flash Drives should not be used on office systems.

2.2 Password

- Keep the system screen saver enabled with password protection.
- Don t share or disclose your password.
- User should not have easily detectable passwords for Network access, screen saver etc.
- A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks.
- Never use the same password twice.
- Change password at regular intervals.
- Company's official Password Policy must be implemented strictly.

2.3 Backup

- Backup should be maintained regularly on the space provided on the storage media/ Shared drives as per the company's official Backup policy.
- Keep the removable media in a secure location away from the computer.
- Always keep a copy of all sensitive and important data on the network drives.
- All important files should be backed up before making any major changes.

2.4 Physical Safety of System

- Protect the system from unauthorized use, loss or damage.
- Keep portable equipment secure.
- Position monitor and printers so that others cannot see sensitive data.
- Keep Flash drives, HDDs and other media in a secure place.
- Seek advice on disposal of equipment.
- Report any loss of data or accessories to the System Administrator/IT In charge.
- Keep the system and sensitive data secure from outsiders.
- Get authorization before taking equipment off-site.
- Take care when moving equipment.
- System should be properly shut down before leaving the office.
- Log-off the system if you are leaving your seat.
- Never remove the cables when your PC is powered ON since this can cause an electrical short circuit.
- Do not stop scandisk if system prompts to run it at the time of system startup.
- Always use mouse on mouse pad.
- Be gentle while handling keyboard and mouse.
- Do not open case of the hardware.
- Make sure that there is some slack in the cables attached to your system.

2.5 Computer Files

- All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set.
- Any default shares should be removed.
- Only required file and object shares should be enabled on the server.
- Never download or run attached files from unknown email ID.
- Always keep files in the computer in organized manner for easy accessibility. If required create new folders and sub-folders.
- Avoid creating junk files and folders.
- System files and libraries should not be accessed as it can cause malfunctioning of system.
- When transferring data, be sure it is going to the destination. If asked "Would you like to replace the existing file" make sure, before clicking "yes".

2.6 General Instructions

- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Follow instructions or procedures that come from System administrator/IT Incharge time to time.

- Users are not supposed to do his or her personal work on computers.
- Please intimate System administrator/IT Incharge in case of system malfunction.
- User should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of System administrator/IT Incharge.
- Antivirus software should be updated timely in consultation with System Administrator/IT Incharge.
- Don't give others the opportunity to look over your shoulder if you are working on sensitive data/contents.
- Do not use unnecessary shareware.
- Do not install or copy software on system without permission of System administrator/IT Incharge.
- Avoid unnecessary connectivity of Internet.
- Don t panic in case system hangs. Report it to the System Administrator/IT Incharge.
- If lock and key system is available then user should ensure the security of all the parts of the computer.
- Please ensure that the Antivirus is running on the system.
- Food and drinks should not be placed near systems. Cup of Tea/ Coffee or water glass should not be on CPU or Monitor or Key Board.
- Always power off the system when cleaning it.
- Never use wet cloth for wiping the screen.

- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.
- Never stack books/ files or other materials on the CPU.
- Place the cover (If available) on the computers when you close the computers at the end of the day.

B. Policy For IT Department

3 **Departmental Policies**

- Departmental staff should be aware of the company's Information Security policies.
- Personnel in the department should have sufficient authority to accomplish IT security related duties and policies.
- Computer equipment should be situated safely and free from potential danger.
- Uninterruptible Power Supply (UPS) should be used to protect servers and workstations.
- Heating, cooling and ventilation should be properly maintained to keep the systems at the appropriate temperature and humidity.
- Department should strictly apply the company's official Password Policy on all servers and workstations to enforces strong passwords.
- There should be procedures for forgotten passwords/ Blocked accounts.
- There should be proper locking of Server room, Network racks etc.
- Accesses should be secure when offices/departments are vacant.
- Workstations and laptops should be locked down to deter theft.
- Department should have a network map/diagram of the LAN (Local Area Network).
- Department should maintain physical security standards (access control for Server Room, CCTV etc.)
- There should be a partnership with vendors (AMC of all computers, server ect.) who can help in an emergency if your equipment is damaged due to disaster.
- Backup files should be sent off-site to a physically secure location.
- Trained authorized individuals should only be allowed to install computer equipment and software.

4 Security Policy for Access Control

Policy for access control defines access to computer systems to various categories of users. Access Control standards are the rules, which an organization applies in order to control, access to its information assets. Such standards should always be appropriate to the organization s operation and security needs. The dangers of using inadequate access control standards range from inconvenience to critical loss or data corruption.

4.1 User Access

Access to all systems must be authorized by the owner of the system and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control List. Such records are to be regarded as Highly Confidential documents and safeguarded accordingly. A User Access Management Policy has been separately maintained and is to be read in conjunction with this policy.

Information Security issues to be considered, when implementing the policy, include the following:

- Lack of a managed access control procedure can result in unauthorized access to information systems thereby compromising confidentiality and potentially the integrity of the data.
- Logon screens or banners, which supply information about the system prior to successful logon, should be removed as they can assist unauthorized users to gain access.
- Allocating inappropriate privileges to inexperienced staff can result in accidental errors and processing problems.

4.2 Securing Unattended Workstations

Equipment is always to be safeguarded appropriately – especially when left unattended.

Computer equipment, which is logged on, and unattended can present a tempting target for unscrupulous staff or third parties on the premises.

Information Security issues to be considered, when implementing the policy, include the following:

- Unauthorized access of an unattended workstation can result in harmful or fraudulent entries, e.g. modification of data, fraudulent e-mail use, etc.
- Access to an unattended workstation could result in damage to the equipment, deletion of data and/or the modification of system/ configuration files.

4.3 Managing Network Access Controls

Access to the resources on the network must be strictly controlled to prevent unauthorized access, Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized. Connections to the network (including user s logon) have to be properly managed to ensure that only authorized devices / persons are connected.

Information Security issues to be considered, when implementing the policy, include the following:

- Unauthorized access to programs or applications could lead to fraudulent transactions or false entries.
- Where physical or logical access has not been controlled, users may find (and exploit) unintentional access routes to systems and network resources.
- Unauthorized external access to the network will usually result in damage, corruption and almost certain loss of confidentiality of information. Such hacks are usually motivated by malicious or fraudulent intent.

4.4 Controlling Access to Operating System Software

Access to operating system commands is to be restricted to those persons who are authorized to perform systems administration / management functions. All systems, from PCs to large servers, should be hardened to remove all unnecessary development tools and utilities.

Information Security issues to be considered, when implementing the policy include the following:

- Operating system commands could be used to disable or circumvent access control and audit log facilities, etc.

4.5 Managing Passwords

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guideline stated in the company's official Password Policy. In particular, passwords shall not be shared with any other person for any reason.

Information Security issues to be considered, when implementing the policy include the following:

- Passwords that are shared may allow unauthorized access to the information systems.
- Users who need to access multiple systems may keep a hand written note of the different passwords- e.g. in a diary- especially where they are changed frequently. However, such insecure records make an easy target for ill-intentioned persons wishing to break into the system.

4.6 Securing Against Unauthorized Physical Access

Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorization to enter such areas is to be provided with information on the potential security risks involved. Personal who work in, or have access to, high security areas may be put under pressure to reveal access codes or keys, or to breach security by performing unauthorized/illegal tasks, such as copying confidential information. The organization should provide adequate information regarding, and safeguards to prevent, such eventualities.

Information Security issues to be considered, when implementing the policy include the following:

- Biometric or other forms of physical security aspects should be used to maintain high security of data.

4.7 Restricting Access

Access controls are to be set at an appropriate level which minimizes information security risks yet also allows the organization's business activities to be carried without undue hindrance. Access to systems and their data must be restricted to ensure that information is denied to unauthorized users.

However, inappropriate restrictions could result in individual users being unable to do their job, and cause delays and errors in legitimate data processing. Similarly, excessive privilege could allow an authorized user to damage information systems and files, causing delays and errors.

Information Security issues to be considered, when implementing the policy, include the following:

- Excessive systems privileges could allow authorized users to modify (or, more likely, corrupt/destroy) the operating system configuration and application software setting with grave results.
- Lack of access restrictions could: - Allow staff and third parties to modify documents and other data file.

4.8 Monitoring System Access and Use

Access is to be logged and monitored to identify potential misuse of protected systems or information.

Information Security issues to be considered, when implementing the policy, include the following:

- Without frequent monitoring, it is difficult to assess the effectiveness of access controls. Unauthorized access can remain undetected, enabling knowledge of this security hole to be passed to persons with possible malicious or fraudulent intent. The consequences can be serious.

- Without hard evidence of a security breach, it is difficult to take disciplinary action, and it may be impossible to take legal action.

4.9 **Giving Access to Files and Documents**

Access to information and documents is to be carefully controlled, ensuring that only authorized personal may have access to sensitive information.

Information Security issues to be considered, when implementing the policy, include the following:

- With poor or inadequate access control over documents and files, information may be copied or modified by unauthorized persons, or become corrupted unintentionally or maliciously.
- Where the Access Control is seen as overly restrictive, users could be tempted to share privileged accounts (login + password) in order to access information.

4.10 **Controlling Remote User Access**

Remote access must be governed by the System administrator/ IT Incharge to provide adequate safeguards. Remote users, either tele-workers or personal on official trips etc., may need to communicate directly with their organizations systems. Such users are physically remote, and they will often be connecting through public (insecure) networks. This increases the threat of unauthorized access.

Information Security issues to be considered, when implementing the policy, include the following:

- The use of a User ID and password as the sole means of access control may provide inadequate security to enable access to the organization’s system.

4.11 **Recommendations on Accounts and Passwords**

- Passwords should be changed frequently.
- Department should have an account removal process for persons who have gone out of department.
- Department should have a method for identifying unauthorized users. Regular cross checking should be done to make sure the presence of authorize user. This can be done through verifying with other maintained data like attendance record etc.
- There should be procedures for closing accounts when an employee terminates employment or moves out of the department.

5 Security Policy for Networks

5.1 Configuring Networks

The network must be designed and configured to deliver high performance and reliability to meet the needs of the operations.

Information security issues to be considered, when implementing the policy, include the following:

- Poor network stability can threaten operations.
- Inadequate control over access to network can jeopardize the confidentiality and integrity of data.

5.2 Managing the Network

Suitably qualified staff are to manage the organization's network, and preserve its integrity in collaboration with the individual system owners.

Information security issues to be considered, when implementing the policy, include the following:

- Inappropriate control over access to the network will threaten the confidentiality and integrity of data.
- Inadequate capacity can make efficient operation difficult or impossible.

5.3 Accessing Network Remotely

Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated and privileges are restricted.

Information security issues to be considered, when implementing the policy, include the following:

- Inadequate Internet Security safeguards can allow unauthorized access to the network, with potentially disastrous consequences.

5.4 Defending Network Information from Malicious Attack

System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion. The measures should be taken to defend computer hardware against physical damage and software from unauthorized usage.

Information security issues to be considered, when implementing the policy, include the following:

- Hardware can be physically damaged, through a malicious act, perhaps necessitating a system close down or delayed operations.
- Unauthorized and inappropriate use of software can lead to malicious and/or fraudulent amendment of data.

5.5 Recommendations on Network and Configuration Security

- Department should have an inventory of devices attached to the network.
- Department should have network documentation to assist problem resolution of a computer or network device.
- Department should have the ability to continue to function in the event of a wide area network failure (Secondary Internet connectivity).
- Department should have a network diagram.
- End users should be prevented from downloading and/or installing software.
- Contents of system should be protected from unauthorized access, modification, and/or deletion.
- Trusted workstations should be secured if used for other purposes.
- Trusted workstations should be required to have complex passwords.
- Administrator account, and any equivalent accounts, on all workstations should be limited to the office technical support person.
- File sharing should be properly permitted and secured on any workstation in the department.

5.6 **LAN Security**

This network policy addresses the following specific issues:

- Data confidentiality, integrity, and availability over the network.
- Frequency and retention periods for network backup
- Authorized use of network resources
- Network Hardware maintenance
- Problem logging/reporting and monitoring
- User responsibilities for security, workstation maintenance, and backup of data files
- Prevention and detection of network viruses

6 Security Policy For Operating System

Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than with processing work for users are known as Operating System. Computers can operate without application software, but cannot run without an Operating System.
Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to. The operating system of desktop systems within departments will generally run without substantial interference. However, for servers, mini-computers and mainframes, especially those running mature Operating Systems (OS), day to day housekeeping is usually required.

Information security issues to be considered, when implementing the policy include the following:

- Where an upgraded operating system fail to perform as expected, this can result in a loss of stability or even the total failure of some systems.
- Where housekeeping and routine support are informal or incident led, weaknesses in the security safeguards can go undetected and offer the potential for fraud or malicious damage.

7 Security Policy for Software

Only designated staff may access operational and accounting software (Tally ERP). Unauthorized use of software can cause disruption to systems or fraud against the department. Controlling taking printouts, reports, electronic or hard copy from the application. Beware of old versions of programs being confused with the latest version, resulting either in the loss of recent enhancement or a failure of other systems, which depend on recent features.

8 Backup Policies

Departments should also try to set infrastructure for taking backup over the network. Remote Backup Services could also be taken for backup and recover important data using a secure and trusted server.

Departments should maintain backup infrastructure, including upgrading the hardware and software as needed. The official Backup Policy of the company should be followed properly.

Backup and Recovery & Incident Management Planning

- Files should be kept on-site in a secure location.
- Critical files should be regularly backed up.
- Backup files should be periodically restored as a test to verify they are usable.
- There must be a contingency plan to perform critical processing in the event that on-site workstations are unavailable (Referred to as ‘Incident’).
- There should be a plan to continue departmental working in the event when the central systems are down for an extended period.
- Contingency plan should be periodically tested to verify that it could be followed to resume critical processing.
- Critical data should be stored on a department server to protect from compromise

Prevention and Detection of Viruses

- Proper Antivirus solution (Including e-mail security, Firewall, antimalware, Internet use control facilities) must be purchased and installed on all workstations.
- The scheduler for the network’s antivirus software will be set to scan memory and all files on the network on a daily basis.
- Warning messages will be carefully evaluated and corrective action taken.
- If a virus is discovered, the origin of the virus should be investigated.
- The origin of most viruses is "pirated" software or shareware or public domain software downloaded from a bulletin board, on-line service, or the Internet. All software will be scanned for viruses before being loaded on a PC.
- The network administrator will install anti-virus software updates as they become available.
- If the origin of the virus is due to negligence or policy violation on the part of an employee, that employee will be subject to appropriate disciplinary action, which may include termination.

Usage of Anti-Virus Programs

- Always see that the latest antiviral software version available. If software updates are available, check them for "freshness".

- If a virus is found in some newly arrived file(s) and has not infiltrated the system yet, there is no reason to worry: just kill the file (or remove the virus with antivirus

program) and keep on working. If virus is found in several files at once or in the boot sector, the problem becomes more serious, but still it can be resolved.

- In the case of file-virus detection, if the computer is connected to a network, disconnect it from the network and inform the system administrator. If the virus has not yet infiltrated the network, this will protect the server and other workstations from virus attack.

- If the virus has already infected the server, disconnection from the network will not stop the virus from infiltrating into the computer again after its treatment. Reconnection to the network must be done only after all the servers and workstations have been cured.

- If a boot virus has been found, don t disconnects the computer from the network; viruses of this kind do not spread over it (except file-boot viruses).

- If the computer is infected with a macro-virus, then instead of disconnecting from network, it is enough to make sure that the corresponding editor (Word/Excel) is inactive on any computer.

- If a file or boot virus has been detected, make sure that either the virus is nonresident, or the resident part of it has been disarmed: when started, some (but not all) anti-viruses automatically disable resident viruses in memory.

Job Description of the System Administrator/ IT Manager

The duties of the System administrator shall include monitoring network efficiency (response time, utilization of disk space, etc.); troubleshooting network problems, monitoring environmental conditions; backing up the system, shared data files, and application programs on the file server; and preventing and detecting computer viruses.

Other duties include ensuring that network security features in the NOS are implemented, recommending software and hardware acquisitions needed to maintain operating efficiency, contacting network maintenance contractors regarding technical problems, deleting and adding users, coordinating the installation of new network hardware and software, and maintaining an inventory of network hardware and software.

Compliance with Policy

The Heads of the department are responsible for ensuring that their employees comply with the policy. The IT Manager is responsible for implementing the policy.