# INFORMATION TECHNOLOGY POLICY

# OF

# ORRISH FINANCE PRIVATE LIMITED

## RBI REGISTERED NBFC

## REGISTRATION NO. B-03.00208

## 1. INTRODUCTION AND POLICY STATEMENT

1.1 This document sets out the Information Technology (IT) Policy for the protection of IT network, hardware including portable media, system and application software, communication components, documentation, physical environment and other information assets.

1.2 The equipment covered by this policy includes:

- Network Infrastructure – The equipment housed internally to provide the IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems and devices.
- Desktops – Personal Computers (PCs) provided to staff in the course of carrying out their duties
- Media/Portable Media – Electronic Storage Devices such as pen drives/hard drives provided to staff in the course of carrying out their duties
- External Communications Infrastructure – Equipment used to connect to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines and all related equipment and services.

1.3 The objective of this policy is to ensure: -

- the confidentiality of data and information assets are protected against unauthorised disclosure and incidents are promptly reported
- integrity of data and information assets so that they are protected from unauthorised or accidental modification
- the availability and accessibility of IT systems as and when required by staff

## 2. RESPONSIBILITIES

2.1. Defining responsibilities ensures that all users of IT systems are aware of their responsibilities to minimise the risks to IT security and operations.

2.2. The Business Planning department is responsible for ensuring that:

- electronic filing systems and documentation are well maintained for all
- no unauthorised staff are allowed to access any IT systems in any location, as such access could compromise data integrity;
- named individuals are given authority to administrate specific computer systems according to their job function and role following the principle of least privilege;
- all current and new users are instructed in their security responsibilities;

- Procedures are implemented to minimise exposure to fraud, theft or disruption of its systems; these include segregation of duties, dual control and staff rotation in critical susceptible areas.
- critical job functions to ensure continuity;

2.3. The Human Resources department is responsible for ensuring that:

- all staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment, and any contactors, temporary staff
- new staff are given basic user training in IT Security as part of their induction.

2.4. Users who do not have administration rights over their issued equipment_are responsible for ensuring that:

- No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IT equipment they are issued together with confidential data stored on it when taken outside secure offices.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimise the risks and impacts should a security breach or loss of that equipment occur.

## 3. SECURITY

- Technical security measures will be put in place to protect systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.
- Email and internet use will be governed in accordance with the Email and Internet policy.
- All IT equipment, including virtual systems, will be uniquely identified and recorded.
- Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.
- Records of all faults and suspected faults will be maintained.

## 4. PHYSICAL ACCESS CONTROLS

- The server/communications rooms and store rooms for IT equipment will be locked at all times and the keys/codes held securely by the IT department.
- No remote access to systems will be given to third parties at any time unless specific authorisation is received.

## 5. DISPOSAL/REALLOCATION OF EQUIPMENT

- Equipment allocated to an individual user must not under any circumstances be reallocated within a department and must always be returned to IT for reallocation to ensure correct management of sensitive data.

## 6. SECURITY INCIDENT INVESTIGATION AND REPORTING

- The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach.
- A security incident is an event that may result in:
  - degraded system integrity
  - loss of system availability
  - disclosure of confidential information
  - disruption of activity
  - financial loss
  - legal action
  - unauthorised access to applications
  - loss of data
- All users must report actual security breaches, or any concerns or suspicions about security breaches, as soon as they arise.
- All actual security incidents will be formally logged, categorised by severity and actions recorded by the IT department, and reported to the Directors.

## 7. BACK-UP OF DATA WITH PERIODIC TESTING

- In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility of backing up the information located in shared access servers is the network administrators.
- Restoration testing on a time to time basis is done as both hard disks and magnetic tapes are prone to errors. As general rule, daily full backup happens for all critical business application and complete weekly full backup is carried out including file servers/old data kept on servers.

## 8. REVIEW

- This policy will be monitored by the IT department to ensure it is fit for purpose and reviewed every 3 years.