Information Transfer / Handling Policy

for

Tierney's Office Automation Ltd.

1. Introduction

Tierney's Office Automation Ltd. and Tierney's Office Automation Ltd.'s employees have an inherent responsibility to protect the information assets of the company, as well as confidential client data and intellectual capital owned by the company. These critical assets must be safeguarded to mitigate any potential impacts to Tierney's Office Automation Ltd. and to Tierney's Office Automation Ltd.'s clients. Information Security at Tierney's Office Automation Ltd. is, therefore, a critical business function that is incorporated into all aspects of Tierney's Office Automation Ltd.'s business practices and operations.

To achieve this objective, policies, procedures, and standards, have been created to ensure secure business practices are in place at Tierney's Office Automation Ltd. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

Tierney's Office Automation Ltd. is subject to numerous laws, regulations and contractual obligations, which if not complied with, could potentially result in fines, audits, loss of client confidence, and direct financial impacts to the company. Compliance with all applicable regulations is the responsibility of every employee at Tierney's Office Automation Ltd.

2. Asset Classification and Control

The purpose of this policy is to determine the protective controls associated with each Tierney's Office Automation Ltd.'s information asset and to provide a foundation for all employees (and contractors, third parties, etc. who deal with information assets) to understand the security and handling of such assets.

Tierney's Office Automation Ltd.'s data classification system has been designed to support access to information based on the need to know so that information will be protected from unauthorised disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, Tierney's Office Automation Ltd. unduly risks loss of

client relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

This data classification policy is applicable to all information in Tierney's Office Automation Ltd.'s possession, including electronic data, printed reports, and backup media.

Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, all employees are expected to apply and extend these concepts to fit the needs of day-to-day operations.

2.1 Classification Guidelines

Asset classification is the process of assigning value to data in order to organise it according to its sensitivity to loss or disclosure. All information assets shall be classified, using a company-wide asset classification system. All data, regardless of its classification, will be protected from unauthorised alteration; this policy provides guidance on the proper handling of data.

The classification system will allow that classifications of information assets may change over time.

2.1.1 Classifying Information

This policy requires that all information assets be classified and labelled in a manner that allows the asset to be readily identified to determine handling and protection level for that asset.

Care will be taken when interpreting the classification systems from other organisations as their classification systems may have different parameters. Information assets shall be assigned a sensitivity classification by the asset information owner or their nominees, in accordance with the following classification definitions:

- **Confidential:** Sensitive information requiring the highest degree of protection. Access to this information shall be tightly restricted based on the concept of need-to-know. Disclosure requires the information owner's approval and, in the case of third parties, a signed confidentiality agreement. If this information were to be compromised, there could be serious negative financial, legal, or public image impacts to Tierney's Office Automation Ltd. or Tierney's Office Automation Ltd. clients. Examples include subscriber details, Financial / accounts / payroll records, board meeting minutes, client passwords etc.
- **Public:** Information that requires no special protection or rules of use. This information is suitable for public dissemination. Examples include press releases, marketing brochures, etc.

Senior Management is responsible for maintaining this policy and ensuring the infrastructure exists to support this policy.

2.1.2 Handling and Protection Rules

Each asset classification shall have handling and protection rules. These rules must cover any media the assets may reside in at any time.

All computer-resident confidential information shall be protected via access controls to ensure that it is not improperly disclosed, modified, deleted or otherwise rendered unavailable.

Employees are prohibited from recording confidential information with tape recorders, digital/analogue recording devices, etc., without the consent of the Senior Management. This includes the use of camera equipment (of any kind).

Unless it has specifically been designated as "Public", all Tierney's Office Automation Ltd.'s internal information shall be assumed to be confidential and shall be protected from disclosure to unauthorised third parties.

No confidential information of Tierney's Office Automation Ltd. or of any third party shall be disclosed to the public or any unauthorised third party without the prior approval of Tierney's Office Automation Ltd.'s Senior Management.

Access to every office and work area containing confidential information shall be restricted, and employees shall take all reasonable steps to protect confidential information under their control from inadvertent disclosure.

Handling and protection rules must include all parts of an asset's life cycle, from creation/installation through use and finally to destruction/disposal. Sensitive information or systems must be appropriately disposed of when no longer needed.

2.1.3 Information Labelling and Handling

It is important that an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by Tierney's Office Automation Ltd. These procedures must, where possible, cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity;

- Copying
- Storage
- Transmission by post, fax, and electronic mail
- Destruction

Where feasible, all printed, handwritten, or other paper manifestations of confidential information should have a clearly evident sensitivity label within the footer of each page or a watermark that indicates the sensitivity classification. However, it is recognised that due to the business profile of Tierney's Office Automation Ltd. is may be necessary not to have such markings on physical paper so as not to highlight the importance of the material

3. Procedures

3.1 Information Exchange

All information exchange of Confidential data with Third Parties will require a signed Non-Disclosure Agreement between all parties.

3.2 Paper / Physical Documents or Media

It is Tierney's Office Automation Ltd. Policy to ensure all physical information in transit that has been deemed Confidential will be dealt with in one of the following ways.

- Hand Delivered by approved member of Tierney's Office Automation Ltd. Staff.
- Delivered by Registered Post.
- Delivered by approved Courier.

Paper documents should be clearly marked as Confidential

Physical Media will be stored on an encrypted device.

Transit of all physical media will be logged in Physical Media Audit Log.

3.3 Electronic Media

It is Tierney's Office Automation Ltd. Policy to ensure all electronic information in transit that has been deemed Confidential will be dealt with in the following way.

- Email - all confidential emails are encrypted using approved encryption software.
- USB Keys/External Drives – all USB keys that contain confidential information will be encrypted.

Transit of all confidential electronic media will be logged in Electronic Media Audit Log.

3.4 Data Transfer

Data transfer of any confidential information through remote access software must be authorised by the data owner via email.
Confirmation Email must be stored in the Ticket associated with the work being carried out.
Process:

- Request for authorisation is sent directly from RMM system.
- Data owner replies with approval.

3.5 Cloud Backups

All Cloud backups are encrypted in transit and are stored on encrypted servers.

3.6 Passwords via Email

Passwords will not be sent in body of email. Password Encryption tool will be used to send passwords and other confidential information. Passwords are not to be stored in tickets.

3.7 Information Exchange Audit Logs

Audit logs for both Physical Media transit and Electronic Media transit will be maintained.

4. Information Retention

Information shall not be retained any longer than the business requires it to be retained and in accordance with data protection, privacy, legal, and other regulatory requirements. This reduces the window of time that data can potentially be available for misuse. Controls should be implemented to delete data that exceeds required retention time.

4.1 Paper Disposal Procedure

It is Tierney's Office Automation's Policy to destroy/shred all confidential data once no longer required.
Where possible documents will be shredded on shredders in office.
For large volumes:

- Tierney's will engage a third-party company when needed to dispose of large amounts of paper who will provide secure on-site destruction in a specialist shredding vehicle, on-premise – all material is destroyed before the vehicle leaves site and EN15713 accredited secure chain of custody with Certificate of Destruction for records/audit trail.
  This process will be scheduled to take place twice annually depending on volume. Register and copy of Certificates maintained.
- All documents to be shredded will be stored in secure storage.

Accounts records will be held for 7 years as required for Auditing purposes.

4.2 Physical Storage Disposal Procedure

It is Tierney's Office Automation's policy to remove any physical storage from devices removed from customers site for disposal. This mainly includes hard drives but may include USB drives/keys
Storage is held for 3 months and destroyed on 4th month – unless immediate destruction requested.
All hardware disposed of is sent for recycling - WEEE Registered.
CD's can be shredded using on-site shredder.

4.3 Client Data Backup – Temporary Storage

As part of our repair / support services we may be required to copy data to temporary storage. Including NAS / USB / External Hard Drives.
Data copied to temporary storage will only be held for duration of the repair. Then fully deleted.
Once a month Workshop NAS will be cleaned using low-level format.
Drives used by On-site Engineers are encrypted.