INFORMATION SECURITY POLICY

TEXTILE RECYCLING INTERNATIONAL

Return, Renew, Reuse, Recycle

1. INTRODUCTION & PURPOSE

Information is a vitally important TRI Group asset, and we all have a responsibility to make sure that this information is kept safe and used appropriately. Without due care, personal, research or company information can be misplaced or leaked, which is a significant issue. Outwith this, there is the increasing difficulty of having to protect data against proactive and sophisticated attempts at theft.

Therefore, TRI Group has adopted an Information Security Policy (ISP) that complies with stringent legal requirements and provides the necessary assurance that data held and processed by the TRI Group is treated with the highest appropriate standards to keep it safe.

This ISP is a key component of TRI Group's overall business management system and provides a framework for more detailed information security documentation including system level security policies, security guidance and protocols or procedures. This policy applies to TRI Group and all Group Companies.

2. POLICY AIM

The aim of this policy is to set out the rules governing the secure management of our information assets by ensuring that all members of the team:

- Are aware of and fully comply with the relevant legislation as described in this policy.
- Creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day to day business.
- And protecting information assets under the control of the organisation.

3. SCOPE

This policy applies to all information, information systems, networks, applications, locations and users of TRI Group equipment, or equipment supplied under contract to it, as well as any hardware such as laptops, mobile devices, tablets and more.

4. RESPONSIBILITIES

Ultimate responsibility for information security rests with the Chief Financial Officer of TRI Group. They will be responsible for managing and implementing the policy and related procedures.

Team leaders are responsible for ensuring that their permanent and temporary team members and contractors are aware of:

- The information security policies applicable in their work areas
- Their individual responsibilities for information security
- How to access advice on information security matters

All team members and contractors shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action, including dismissal.

Team leaders shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of the team shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

Contracts with external parties that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the team members or sub-contractors of the external organisation shall comply with all appropriate security policies.

5. LEGISLATION

TRI Group is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of TRI Group, who may be held personally accountable for any breaches of information security for which they are responsible.

The requirement to comply with this legislation shall be devolved to employees and agents of TRI Group, who may be held personally accountable for any breaches of information security for which they are responsible.

6. POLICY FRAMEWORK

6.1 Personnel Security

6.1.1 Contracts of Employment

- Team members security requirements shall be addressed at the recruitment stage, and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of team members shall be included within appropriate job definitions.
- All access rights shall be removed immediately on termination of the contract.
- All associated accounts shall be deleted or disabled on termination of the contract.
- All company assets must be returned immediately upon termination of the contract.

6.1.2 Intellectual Property Rights

The organisation shall ensure that all software, applications and operating systems are properly licensed in accordance with the publisher's recommendations.

6.2 Asset Management

Company devices include any computer, laptop, tablet or mobile phone that can access company data. These devices meet the following criteria:

- All obsolete or not used software must be deleted or disabled.
- Have anti-malware installed.
- Not be jailbroken.
- Only have apps installed from their official application store.

6.3. Bring Your Own Device Policy

In certain circumstances, the Company may allow devices that have not been provided by the Company to access Company systems in order to allow working from home. This must be arranged in advance of using these devices for work purposes and must be done through the Company's preferred Remote Desktop Software.

Any device used for Company purposes must also adhere to the following constraints:

- The device must be supported by the manufacturer.
- All security updates must be installed within 14 days of release.
- The device must automatically lock when not in use.
- The device must have at least an 8-character password (or pin code), using biometrics or multi-factor authentication if available.
- The device must be encrypted.
- An anti-malware application must be installed.
- Unused applications must be uninstalled.
- Where applicable, applications must only be installed from the manufacturers respective store.
- Rooting or Jailbreaking devices is not permitted.
- If the device is lost or stolen, it must be reported to the Company promptly.

7. ACCESS MANAGEMENT

- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.
- Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.
- Team members can only access laptops, computers and servers including applications they contain, by entering a unique username and password.
- Team members shall only have admin privileges if they have a bona-fine case. The Head of IT shall have final review on whether someone should be granted administrator privileges.
- Administrator accounts shall not be used for accessing emails or for web browsing.
- Administrator accounts shall be regularly reviewed by the Head of IT, to assess if the individuals still have a business need for privileged access.
- All administrator accounts shall enable two-factor authentication for access to all admin accounts on all accounts, applications and machines.
- The boundary between the business systems and the Internet or other non-trusted networks shall be protected by a firewall, which shall be configured to meet the threat landscape and be regularly monitored.

- All administrative accounts must have a strong password. To achieve a strong password, the following checks must be met:
- At least eight characters in length
- At least one capitalised letter
- At least one number
- At least one special character (!@£$%&*)
- All user and administrator accounts should have their default passwords changed to a strong password.

8. FURTHER INFORMATION

Further information and advice on this policy can be obtained from the Head of IT, it@t-r-i.co.uk, 01902 357 300.

Comments and suggestions to improve security are always welcome.