Section		**Version**	1	FINAL
Distribution	CTI	**Document Type:**	Policy	
Responsible	Andrew Lewis	**Created**	08 February 2022	
Author	Paul Cavicchia	**Revision Due**	30 June 2024	
File Path				

EMAIL SECURITY/ACCEPTABLE USE POLICY

Policies & Procedures

Version	Date	Author	Approved by	Review Due	Summary of Changes
1	20/10/2020	Karen Prelovsky	Andrew Lewis	30/06/2024	Initial Version
2	16/04/2021	Karen Prelovsky	Andrew Lewis		Added removal of media

Approval

Name	Position	Signature	Date
Andrew Lewis	CEO		16 April 2021

Policy Statement

To meet the organisation's business objectives and ensure acceptable use of its information systems and networks, **RTO** shall adopt and follow well-defined and time-tested plans and procedures and follow guidelines to exercise judgement regarding use of organizational resources. **RTO** is deploying IT-enabled services at various internal divisions for managing its business activities. Presently **RTO** depends on the following IT-enabled processes for managing its business activities:

- E-Publishing;
- Financial Accounting Package (FAP);
- Procurement Monitoring System (PMS);
- Release Order (RO) Module
- Business Operating System (BOS)

The following processes are in conceptualization / development stage will be implemented in future:

- CRM

The acceptable use policy and guidelines shall be communicated to and understood by all the employees of **RTO**. The acceptable use policy and guidelines shall be available to the CEO, GMs, Directors and Managers

1. Purpose

The purpose of this policy is to outline the acceptable use of IT assets at **RTO**. These rules are in place to protect the employees and the organization. Inappropriate use exposes **RTO** to risks including virus attacks, compromise of network systems and services, and legal issues.

2. Scope

2.1. Employees

This policy applies to all **CTI** Employees, Contractors, and Third-Party Employees, who have access to IT assets of **RTO** and may be bound by contractual agreements.

2.2. IT Assets

The policy is applicable to all Hardware assets, Software assets, Network assets, and Utilities, including Air Conditioner, Power and Telecommunication services (that serve IT assets of **RTO**). Equipment owned by third parties, but in the custody of **RTO**, will also be covered under the scope.

2.3. Documentation

The documentation shall consist of Acceptable Use Policy, guidelines and policies & procedures for acceptable use of each service.

2.4. Document Control

The Acceptable Use Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

2.5. Records

Records being generated as part of the Acceptable Use Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

2.6. Distribution and Maintenance

The Acceptable Use Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the system administrators.

2.7. Removable Media

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks not provided by RTO.

3. Privacy

The Acceptable Use Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

4. Responsibility

1. The Acceptable Use Policy shall be implemented by the management.
2. Management is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.
3. SimpleBiz is responsible for building, configuring, operating and maintaining the corporate email facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy.
4. IT Help Desk (SimpleBiz) is responsible for assisting users with secure use of email facilities and acts as a focal point for reporting email security incidents.
5. All relevant employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.
6. Internal Audit is authorized to assess compliance with this and other corporate policies at any time.

5. Policy

5.1. General Use and Ownership

- While the security administration of **RTO** desires to provide a reasonable level of privacy, users should be aware that the data they create on corporate systems remains the property of **RTO**. Because of the need to protect the IT assets of **RTO**, management cannot guarantee the confidentiality of personal information stored on any IT asset belonging to **RTO**.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet and Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- It is recommended that any information that users consider sensitive or vulnerable be protected.
- For IT system security and network maintenance purposes, authorized individuals within **RTO** shall monitor equipment, systems and network traffic at any time, as per orders issued by the competent authority.

- **RTO** reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- **Removal Media**: CTI staff may use removable media in their work computers. Sensitive information should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information. When sensitive information is stored on removable media, it must be encrypted in accordance with the instructions from SimpleBiz. Exceptions to this policy may be requested on a case-by-case basis by petition to the CEO.

5.2. Security and Proprietary Information

- The user interface for information contained on Internet and Intranet-related systems shall be classified accordingly. Employees shall take all necessary steps to prevent unauthorized access to this information.
- Authorized users shall be responsible for the security of their passwords and accounts.
- Encryption of information, if used, shall be in compliance with instructions of SimpleBiz.
- Information contained on portable computers shall be protected.
- Users and employees shall use suitable procedures and guidelines for acceptable use of E-mail and internet resources.

5.3. Unacceptable Use

Under no circumstances is an employee of **RTO** authorized to engage in any activity that is illegal under national or international law while utilizing RTO's-owned resources. The guidelines for Acceptable Use can be referred for a list of activities which fall under the category of unacceptable use.

5.4. Email Security

1. Do not use email:
    - To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;
    - To create, send, forward or store emails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public i.e. sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
    - To commit the organization to a third party for example through purchase or sales contracts, job offers or price quotations, unless you are explicitly authorized by management to do so (principally staff within the Executive Team). Do not interfere with or remove the standard corporate email disclaimer automatically appended to outbound emails;
    - For private or charity work unconnected with the organization's legitimate business;
    - In ways that could be interpreted as representing or being official public statements on behalf of the organization, unless you are a spokesperson explicitly authorized by management to make such statements;
    - To send a message from anyone else's account or in their name (including the use of false 'from:' addresses). If authorized by the manager, a secretary may send email on the manager's behalf but should sign the email in their own name per pro ('for and on behalf of') the manager;
    - To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, colour, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or

patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;

- For any other illegal, unethical, or unauthorized purpose.

2. Apply your professional discretion when using email, for example abiding by the generally accepted rules of email etiquette. Review emails carefully before sending, especially formal communications with external parties.
3. Do not unnecessarily disclose potentially sensitive information in “out of office” messages.
4. Emails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the scanning process is not 100% effective (e.g. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavoury emails are sometimes delivered to users. Delete such emails or report them as security incidents to IT Help Desk in the normal way.
5. Except when specifically authorized by management or where necessary for IT system administration purposes, employees must not intercept, divert, modify, delete, save or disclose emails.
6. Limited personal use of the corporate email systems is permitted at the discretion of management provided always that it is incidental and occasional and does not interfere with business. You should have no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.
7. Do not use Gmail, Hotmail, Yahoo or similar external/third-party email services (commonly known as “web-mail”) for business purposes. Do not forward or auto-forward corporate email to external/third party email systems. [You may access your own web-mail via corporate IT facilities at management discretion provided that such personal use is strictly limited and is not considered private.
8. E-mail shall only be used for business purposes, using terms, which are consistent with other forms of business communication. E-mail guidelines are intended to help users make the best use of the electronic mail facilities at their disposal. When using the organization’s electronic mail facilities, users should comply with the E-mail guidelines.

6. Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy

This Policy shall be governed by the laws of Australia and the parties submit to the exclusive jurisdiction of the Courts of Australia.