Use of Company Technology Assets Policy and Procedure

Revision history

Rev.	Issued	Description	Prepared	Approved by Board
1.6	29/7/25	Annual Review	Fitzgerald	14/8/25
1.5	29/7/24	Annual Review	Fitzgerald	15/8/24
1.4	18/8/23	Annual Review	Fitzgerald	24/8/23
1.3	1/8/22	Annual Review	Donovan	1/8/22
1.2	28/1/20	Annual Review	Robson	28/1/20
1.1	31/1/19	Annual Review	Robson	31/1/19
1.0	21/12/17	Review	Robson	21/12/17
0	23/7/15	Policy created	Robson	23/7/15

Sipa Resources Limited Use of Company Technology Assets

1 Purpose

Sipa Resources Limited (Company) and its subsidiaries (collectively, Sipa) utilise a variety of information technology systems, including electronic mail, networks, internet, and phones, (collectively, Technology Assets) to support its business goals. The Technology Assets are Sipa's property and are to be used primarily for business purposes. Incidental appropriate personal use is permitted provided it does not interfere with your business activity, is in compliance with this policy, and complies with the Sipa Code of Conduct. Inappropriate use is strictly prohibited. You should not expect that any of your e-mail or internet communications are private.

The following guidelines should be observed at all times.

2 Requirements of use of Technology Assets

Employees acknowledge that Sipa has various systems in place designed to ensure security of its confidential information. To assist in the protection of this confirmation, the following guidelines should be observed at all times.

(a) Employees must use their own username/login code and/or password when accessing the Technology Assets. Guests may be permitted only upon approval by the **Information Technology** personnel or Managing Director.

(b) Employees should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.

(c) Passwords should be changed from time to time with obvious choices such as birthdates, names being avoided.

(d) Technology Assets should be logged off when not in use and always when the employee has left the office.

(e) Circumventing or attempting to circumvent normal resource limits, logon procedures and security regulations is strictly prohibited.

3 Copying or Amending Software and other Copyright works

(a) Software and documentation licensed to the Company may only be used for the purpose permitted in the licence agreement and must not be copied, distributed or used except in accordance with the licence agreement or the Copyright Act, 1968, e.g. to make a backup copy.

(b) To ensure the Company complies with each licence and does not breach the Copyright Act, 1968, each employee must observe the following rules:

  (i) An employee must not and must not attempt to copy, reproduce, transmit to another computer system, translate, modify or adapt in any manner or form or in or on any medium the whole or any part of any computer software (other than a backup copy) or documentation;

  (ii) An employee must not attempt to load or install any computer program onto a computer or computer system, without the express permission of the **Information Technology** personnel.

4 Electronic Mail

(a) Electronic mail sent should be business related and thus language and tone must be appropriate to the business purpose.

(b) Extreme care should be taken when sending something humorous, as what seems humorous to one person may be offensive to another, particularly given the cultural differences operating in emerging markets. If there is any doubt, do not send the email.

(c) Email is not to be used by employees for private commercial uses or personal monetary gain. No personal business is to be conducted via Sipa's email system.

(d) Occasional use of email and the Internet for personal domestic purposes is allowed on the condition that its use is governed by this policy (including the Company's right to monitor email and Internet usage) and that Sipa undertakes no liability for any loss or harm, in connection with the personal email or Internet usage, incurred by any party, including an employee.

5 Viruses

(a) Computer software, either programs or data attachments (e.g. documents, spreadsheets, MP3 files, etc.) may contain a "computer virus".

(b) To avoid the introduction of viruses:

(i) Employees must not load or install any computer software onto a computer or computer system without the prior written consent of **Information Technology** personnel.

(ii) Each employee must notify **Information Technology** personnel as soon as they become aware of a computer virus.

(c) Employees must not delete or disable any of the anti-virus software or software updates from PC's.

(d) **Extreme care should be taken when receiving email attachments**, or downloading data from the Internet, especially from unknown sources, as they may contain computer viruses. The virus protection is only as up to date as the last detected and documented virus. If an employee does not know the sender of e-mail, he/she should not open the attachment. If an employee does not have reasonable grounds to believe that a website is reputable, he/she should not access the site, and in particular shall not download data from the site. All reasonable care should be taken to ascertain the sender is genuine. An example spoof email is at Appendix 1.

6 Usage Prohibitions

(a) Employees are prohibited from sending, receiving, downloading, displaying, printing or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, discriminatory, political, intimidating, abusive, defamatory or otherwise unlawful.

(b) Employees are prohibited from downloading copyright works that typically have commercial value and are offered for sale by the copyright owner, such as files containing music or film, if such files are being offered for downloading for free, or copying otherwise does not appear to be authorised by the copyright owner. In addition such files are not to be stored on the business assets of the Company.

(c) The Company's internal business records and documents are confidential information and must not be sent to unauthorised persons.

7 Monitoring of Information Technology Usage

(a) The Company reserves the right to enter, search, and monitor Company **Technology Assets** including an employee's email, voicemail, internet use, file storage, etc., without advance notice and consistent with applicable laws. Staff are advised that e-mail deleted from an employee's inbox or outbox will still be recorded on the Company's server and be able to be monitored by Information Services personnel and senior management if required.

(b) Any personal information transmitted using the Company's information technology systems shall not be absolutely confidential. The Company may disclose it to third parties if legally compelled to do so or the Company considers disclosure to be in the Company's best interest.

8 Email Etiquette, Security and Legal Considerations

(a) Extreme care should be taken when sending attachments, as, should it contain a virus, Sipa could be held legally liable for the damages.

(b) Exercise care when forwarding email/s from other sources, as even though you may not be the originating author; you could still be held legally liable for the contents of the email. For example, it is a defamatory act to re-send a defamatory statement about someone else, even if you were not the original author of it.

(c) As your employer, Sipa might be held legally liable to other persons for wrongful acts committed by you in the workplace. If the Company incurs liability to others because of an employee's breach of this policy, the employee will be obliged to indemnify the Company.

(d) Electronic mails are legal documents and can be required to be produced as evidence in legal proceedings. Therefore, care should be exercised never to make any statement which may embarrass you or the Company, if made public.

9 Use of Sipa Intellectual Property on Artificial Intelligence Platforms

(a) **Purpose**: This clause outlines the rules and guidelines for using Artificial Intelligence ("AI") platforms and handling Company-specific information to ensure data security and compliance with company policies.

(b) **Scope**: This clause applies to all employees, contractors, and third-party vendors who have access to Company Technology Assets and use AI in their work.

(c) **Guidelines**:

(i) **Confidentiality**: Employees must not input, share, or disclose any confidential or sensitive Company information to an AI platform. This includes, but is not limited to, proprietary data, trade secrets, financial information, and personal employee information.
(ii) **Data Security**: Employees must ensure that any data shared with AI is anonymized and does not contain any identifiable Company-specific information, unless the information is already publicly available.
(iii) **Compliance**: Employees must comply with all relevant Company policies, including data protection and privacy policies, when using AI.
(iv) **Monitoring and Reporting**: The use of AI will be monitored to ensure compliance with this policy. Any breaches or suspected breaches must be reported immediately to the IT department or the designated compliance officer.

(d) **Enforcement**: Violations of this clause may result in disciplinary action, up to and including termination of employment, in accordance with Company policies.

10 Reporting non-compliance with this Policy

(a) Any employee who becomes aware of a possible breach of this Code should report the breach to their manager, or the Company Secretary. Such reports will be treated confidentially to the extent possible consistent with Sipa's obligation to deal with the matter openly and according to applicable laws.

(b) No employee will be subject to retaliation or disadvantage for reporting in good faith a possible violation of this Code.

11 Consequences for non-compliance with this Code

Adherence to this Code and Sipa's policies is a condition of employment at Sipa. Breaches of the Code may be subject to disciplinary action including termination of employment, if appropriate and also made be subject to Civil or Criminal actions.

Appendix 1 – Example Spoof Email