1. Acceptable Use Policy

The purpose of the policy is to establish rules for the acceptable use of information and communications technology at Visascape Pty ltd. This policy is in place to protect employees and the Visascape Pty ltd business. Inappropriate use exposes the organization to risks including virus attacks, compromise of network systems and services, and legal liability.

The principles contained in this policy apply to computing devices and services provided by Visascape Pty ltd for business use. All personnel working for or on behalf of Visascape Pty ltd are required to comply with this policy.

This policy is primarily concerned with the following:

1. Computers.
2. Internet.
3. E-mail.
4. Instant messaging.
5. Information protection.
6. Password use.
7. Clear desk and screen.
8. Handling and use of removable media.
9. Security equipment was taken outside Visascape Pty ltd.

However, the principles are equally applicable to the use of any other computing and communication methods.

This policy applies to the use of information, electronic and computing devices, property or resource at any time, whether during or outside office hours and includes the use of remote access facilities. Further, this policy also applies to the use of personal devices accessing the Visascape Pty ltd resources.

The requirements and expectations outlined in this policy apply equally to:

1. All fulltime, part time, temporary or casual Visascape Pty ltd employees.
2. All contractors engaged by Visascape Pty ltd.
3. All suppliers providing services to Visascape Pty ltd.

Responsibilities

Role	Responsibilities
Managing Director	Reviews and approves this policy.
Chief Operating Officer	The establishment and support of systems to provide and manage user access. The establishment

	and maintenance of monitoring and compliance systems and processes to ensure that the supporting mechanisms are functioning effectively. The granting of exemptions to this policy.
Business Managers	The proper induction of new users, including non-permanent personnel, and to ensure that all users in their area are made aware of this policy and the consequences of breaching it. Regularly reviewing the compliance of information processing within their area of responsibility.
Employees, contractors, volunteers, and suppliers.	Responsible for compliance with this policy, and any supporting policies, standards, and procedures.
All personnel	Reporting security incidents and any identified weaknesses.

Key Principles

Unless otherwise authorised in this policy, Visascape Pty ltd systems and facilities must be used only for official business purposes.

1. All users must accept full responsibility for using Visascape Pty ltd resources and systems in an appropriate, ethical, safe and legal manner.
2. Only authorised users may use the facilities such as internet, email and other communication facilities and a user may only use the facilities they are authorised to use.
3. The systems may not be used for the transmission of information which infringes the copyright of another person / organisation, or the creation or transmission of defamatory, unlawful, abusive material.
4. Each user is responsible for all information sent and accessed under their user login.
5. User must apply professional integrity and respect other's right to privacy and must comply with the requirements of the Privacy Act 1988.
6. No user shall use the IT facilities for private gain or to facilitate financial gain to an unauthorised third party.

Limitation of Liability

Visascape Pty ltd does not guarantee that the functions or services provided by or through information and communications technology will be error free or without defect.

1. Visascape Pty ltd will not be responsible for any damage staff may suffer including, but not limited to, loss of data or interruptions of service, whether such loss of data or interruptions of service is incurred through a breach of this policy.
2. Visascape Pty ltd is not responsible for the accuracy or quality of the information obtained through or stored on the network.
3. Visascape Pty ltd will not be responsible for financial obligations arising through the unauthorised use of provided technology.

Employee Acknowledgement

Users must acknowledge that they have read, understood, and agreed to abide by policies relating to the use of Visascape Pty ltd systems and facilities and are required to sign an acceptable use agreement.

Monitoring and Privacy

Visascape Pty ltd has established procedures to assist in the provision of information technology services and the maintenance of security. This includes the use of network accounts and passwords to restrict access to the network to authorised use only.

The contents and usage of email and Internet access are subject to regular monitoring by Visascape Pty ltd. This will include electronic communications which are sent or received, both internally and externally. Where inappropriate use is suspected through this means or other incidents, the system administrators may be authorised by the Managing Director to examine access logs and / or email accounts.

Visascape Pty ltd seeks to comply with privacy and confidentiality requirements; however, emails may contain personal or classified information or material in which third parties own or claim copyright. Visascape Pty ltd may access, review, monitor, and disclose the contents of all messages created, sent or received for the purpose of monitoring compliance with this policy or compliance with any terms and conditions of employment or engagement.

Acceptable Use

Visascape Pty ltd resources, equipment and information are to be used for business operation purposes. Their use must be ethical, lawful, and appropriate, in accordance with Visascape Pty ltd values and policies, and with any applicable contractual requirements.

Equipment

1. Users must take due care when using IT equipment and take reasonable steps to ensure that no damage is caused to IT equipment.
2. Users must report any damage or loss of IT equipment to the Service Desk.
3. The use of printers, scanners, digital cameras, projectors, and other technologies available within Visascape Pty ltd shall be limited to business operational activities except where authorised.
4. Users shall not connect any unauthorised equipment or device such as USB drives to Visascape Pty ltd resources.

Information and Information Systems

1. While using Visascape Pty ltd information systems, users must:
    a. Always protect their user id and passwords.
    b. Be mindful of email etiquette.
    c. Log out of systems when not in use.
    d. Exchange information only through approved channels.
    e. Report suspected breaches of compliance.
    f. Use only authorised software.

2. All documents created and stored on the network will be treated as related to Visascape Pty ltd. Accordingly, users should not expect that any information or document transmitted or stored on the Visascape Pty ltd computer network is personal to them.
3. Authorised users must use the allocated storage space for storing business relevant operations artefacts. Any files that are no longer required should be securely disposed of.
4. Consider intellectual property rights and copyright when using information and images.
5. The Privacy Act 1988 requires individuals and Visascape Pty ltd to take reasonable steps to protect personal information that is held from misuse and unauthorised access. When logged on, each user is responsible for the activity undertaken using their login.

Internet Access and E-mail

Visascape Pty ltd permits users to access and use the internet, including email and web services, to facilitate greater efficiency in business operations, communication among internal users and external entities. Using the internet and emails in a manner that may cause offence or bring Visascape Pty ltd into disrepute is prohibited and may result in disciplinary action. Likewise, deliberate circumvention of the principles of this policy may lead to disciplinary action.

Users must observe the following with respect to accessing the internet:

1. Take all reasonable care when downloading, accessing, or executing files on or from internet services. Users are not to download or post material that could cause damage or disruption. This includes, but is not limited to, viruses and instructions on creating malware.
2. All internet files including web pages, graphics and files may be subject to copyright and users must be aware that copyright restrictions apply.
3. Information classified Confidential or above must not be shared on social networking sites or on the internet.
4. Staff shall not access Internet based file storing services unless required to for official business.

All users shall observe the following with respect to email usage and should be conscious of the following facts:

1. Use their access with respect and courtesy for others and in a responsible and professional manner.
2. Ensure emails that constitute a business record are saved to the appropriate location on Visascape Pty ltd's shared locations.
3. Personal views or information transmitted using Visascape Pty ltd resources should include a disclaimer mentioning the views and thoughts expressed in the email are of the sender and doesn't represent that of Visascape Pty ltd.
4. The delivery, confidentiality and privacy of email cannot be guaranteed across the Internet.

5. Emails are saved and can be accessed and read by authorised system administrators and managers.
6. In certain circumstances, Visascape Pty ltd may make staff emails available to investigative bodies as legal evidence.

Social Networking Services

Business use:

1. Staff are prohibited from revealing any Visascape Pty ltd classified information when engaged in social networking.
2. Staff should not engage in any social networking activities that may harm or tarnish the image, reputation and / or goodwill of Visascape Pty ltd and / or any of its staff.
3. Staff are prohibited from making any discriminatory, disparaging, defamatory or harassing comments or otherwise engaging in any conduct prohibited by Visascape Pty ltd code of conduct; and
4. Staff should not attribute personal statements, opinions, or beliefs to Visascape Pty ltd.

Personal use:

1. Limited and occasional personal use of Visascape Pty ltd systems to engage in social networking is acceptable, provided that it does not interfere with regular work duties.
2. Personal use shall be performed in a professional and responsible manner which does not otherwise violate Visascape Pty ltd policies or is not detrimental to Visascape Pty ltd best interests; and
3. Staffs assume any risk associated with the personal use of social networking.

Instant Messaging

1. Instant messaging should primarily be used for work purposes, personal use should be infrequent and brief.
2. Use of instant messaging at work is not considered private so staff using instant messaging do not have the same personal privacy rights as they would have when using their own private phones for conducting personal conversations.
3. Instant messaging should not be used to send fraudulent, unlawful, or abusive messages.
4. Staff who initiate threatening, intimidating, or harassing message will be subject to disciplinary action; and
5. Communicating matters of a classified information should be limited via instant messaging.

Password Use

Staff are required to comply with the requirements identified in the password guidelines.

Clear Desk and Clear Screen policy

Staff should follow a moderately clear desk and clear screen policy for information processing facilities in order to reduce the risks of unauthorised access, loss of and damage to information.

4. Staff shall not leave classified papers unattended on printer trays, or photocopiers, etc.
5. Staff shall log off from active sessions and lock their screen holding classified information, when away from their computer.
6. Staff shall activate a password-protected screensaver when away from their desk.

Remote Access

Authorised remote access staff should:

1. Safeguard the laptops provided by Visascape Pty ltd.
2. Notify the Service Desk if their credentials are lost or compromised; and
3. Report actual or suspected remote access security breaches to senior management.

Handling and Use of Removable Media

1. Use of any personal removable media for copying Visascape Pty ltd information is strictly prohibited.
2. Staff shall keep their official removable devices secure to avoid any theft or unauthorised data access.
3. Staff shall not copy information from removable media (media received from external source) to Visascape Pty ltd assets (even if for business purposes) without checking the source for any type of malicious code presence.
4. Removable media access shall be reviewed whenever there is change in responsibility, staff, and project.

Security of equipment off premises

1. Portable IT equipment (e.g. laptops, phones, removable media, etc.) should not be left unattended in public areas.
2. Portable IT equipment should always be carried as hand luggage whilst travelling.
3. In the event of portable IT equipment being stolen, the concerned personnel shall file a police report immediately. The personnel shall also inform the Service Desk about the theft.
4. Portable IT equipment should not be left on the desk or in the work area or any other visible location unattended or overnight. It should be locked in a secure area earmarked for the safekeeping of laptops when not in use.

Unacceptable Use

IT resources including internet, email or messaging should never be used for the following purposes:

1. To post personal contact information about themselves or other staff.
2. To represent others without express authority.
3. The Privacy Act prohibits the use of photographs or other forms of illustration that may identify an individual without their direct consent. This includes (but is not limited to) the use of digital cameras and mobile telephones to record and transfer images.
4. To abuse, vilify, defame, harass, degrade, or discriminate (on the grounds of, for example, sex, race or disability etc.) Defamation refers to any statement (including photographs and cartoons) that can harm another person's reputation.
5. To send, assent to receive or store obscene, offensive, or pornographic material.
6. To discuss or comment on the physical appearance of other persons (whether they receive the message or not).
7. To harass any person whether through language, or message.
8. To injure the reputation of the Visascape Pty ltd in a manner that may cause embarrassment to any member of Visascape Pty ltd.
9. To offend the values of Visascape Pty ltd.
10. To send unsolicited mail to multiple people (i.e. spam).
11. To send anonymous email intended to disguise one's identity or origin (i.e. spoofing).
12. To infringe the copyright or other intellectual property rights of another person.
13. To deliberately access or remain at a website with inappropriate or offensive content. From time-to-time users may be redirected to, or accidentally access, inappropriate material. These sites should be brought to the attention of the Service Desk in order for them to be blocked by the Visascape Pty ltd content filtering software and to ensure that it is noted that the material was not accessed intentionally.
14. To perform any other unlawful or inappropriate act.
15. Users are not to download or post material that could cause damage or disruption. This includes, but is not limited to, viruses and malware; and
16. Users are not to download or forward games, audio clips, movie clips or other files that do not constitute business purposes. The downloading and installing of music sharing software is strictly prohibited.

Chat GPT and AI

1. Guidelines for the responsible and secure input of client information and company data into Chat GPT.
2. Definitions
3. **Chat GPT:** A large-scale artificial intelligence language model developed by OpenAI, used for generating human-like text based on provided input.
4. **Bing:** A web search engine owned and operated by Microsoft. Bing uses Chat GPT and although it has a discrete front-end, it leverages Chat GPT on the back end such

that from a data privacy standpoint it should be considered as synonymous with Chat GPT.

5. **Client Information:** Any data or information related to clients, such as names, contact details, financial information, or other confidential and sensitive details.
6. **Company Data:** Any data or information related to the company's internal processes, trade secrets, intellectual property, financials, or other confidential and sensitive details.
7. Employees are strictly prohibited from inputting, sharing, or discussing sensitive client information or company data in Chat GPT. This includes but is not limited to:
8. Personal Identifiable Information (PII), such as names, addresses, or any other information that can identify an individual.
9. Financial information, such as account numbers, credit card details, or transaction histories.
10. Confidential client records or communications.
11. Proprietary company information, including intellectual property, trade secrets, and internal strategies.
12. Employees are expected to adhere to the company's data security and privacy policies whilst using Chat GPT. This includes reporting any suspected data breaches or unauthorised use of Chat GPT to the IT department or designated data security officer.
13. Data Input Best Practices
14. When using Chat GPT, employees should:
15. Always anonymise client and company data by using generic placeholders or pseudonyms when discussing specific cases or scenarios.
16. Avoid discussing specific client or company projects in detail, focusing instead on high-level concepts and strategies.
17. Verify the accuracy and relevance of any information generated by Chat GPT before sharing it with clients or colleagues.

Reporting Security Weaknesses / Incidents

All staff are expected to report immediately, any observed security weaknesses or violations, to support@fusetechnology.com and the Service Desk, examples include:

1. Classified Visascape Pty ltd information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties.
2. Unauthorised use of Visascape Pty ltd information systems has taken place or is suspected of taking place.
3. When passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
4. All unusual system behaviours, such as missing files, frequent system crashes and misrouted messages.
5. Any other suspicious activities.