Truscreen Group Limited
Technology Governance and Cyber Risk Policy

TruScreen's (the "Company") Information technology governance falls under three categories which are:

1. Being aware of information and digital technology changes and their possible application to TruScreen's business – both as an opportunity and as a threat.
2. Ensuring the Company has current computing and other related technology that enables the efficient and accurate running of the business.
3. Being aware of, and mitigating against, Cyber security and other digital technology risks.

1. Awareness of changes in information and digital technology

The nature of TruScreen's business is ultra-high tech, with advanced algorithms being processed on advanced circuit boards with world leading optical and electrical data conversion. The Directors and Senior Executives of TruScreen are being constantly exposed to the latest innovations in digital technology.

The company needs to ensure it continues to effectively monitor changes in information and technology relevant to the business and it has the right systems and processes in place to capture these changes and respond in a timely manner.

2. Sufficient Computer and Related Technology

For the Company's business to operate efficiently, all computer hardware and software needs to be up to date and fit-for-purpose and all staff have to have access to any technology that is essential for them to perform their job. Accounting, invoicing and reporting packages need to conform to all current legislation and be on platforms that enable them to perform effectively.

Any issues/problems need to be resolved in a timely manner that does not put the business at risk.

3. Cyber Risk

To ensure that TruScreen is and continues to be protected against all forms or Cyber Risk the following procedures and practices are to be followed at all times.

Review of Risks

The CEO is to report on the management of Cyber Risk to the Audit and Risk Committee at 6 monthly intervals.

User Error

All staff are to be counselled on user error risk and the need to guard against user risk;

All work is to be backed up daily on an external hard drive or by using a reputable cloud based back-up service;

Key documents are to be locked for editing as read only documents or saved as PDF's to protect against inadvertent amendment.

Confidentiality

All staff are to have confidentiality clauses in their employment agreements that control the use of any and all data and information in possession of the Company.

Physical Security

The company's critical computers and servers are to be secured in an office with 24 hour security;

Access to key intellectual property is to be restricted and monitored regularly.

Virtual Security

The company's servers and computers are to be protected by a recognised firewall(s) and Internet Security program(s);

All firewall and security software is to be kept up to date and the latest patches uploaded to all computers when prompted;

All mobile devices that have access to TruScreen's emails or other communications are to be PIN or Password protected.

Remote Access

No remote access to the Company's servers is to be granted without first assessing physical and virtual security.

Review of Host Services

TruScreen's host services are to be assessed every 6 months for their security practices.

Credit Card/Bank Account risk

The passcode for Executives and staff who possess company credit cards is not to be part of any other passcode to any computer or server in the company;

The company's bank accounts are to be dual protected by PIN/Password and by dongle/passkey – ensuring that a cyber-hack could not get the information necessary to access the accounts.

Web Attacks

Web attacks are to be managed by the Company's Web Host(s) and reported to the company immediately. This needs to be included in any contractual agreements with the Host(s).

Internet Point of Sale

Any internet point of sale portals must be secured behind adequate fire walls and protected by up to date encryption technology.

Malware Protection

All Firewalls and Internet Security are to be reviewed annually to ensure that they have adequate counter measures in place to guard against Spam, Phishing, Worms, Viruses and other Malware;

Staff are to be trained, and re-trained annually, on the avoidance of Malware;

Staff mailbox limits are to be reviewed six monthly.

Staff Termination/Resignation

All relevant IT accounts are to be deleted or disabled upon a staff member's resignation or termination;

All passwords that are known to the leaving staff member are to be changed.

Sensitive Data

All sensitive data is to be managed via a 'user privileges basis' and all staff are to comply with any instructions issued from time to time on the restriction of access to any information;

The CEO is the sole authority for granting user privileges to access sensitive data.

IT Register

All IT equipment possessed by the Company is to be logged into an IT register and tracked for its physical location and custody.

Portable Data Storage Devices

All staff are to be instructed in, and re-instructed annually, in the safe custody of any portable data storage devices including but not limited to laptops, notebooks, tablets, smartphones, USB drives, cd and dvds to ensure that all TruScreen's information contained therein is protected against theft or duplication.

Virtual/Cloud Storage

No Company information is to be kept on any cloud based or other virtual server/storage provider service without that service/provider being assessed by the CEO as having an acceptable level of security in place.

Staff Training and Practices

TruScreen Staff are, upon employment and annually, to be trained and instructed on compliance with this Cyber Risk policy;

TruScreen staff are, upon employment and annually, to be trained and instructed on the compliance of the provisions of their employment agreement detailing the need to follow all company policies and specifically with the need to follow the confidentiality provisions of their agreements;

The CEO will regularly, on both an Ad Hoc and on a minimum quarterly basis, conduct surveillance of the workplace to ensure compliance with all provisions of this Cyber Risk policy;

the CEO is charged with the maintenance of the Company's IT capability and security, and the CEO is responsible to the Board to oversee that this is done.

Incident Management Plan

All staff are to be trained, upon employment and annually, to follow the Incident Management Plan set out in Appendix 1 of this Policy.

Review and Update

The CEO and the Audit and Risk Committee, will on an annual basis review this policy, the Incident Management Plan, the Cyber Protection software and technology, and any other component of Cyber Risk and IT governance. Items to be addressed in this review will include but are not limited to:

Security Breaches – both inside and outside of the Company and is TruScreen capable of preventing a similar breach;

Monitoring and testing of the current Policy;

Security of any additional hardware, software, portals or web pages added since the last review;

Removal of any software no longer needed;

User privileges.

The result of this review will be reported to the Board at the next Board Meeting following the review.

Appendix 1
Cyber Incident Management Plan

Step 1. Monitor, Detect and REPORT

- All staff are to be alert to any potential, suspected or actual cyber breaches and to report the same immediately to the CEO, or in his absence, a member of the Board;
- All staff are to be alert to media reports of cyber breaches in other businesses and report these to the CEO if they suspect that TruScreen may have suffered a similar breach.

Unusual activity or events may include:

- Alerts and reports about potential malicious activity or vulnerabilities. This can include alerts from Intrusion Detection System software or reports from a technology or network provider;
- The theft, loss or breach of a device, including personal mobiles used to access work emails;
- External events and publicised or high-profile cyber security incidents, both overseas and in Australia or New Zealand. Read media reports and ask whether the Company could be impacted – don't assume you are immune;
- General day-to-day indicators, such as unusual email activity, incident reports, or being informed by staff or customers that a breach has already occurred.

Step 2. Report and Record

The suspected or actual breach should be reported to the CEO via an emailed file note (or handwritten note if all systems are down) that contains:

1. Date;
2. Time;
3. Place;
4. Description;
5. Suspected Perpetrator (if identified);
6. Any relevant comments or information.
   If the matter is urgent, it should be escalated to a member of the Board.

Step 3. Action – Cyber Incident Report (CIR)

The CEO, will, upon receipt of the report of any Cyber Breach immediately conduct the following CIR assessment:

- **Categorise** the incident – how severe is it and what are the potential impacts?
- **Prioritise** – does this require an urgent escalation or can it be easily resolved?
- **Assign** – who is responsible for managing and resolving the incident, and by when? This information then informs the Response process.

Step 4. Response

Technical:

The Staff member **Assigned** to manage and resolve the incident will be guided by the following minimum recommended process:

- Plan a resolution;
- Co-ordinate internal and external actions;
- Contain ongoing malicious activity;
- Repair or recover affected systems;
- Generate a post mortem analysis;
- Generate an incident closure report.
  Advice from the company's IT service providers should be sought where needed.

Management:

Management shall follow the following process:

- Notify affected staff and or customers/suppliers of the breach;
- Advise them of steps taken to resolve the incident;
- Approve courses of action taken or advised to be taken;
- Communicate with all affected Parties.

Legal:

The CEO will manage the Legal actions associated with the incident with regard to the following factors

- Does the incident involve privacy, non-disclosure, copyright or other legal matters;
- Does it involve Fraud or Cybercrime –if so report to the police.

Step 5. Resolve and Review

Once the incident has been resolved, the CEO will review both the incident and the resolution of the incident.

The CIR for the incident will be closed off with full Corrective and Preventative action steps detailed.

Issues that need to be specifically addressed are:

- **The gaps** in the company's Cyber security or work practices that allowed the incident to occur;
- **The steps recommended to prevent** a repetition of the incident;
- **A review of the management of the incident** to see, with the benefit of hindsight, whether the incident could have been better managed and make any recommendations to improve the management of future incidents.

The CEO is responsible to ensure that any recommended preventative actions in the CIR are put in place, subject to the company's financial and practical ability to do so.