DATA AND PRIVACY - WORKPLACE SURVEILLANCE/ACCEPTABLE USE POLICY

Summary

This policy sets out guidelines for acceptable use of various forms of electronic communications by our employees (**you**). It also provides details of the monitoring that we may undertake of your use of the Company's electronic communications facilities and resources.

The primary purpose for which access to electronic communications is provided by us to our employees is to assist you in carrying out the duties of employment. Employees may also use electronic communications for reasonable private purposes that are consistent with this policy. We may modify this policy upon 14 days notice in writing to you.

This policy applies to all electronic communications which make use of resources, infrastructure or equipment of IAmVerified Pty Ltd accessible to you when you are at any workplace or other place where work for the Company is carried out, whether or not you are actually performing work at the time, or at any place while performing work for the Company. It also applies to monitoring of use of electronic communications when you are not at work but where the monitoring is computer surveillance of your use of equipment or resources provided by or at the expense of the Company.

What are electronic communications?

Electronic communications covered by this policy include each of the following:

(a) Computers connected to any network or data circuit.
(b) Electronic data interchange.
(c) Electronic mail.
(d) Messaging services, including pagers, paging services and SMS.
(e) Internet, intranet and extranet services, including blogs and podcasts.
(f) Telephones including mobile telephones.
(g) Personal digital assistants.

Record keeping

Electronic communications and electronic records are no different to paper documents and records and are important parts of our business records. They are subject to the same laws and record keeping requirements as our other documents and records. Accordingly, you are responsible for ensuring that your electronic communications and all other electronic records

are recorded and stored in accordance with the Company's document management procedures and policies.

Use of electronic communications

Your use of any electronic communications must comply with this policy, your terms and conditions of employment, any other policies of the Company that may be notified to you from time to time as well as normal standards of professional and personal courtesy and conduct. These standards are expanded upon in this policy. Your use of any electronic communications for any purpose other than undertaking your duties as an employee is acceptance by you of the Company's collection, use, disclosure and storage of any personal information resulting from that use.

Confidentiality

Electronic communications are not private. In the course of delivery, an electronic communication may pass through multiple servers or other infrastructure outside the control of the Company and may be viewed or copied by third parties. Care must be taken in forwarding information or documents out of our office, so that they are sent in accordance with our security and confidentiality policies.

In addition, electronic communications are monitored by the Company (see below).

Communicating externally about aspects of the Company, its operations or customers or information of our customers/ clients or copying or removing files or data that are confidential or subject to other restrictions on disclosure is absolutely prohibited and is grounds for disciplinary action, including immediate termination, and other legal action. As an employee you may have access to personal information about other Company employees and customers of the Company. Confidentiality of that information must be maintained. Communicating internally about the personal information of other Company employees and clients is absolutely prohibited unless for the purpose of carrying out your duties in the course of your employment.

What is acceptable use?

Subject to the terms of this policy, you may use the electronic communications resources provided by the Company for each of the following:

(a) Work or client related purposes.

(b) Sending and receiving personal communications, provided that for any personal communication sent with a Company email address in the From: or Reply-To: header, a disclaimer must accompany the email that the communication is a personal

communication and the views of the sender may not represent those of the Company. The Company accepts no responsibility for personal electronic communications.

(c) Accessing the World Wide Web for personal purposes. Purchasing products or services via the internet is not prohibited but the Company accepts no liability for risks or costs associated with any use of the internet for making purchases of any sort.

(d) Utilising any other electronic communications service or protocol for personal purposes, after obtaining permission to do so from the General Manager or Chief Information Officer.

Any personal use within normal business hours must be moderate in time. Any personal use must not incur significant cost for the Company and must not interfere with your employment duties or those of any other person.

What is not acceptable use?

Except in the course of your duties or with the express permission of the General Manager or Chief Information Officer, the electronic communications resources provided by the Company must not be used for any of the following:

(a) Excessive personal use within normal business hours.

(b) Personal use that incurs any significant cost for the Company.

(c) Personal use that interferes with the employment duties of the employee or any other person.

(d) Personal commercial purposes.

(e) Making our infrastructure available for third parties to use without the permission of the General Manager or Chief Information Officer.

(f) Sending Spam within the meaning of the Commonwealth Spam Act 2003 (Spam).

(g) Subscribing to or accessing external email services or personal email accounts.

(h) Subscribing to or accessing news groups without the permission of the General Manager or Chief Information Officer.

(i) Instant messaging.

(j) Disseminating confidential information of the Company or of any customer of the Company.

(k) Any illegal activity or purpose.

(l) Knowingly or recklessly causing interference with or disruption to any user of any, or to any, network, information service or equipment.

(m) Disseminating any personal information (within the meaning of the Privacy Act 1988) of any officer, employee or customer (or an officer or employee of a customer) of the Company without consent.

(n) Sending or otherwise knowingly or negligently causing any other person to view content that may render the Company liable as a result, whether pursuant to equal opportunity, sex or racial discrimination or any similar legislation or other law, including defamation, racial vilification, misleading and deceptive conduct or any other law, at the suit of that person.

(o) Knowingly downloading or requesting software, media files, data streams or other content or information that a reasonable person believes will use a greater amount of network bandwidth than is appropriate or that are, or any copy is likely to be, infringements of the rights of any person (including intellectual property rights).

Monitoring

Our professional obligations to our clients, business partners and employees require adequate security protection between internal systems and customers' external electronic communication systems. This requires monitoring of electronic communications. Monitoring is also necessary to help manage our resources, including bandwidth, in an appropriate and cost effective manner and to ensure compliance with all other legal and regulatory requirements. Monitoring is also used by the Company to check compliance with this policy (and our other policies), and to undertake investigations if the Company has cause to believe this policy has been breached and to obtain evidence of unauthorised or unlawful activity.

The Company has a system of continuous and ongoing monitoring by means of software, hardware or other equipment that records the information, input or output or other use of our computer and communication systems and programs including the sending and receiving of emails and accessing of internet websites.

This monitoring includes:

(a) Software programs that automatically scan all incoming and outgoing electronic communications, including email messages, attachments and details of internet sites access.

(b) Generation of detailed user logs, including information in relation to employees' use of the internet, email addresses of those with whom employees have communicated and other information relating to use of our facilities, equipment and infrastructure in relation to electronic communications. These user logs are accessible to the network administrator, the Chief Information Officer and the General Manager.

(c) Filtering devices to detect and block inappropriate electronic communications including incoming executable files.

(d) Filtering devices to deny access to certain websites or other content that we consider

to be inappropriate or to which access amounts to inappropriate use under this policy.

(e) Workflow management and reporting by user and by document or file, including details of when documents are created, accessed or modified and the identity of the user.

The Company may also engage in real time surveillance of electronic communications use. Unless required by law, we may undertake any monitoring without any further notification to any employee that monitoring is occurring.

You also need to be aware that:

(a) The network administrator can and is authorised to access any area, files and electronic communications on our network, even those that are password protected.

(b) All files, data and electronic communications are routinely subject to backup. Backups of data and systems are retained by us for periods up to 12 months. Backups may be accessed at any time for the purposes of monitoring the use of our computer and electronic communication systems and programs.

If the systems or procedures used by us prevent delivery of an email communication to you, we will give you notice (prevented delivery notice) as soon as practicable, by email or otherwise, that delivery of the email has been prevented, unless the law provides that a prevented delivery notice is not required. The Company is not required to give a prevented delivery notice for an email if delivery of the email was prevented in the belief that, or by the operation of a program intended to prevent the delivery of an email in any of the following circumstances:

(a) The email was Spam.

(b) The content of the email or any attachment to the email may reasonably have resulted in an unauthorised interference with, damage to or operation of a computer or computer network operated by us or of any program run by or data stored on such computer or computer network.

(c) The email or any attachment to the email would be regarded by a reasonable person as being menacing, harassing or offensive.

The Company is also not required to give a prevented delivery notice for an email sent by an employee if we are not aware (and cannot reasonably be expected to be aware) of the identity of the employee who sent the email or that the email was in fact sent by an employee.

Nothing in this policy prevents delivery of an email or access to a website merely because of either of the following:

(a) The email is sent by or on behalf of an industrial organisation of employees or an

officer of such an organisation.

(b) The website or email contains information relating to industrial matters (within the meaning of the Industrial Relations Act 1996).

This Policy constitutes notice in writing under the Workplace Surveillance Act 2005 of the intended surveillance for the above purposes.

Privacy

As part of your duties as a Company employee, you may be required to collect personal information of other Company employees and clients. You are bound by privacy law and ethical practice to keep that personal information confidential. You cannot use or disclose that information to any person except for the purposes of carrying out your duties as an employee or for administering the Company's products and services directly to the person whose information is collected. These obligations extend to all information collected by means of electronic communications.

The Company collects personal information from a variety of sources including its website, telephone calls and directly from clients and other parties.

When collecting personal information over the telephone or directly, you must obtain that person's consent and provide an explanation of the use and purpose that you intend to use that personal information.

You must allow the person whose personal information has been collected by the Company to access or update that personal information if requested. Access must be requested in writing and identification must be provided. You may refuse access to personal information in special circumstances specified in the Privacy Act.

You must take all reasonable steps to protect the personal information the Company collects from misuse, loss, unauthorised access, modification or disclosure.

Consequences of a breach of this policy

Responsibility for use of electronic communications that does not comply with this policy lies with each employee. It is a condition of your access to our facilities, equipment and infrastructure necessary for electronic communications that you indemnify us for any direct loss and reasonably foreseeable consequential losses suffered by the Company as a result of any breach of this policy by you.

If the alleged breach is of a serious nature, that amounts to a breach of your duty of fidelity to the Company (for example, emailing our confidential or proprietary information or a

customer's confidential or proprietary information to a competitor or a potential competitor), you must be given an opportunity to be heard in relation to the alleged breach. If the serious breach of this policy is admitted or clearly established to the satisfaction of the General Manager, the breach may be treated as grounds for immediate dismissal.

In all other circumstances, an alleged breach of this policy will be dealt with in accordance with our disciplinary processes and procedures.

If you have any questions in relation to this policy or its application please contact iamverified.nft.id@gmail.com.