IMS 20	I.T Security and Computer Use Policy	SKG Services

SKG Services has built its IT security on 2 fundamental tenets – legal compliance to the Australian Privacy Act 1988 (as amended By Act No.74 2012) and general compliance to the requirements of ISO/IEC 9001:2015 Information Security Management and ISO/IEC 27001:2013 Information Security Management Systems.

Privacy

To comply with both the Act and the Standard, SKG Services has in place monitoring steps to follow inputs, outputs and activities centred on IT risk management. The process approach assists in company staff achieving their main objective of protecting information. SKG Services staff access to the network is controlled by password and only the most trusted employees carry out remote out-of-hours data inputs. Passwords are regularly changed and leaving staff have their access to the system terminated.

In developing its IT Security Policy, SKG Services has drawn on a process approach as staff access confidential personal information as an integral part of their daily work activities. Our information security management is a range of processes - handling, clearing, placing and retaining records of medical practitioners and the health and education facilities involved in offering employment or placements.

In-House Security & Breach Recovery Plan

The context of SKG Services supplying cleaners, maintenance and security staff to a range of business, industrial, retail, health and education facilities is based on the gathering and disseminating of confidential data. SKG Services staff accept communications in many forms – email, social media platforms, phone messages and personal phone calls. It is the responsibility of staff to verify these contacts and not proceed to respond until they are satisfied that the contact is genuine.

SKG Services management is fully aware that staff can be the weak link in IT Security and to overcome this risk the company provides training and staff user accounts that are password protected. Staff is instructed to not allow others including colleagues to have access to their IT equipment.

To overcome accidental disclosure of confidential data SKG Services staff is trained to follow closely the company's key processes, in particular the 'Document and Records Process' and the 'Communications Policy'. These form standard operating processes for staff communicating with potential and current clients, cleaners, security staff, and sub-contractors.

This IT policy is a cover statement for the ongoing training of staff in handling confidential data, regular team meetings to address issues of awareness of the need to only communicate what is required to achieve essential outcomes. Senior management has identified the roles of staff so that there are checks within checks. New staff are required to sign confidential agreements as protection from stealing data and providing it to other cleaning and security companies.

Communication processes are strictly identified – email addresses are monitored so there is minimal scope for scamming and hacking and all data is backed up hourly and daily. If there is a breach of service or security the loss of data would be no more than 15 to 20 minutes. Staff is trained to formalise contacts using identified email addresses and mobile phone numbers within Australia rather than uncertain addresses and phone contacts.

Digital Marketing Security & Breach Recovery Plan

SKG Services has set up a professionally developed interactive digital website to advertise the company to the wider community to attract new clients. The site is data-rich and could be a target for online criminals accessing the confidential information. The most serious likely threat to SKG Services digital platform is linked to the presence of salary and payment information for office staff, cleaners, security guards, and sub-contractors.

To counter threats of malware SKG Services has a strong firewall and encryption tools covering data transmission in place but recognises that the most effective barrier against all forms of hacking is the continued education of staff. Raising staff awareness to the point where they can recognise irregularities in performance, delays in transmission, partial loss of data and unsolicited responses from potential clients or bogus clients.

If these events occur staff terminate the online communication and contact the client, cleaner, guard or sub-contractor direct by phone to verify recent or attempted communications.

Preventative Measures

SKG Services has spent many hours developing preventative action plans to deal with risks and opportunities to strengthen security. Preventative measures have involved linking IT security with the management requirements of ISO 9001:2015 (SKG is ISO certified) – (having documented processes) to overarch all business aspects so that even non-confidential communications adhere to the same rigorous controls. These communications might deal with requests for more information or availability for work without a committal.

Management is aware of the need for Information security objectives and this is included in all team meetings and senior level meetings and agenda include the results of risk assessments. An example of a risk assessment may centre on a potential client who may have lodged documents that reflect an alleged agreement – when no such commitment has been made by SKG Services. If staff are concerned of a possible leak of information, they may terminate the approach or request the potential client to attend an interview.

In complying with ISO 9001:2015 SKG strives to continually define and refine the organisation of its electronic operations to shore up loose ends, regularly update business processes, provide in-house staff training, provide mentoring for new staff, perform risk assessments of potential security breaches, and embrace both annual internal and external audits.

SKG Services is aware that staff with responsibility for IT security must meet the requirements of ISO 9001:2015 to ensure that there is no negative performance to compromise the integrity of electronic data. Current staff members meet these requirements.

Computer Use

It is the policy of SKG Services to operate our business in a manner that does not expose us or our clients or customers to any risk of loss or damage through the use or misuse of electronic data transfer.

To achieve this, we reserve the right to exercise control over the way company computers are used to access the Internet, and in the use of company computers for personal communications, including the right to monitor, log, and/or restrict access to the Internet or email with or without prior notice.

The uncontrolled use of company computers for private purposes can result in loss or damage due to security breaches, corruption or loss of data, programmes and operating systems due to virus and malware, etc., infection, and unauthorised third-party hacking into company servers. Our aim is to ensure the integrity of our computer system(s) is not compromised through application of controls to prevent these unwanted events occurring.

A person must not, unless authorised or permitted to do so:

- Download or install any software on to a company computer
- Use company computers for gaming or other private purposes (such as accessing social networking sites)
- Download or access any material that could be considered offensive, pornographic or objectionable, or send or forward emails of an offensive nature
- Download company information for private purposes.

Computer users must:

- Ensure that anti-virus and spy ware programmes are kept up to date
- Carry out virus checks before opening emails, attachments or executable (.exe) files.
- Users must inform their system administrator immediately of any problems that may be encountered while using a company computer.

Key References

Australian Privacy Act 1988 and as amended By Act No.74 2012,

ISO/IEC 9001:2015 Information Security Management Systems,

ISO 9001:2015, and ISO/IEC 27001:2013