SECURITY AND PRIVACY POLICY

BIC Policy 019 - Issue Date: 16.10.2023

Our Commitment

All B.I.C. Services Pty. Limited (BIC) staff will undergo Federal Police and DIMIA Security Checks.

Scope

This policy applies to all our employees, regardless of employment agreement or rank.

Site Specific Security Procedures

BIC takes the necessary measures to ensure appropriate procedures are adhered to. All general security procedures are outlined and kept in the Operations Folder on site for reference.

The Site Supervisor and/or the Executive Manager is responsible for the keys or codes to access the premises where cleaning is to be performed. BIC staff will ensure that all external doors opened by staff are relocked on entering the premises. All internal doors that are locked on arrival are to be relocked before departure from site.

Only authorised personnel are allowed on site. All personnel entrusted with security alarm details are not to disclose that information to any other person. If security problems occur on arrival or departure, staff must immediately notify to the appropriate Site Supervisor, Executive Manager or Security contractor.

All employees requiring access to nominated areas will be issued keys/cards as necessary, which shall be recorded. No staff are to give access to another staff member, employee or visitor.

All keys/cards are to be returned on termination of employment or as requested from the Site Supervisor, Executive Manager or other authority.

General Security Procedures

B.I.C Services' has developed a number of general security procedures to be followed while working on site at all times:

On Work Sites and After Hours:

- Do not travel on an occupied lift. If somebody goes into the lift with you, get out and take the next one.
- Do not let anybody enter the building. Even if the person is an office employee you know, do not let them in.
- Keep all tenancy doors locked at all times, whether you are in or out of the tenancy.
- Carry your keys at all times while in the building. After finishing the job, return keys to the security or your supervisor (depending on site protocols) and sign out attendance portals.

- If you see strange people or a suspicious situation, immediately inform your Supervisor, Manager and Security.
- Do not assume papers or objects near rubbish bins are rubbish. Take as rubbish only what has been placed into proper waste or recycling bins.
- Wear your identification card at all times in a visible place.

Information Security and Protection of Intellectual Property

BIC has rules governing information management and several implementation rules of them for the purpose of controlling and managing information as valuable assets. Among their functions those rules provide protection to prevent infringement of third-party confidential information.

Responsibility

The Chief Information Officer has the responsibility for promoting information security, and confidence in its ability to not only continuously provide goods and/or services, but also to recover quickly from IT disasters with minimal computer disruptions. This policy helps to provide a safe, secure IT environment to serve BIC's staff and customers' requirements and ensure stability and continuity of the business IT Assets.

Measures to Prevent Leakage of Confidential Information

BIC constantly strives to enhance the security level of the IT systems it uses, and to take effective measures against unauthorised access and computer viruses. Technical presentations and technology licenses are required to review and prevent unintentional disclosure of confidential information.

BIC classifies its facilities based on level of criticality and limits entry to those facilities according to that classification.

Unattended Computers

Unattended logged in computers create easy opportunities for unauthorised access to information and misuse of accounts, such as sending of bogus email messages purporting to come from the genuine account holder.

Computers and other equipment such as smartphones must never be left unattended and unlocked when logged into BIC accounts. Before being left unattended they should be logged out or locked.

BIC requires staff to lock or go to screensaver when leaving a computer or device unattended for an extended period of time. A strong password is required to start up or resume activity. These passwords are not shared with others. To reset a password, staff must contact the IT department.

SECURITY AND PRIVACY POLICY

BIC Policy 019 - Issue Date: 16.10.2023

Protection of Personal Information

All BIC staff are Australian Federal Police (AFP) security cleared.

In the course of performing our services, staff may come across confidential information. We understand that this information belongs to our client and/or the Company and as such, all staff are required to keep this confidential information in confidence and they are not authorised to disclose this information to any person, firm or corporation.

Further, staff who have access to company information sign an agreement which clearly defines what IP is owned by the company, and how the employee is expected to handle confidential information and other IP during and after the course of their employment.

Protection of Intellectual Property

BIC's aim is to implement intellectual property (IP) activities organisationally, respect other companies' technologies, and maximise the values of BIC's proprietary technologies. For those purposes, BIC constantly promotes proper information management, prevent violation of IP-related laws and regulations, manage IP risks by expanding the scope of IP activities, and reduce risks associated with our overall IP activities by enforcing our internal rules.

Efforts for the Protection of Intellectual Property

BIC continuously acquire and utilise IP rights on technologies sustaining our technological edge and eliminate counterfeits that infringe BIC's IP rights. At the same time, BIC respects the IP rights of other companies, and conduct necessary investigations to avoid any infringement.

Any reported infringements are investigated thoroughly and acted upon immediately.

Data Control

BIC maintains full visibility over where critical information is stored, and who is given administrative privileges and access rights to that information.

- Data controls: File management systems that allows BIC to set permissions by user and administrative group.
- Physical controls: Physically secure rooms containing sensitive material and set restrictions on who can gain access to these rooms.
- Computer Malware: The procedure prevents data loss corruption or misuse of BIC's information that may occur when malware or "malicious software" is introduced into its IT network.

SECURITY AND PRIVACY POLICY

BIC Policy 019 - Issue Date: 16.10.2023

Software Security

Software is defined as programs and other operating information used by and installed on BIC's computers or storage media.

All licensing agreements are strictly adhered to and licensing in an appropriate manner to ensure ongoing vendor support. No unlicensed software is to be used. All software must be installed by the IT Department so as to ensure no virus or malware is introduced into the system.

All computers will be protected against viruses and have up to date anti-virus software installed.

Backup Strategy

There are two backup strategies in place at BIC; hardware and data.

The hardware has been configured to include redundant network paths, and redundant hardware where possible. If this is not possible, and where single points of failure exist, spare units are on site to replace failed pieces.

All data is backed up using snapshots and data deltas. A full snapshot is taken initially, and then daily data deltas are copied and applied to on-site and off-site backups. In the event that data restoration is required, individual files or whole servers can be restored quickly and easily from onsite backups. In the event of a catastrophic hardware loss, the backups will be restored to backup BIC hardware or to hardware provided by a third party.

Each night an on-premises backup of each virtual server is copied to a Synology disk array device. A second off-site backup is completed each night to an Azure based cloud storage provider. There are two copies so that for simple file restores, the faster, on-premises backup is used, whereas for a catastrophic event (fire, flood, etc.) at head office, the slower cloud back restore is used.

If one or more data files are deleted due to user error or malicious intention, these can be restored via the Veeam backup and recovery console. The software allows for recovery of not only files and folders, but also restoring of Active Directory elements and other lower level system configuration changes. Recovery of these files is completed by IT personnel on a case by case basis.

Tony Gorgovski
Chief Executive Officer