	BUZZWORKS CYBER SECURITY POLICY	Doc Type:	Policy
		Last Reviewed Date:	16 Jan 2026
		Next Review Date:	16 Jan 2027
		Owner:	S Sarlin

Policy Statement

Buzzworks is committed to providing and maintaining a secure digital working environment for creating, storing and/or working with Buzzworks confidential data, client and/or Government furnished materials and information. Risks to security will be prevented or mitigated, as far as is reasonably practicable, with control measures in place to minimise incident outcomes and restore routine operations as soon as possible.

Scope

This Policy applies to all Workers who are engaged by Buzzworks in any capacity or location during business hours or hours of work, as defined in the Buzzworks Security Policy.

Confidential data is secret and valuable. Its uncontrolled distribution, or unauthorised access, could cause financial, legal or reputational damage to Buzzworks. Confidential data includes, but is not limited to unpublished financial information, patents, formulas or new technologies, customer lists (existing and prospective) and commercial data from clients, consultants, vendors or Defence.

Buzzworks Cyber Security Priorities

This Cyber Security Policy outlines our guidelines and the provisions for preserving the security of our data and technology infrastructure.

Buzzworks directs its Workers to maintain a cyber-safe working environment by following the cyber security priorities listed below:

- Keep all devices password protected
- Ensure they do not leave their devices unlocked or unattended
- Be suspicious of clickbait titles and avoid opening attachments from unidentified sources and clicking in links when the content is not adequately explained
- Manage passwords properly, choose passwords with at least 8 characters and remember passwords instead of writing them down
- Wherever possible, access, modify and use client information on client infrastructure (through their virtual private network)
- Only share confidential data over the company network/ system and not over public Wi-Fi or private connection
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment

Buzzworks will maintain a cyber-safe working environment by ensuring the following the cyber security infrastructure is in place:

- Maintain a cyber safe workspace, by following the Australian Cyber Security Center (ACSC) Essential 8 Top 4, including ensuring that firewalls, anti-virus/malware software, patching and application control, and access authentication systems are installed
- Security and cyber security training are available to all Workers
- Be an active partner in the Australian Cyber Security Center Business Partnership Program, and give Workers regular updates about contemporary cyber threats
- Investigate security breaches thoroughly

Buzzworks Administrators have special system privileges. Buzzworks Admin access is limited to the Directors. When using Admin account access, Administrators are to:

- Refrain from browsing the web, obtaining files from online services or accessing emails
- Consider carefully the “need to access, need to read, need to modify” principle when assigning users access to confidential files and data, especially to clients or consultants outside of Buzzworks

Further Information

For further information contact any of the following:

- Buzzworks IT Security Officer - Shane Sarlin on 0413 417 446 or using the email DISP@buzzworks.net.au
- The ACSC Cyber Security Team via asd.assist@defence.gov.au

Policy Updates

This Policy may change from time to time and is available on our website https://buzzworks.net.au/policies.

Policy Complaints and Enquiries

Buzzworks is committed to providing an environment which is safe for all Workers. You will not be disadvantaged in your employment conditions or opportunities as a result of lodging a complaint.

If you have any queries or complaints about our Security Policy please contact us at:

Buzzworks

Enquiries: info@buzzworks.net.au

Complaints: complaints@buzzworks.net.au

Telephone: +61 7 3366 5080