



SAY IT NOW
VOICE CONSULTANCY

SECURITY POLICY

The following organisational security policy outlines the principles, guidelines, and measures to ensure the confidentiality, integrity, and availability of all information and assets within the SAY IT NOW business. This policy applies to all employees, contractors, third-party vendors, and any other personnel who interact with the organisation's systems and data.

Information Security responsibilities

- a) Management Commitment: Senior management is responsible for establishing and enforcing the security policy and providing the necessary resources to implement security measures effectively.
- b) Employee Responsibilities: All employees are responsible for safeguarding sensitive information, adhering to security policies, and reporting any security incidents promptly.

Access Control

- c) User Authentication: All users must have unique usernames and strong passwords to access organisational systems and data.
- d) Least Privilege: Access privileges will be granted based on the principle of least privilege, ensuring users only have access to the information necessary for their roles.
- e) Account Management: Access to systems and data will be promptly revoked upon termination or change in job roles.


Data Protection

- f) Data Classification: Data will be classified based on sensitivity, and appropriate security controls will be applied accordingly.
- g) Data Handling: Proper procedures will be established for data handling, storage, and disposal to prevent data leakage and unauthorised disclosure.

Information Technology Security

- h) Network Security: Firewalls, intrusion detection/prevention systems, and other security measures will be implemented to protect the organisation's network from unauthorised access and attacks.
- i) Malware Protection: Antivirus and anti-malware solutions will be deployed on all devices to detect and mitigate potential threats.

 07 3532 4073  info@sayitnow.com.au  www.sayitnow.com.au

 Level 22, 127 Creek Street, Brisbane Q 4000 | GPO Box 111, Brisbane Q 4001

ABN 29 524 001 127

Security Awareness and Training

j) Phishing Awareness: Employees will be educated about phishing attacks and social engineering techniques to prevent falling victim to such scams.

Incident Response and Reporting

k) Incident Reporting: All employees are required to report any security incidents, data breaches, or suspicious activities promptly to their designated manager/security team.

l) Incident Response Plan: An incident response plan will be in place to handle security breaches and mitigate their impact effectively.

8. THIRD-PARTY SECURITY

m) Contractual Obligations: Contracts with third-party vendors will include security clauses to ensure they meet the organisation's security standards.

This security policy will be reviewed periodically and updated as necessary to align with changes in technology or business processes. By adhering to this organisational security policy, we/SAY IT NOW aim to foster a secure environment, protect sensitive information, and maintain the trust of our clients and stakeholders.
