TBG INFORMATION SECURITY POLICY

REFERENCE:	TBG 9.0 | 03/2024
OWNERSHIP:	Chief Information Security Officer (CISO-ISM)
AUTHORISED BY	Cyber Security Committee (CSC - ISMS Steering)
REVIEW:	03/2025

PURPOSE

The BUSY Group (TBG) is committed to the confidentiality, security and availability of its information assets.

This policy and the supporting Information Security Management System (ISMS) policies, provide direction and support from top management for information security in accordance with operational requirements, relevant legislation, regulations and contractual requirements.

This policy is based on the principles and standards as defined in:

- ISO/IEC 27001:2022 Information Security, cybersecurity and privacy protection — Information security management systems —Requirements
- ISO/IEC 31000 Information Security, cybersecurity and privacy protection — Guidance on managing Information security risks
- Australian Signals Directorate (ASD) Information Security Manual (ISM) guidelines

Legislation:

- Australian Privacy Act 1988 (Cth)
- Data Protection Act 2018 – UK's implementation of the General Data Protection Regulation (GDPR)

INFORMATION SECURITY MANAGEMENT SYSTEM OBJECTIVES

The objectives of TBG's ISMS are:

- Protect the confidentiality, integrity and availability of information entrusted to TBG
- Provide partner organisations and interested parties with confidence in our systems and processes
- Conduct regular steering committee meetings with top leadership to monitor these objectives and review risks, corrective actions, improvements incidents, systems ownership, and plan uplift activities in relation to risk and actions:
    - Risk assessments and associated treatment and corrective actions plans to reduce and monitor risk.
    - Develop and multi-year strategic plan aligned to ISO 27001 and ASD ISM improvements
    - Regular reviews of ISMS policies and processes
    - Embed information security roles and responsibilities across TBG
    - Raise awareness and build a security-orientated culture across the business through the provision of information and cyber security training

    - Continue the ISO 27001 certification (internally recognised standard for information security)
    - Practice regular desktop and incident response exercises across teams
    - Set up a calendar of planned ISMS activities each year for review at CSC
- Build a security-oriented culture across The BUSY Group by:
    - Provide clear declaration that information and cyber security is everyone's responsibility
    - Regular training, refresher training and cyber security campaigns
    - Create a continuous improvement culture where TBG business units evolve to keep pace with changes in information security requirements
- Build strong collaborative networks to strengthen TBG security capability and provide confidence to interested parties:
    - Align TBG information and cyber security approach to national and international standards where applicable
    - Work with industry partners to share best practice and learnings
    - Leverage the ASD / ACSC partnership and AusCert's threat intelligence and information security capabilities and advice.

SCOPE

This policy applies to all The BUSY Group (TBG) staff, associated third parties; including but not limited to directors, contractors, clients, visitors, suppliers, physical sites, information and associated assets.

Specifically, this policy applies to all persons who

- process, store or transfer information at TBG
- are in roles as system owners
- are custodians of systems and data.

This policy also applies to any new project work that has any information technology, processing or other infrastructure requirement or equipment.

POLICIES

Detailed policies for information security are published on TBG's intranet page called "The Hive"

BACKGROUND

Information is an asset that, like other important operational assets, is essential to The BUSY Group operations and consequently needs to be suitably protected.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it must be adequately protected.

Information security is the protection of information (including systems) from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximize return on investments and operational opportunities.

Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and objectives of the organisation as met.

For each of the risks identified following the risk assessment, a risk treatment decision is made. Options for risk treatment include:

- Applying appropriate controls to reduce the risks;
- Knowingly and objectively accepting risks, providing they clearly satisfy the organisation's policy and criteria for risk acceptance;
- Avoiding risks by not allowing actions that would cause the risks to occur;
- Transferring the associated risks to other parties, e.g. insurers or suppliers;
- Or a combination of the above options to treat residual risk
- Reviewing risk to identify whether the controls had the desired effect or whether further controls are required.

PROCEDURE

The following sections provide the high level control requirements from ISO 27001:2022. Detailed policies and procedures are also provided on the intranet (Hive):

Organisation of Information Security

Objective: To manage the confidentiality, integrity and availability of information security within the organisation.

A management framework must be established by ITS to initiate and control the implementation of information security within the organisation.

Management commitment to Information Security

Management must actively support security within the through clear direction, demonstrated commitment, leadership, planning, resourcing, explicit assignment, and acknowledgement of information security responsibilities. These are defined in TBG Organisational Context and Scope document.

Allocation of information security responsibilities

All information security responsibilities are clearly defined in each Policy and TBG ISMS Roles and Responsibilities Procedure on TBG Intranet (Hive).

Authorisation process for information processing facilities

A management authorisation process for all information processing facilities must be defined and implemented. These are defined in Service Now and Business Support Processes. The ISMS Physical Security Policy can be found on TBG Intranet (Hive). To ensure availability requirements site locations must be tested by ITS for telecommunications suitability before signing contracts.

Performance evaluation
The approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security, improvements, nonconformances and corrective actions) must be reviewed independently at planned intervals, or when significant changes to the security implementation occur. This is achieved via CSC (ISMS Steering) meeting and management reviews, internal audit controls and the annual external audit.

Risk Assessment and Treatment (ISO 31000)

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational harm likely to result from security failures on individuals (privacy breaches) and reputational and contractual harm to TBG.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment must be repeated as often as necessary to address any changes that might influence the risk assessment results, but at least every 12 months.

Risk assessment must be completed as part of any project or hardware/software change or implementation, to make sure that whatever is being changed/implemented will not have a negative impact on exiting risks or creating new ones.

ITS Information security team will manage this process for information security risks. The asset / system owner will plan and action the treatment (mitigate, reduce, accept, transfer) and review with stakeholders and interested parties whether the risk treatment had the desired effect to reduce the risk level or further risk treatment is required. The BUSY Group ITS risk assessment and treatment plans are held in Folio.

RESPONSIBILITIES

Compliance

Document Review, Approval and History
This section details the initial review, approval and ongoing revision history of the standard. Post initial review the standard will be presented to the authorised personnel recommending the formal TBG policy consultation and approval process commence.

A review of this standard will be managed by the CISO on an annual basis or when major changes occur.

Compliance, monitoring and review
The systems development and quality teams are responsible for ensuring compliance with and monitoring implementation of this policy and to undertake reviews as required.

Quality Assurance
This document was developed by developed by internal and external consultation and research with internal key technical subject matter experts and business stakeholders.

Definitions
Refer to 'Roles and Responsibilities' page on the ISMS intranet page for role specific duties.

RACI

(R) Responsible	(A) Accountable	(C) Consulted	(I) Informed
ITS, Managers System Owners	CISO	Top management	Users, staff, suppliers, third parties

***Chief Information Security Officer (CISO-ISM**) – the CISO-ISM is responsible for the ownership, governance and dissemination of this document within TBG.*

***Information Security Officer (ISO**) – The ISO is tasked with maintaining and updating this document on annual basis*

***Managers** – Managers are responsible for the authorisation/registration and deregistration of access to TBG data and/or systems. Managers are to ensure that staff members are aware of the contents and the location of this policy, and that the policy is readily available for staff to view. It is each Manager's responsibility to ensure that any security affecting their area meets their business needs, and if it doesn't, to raise the matter with the Chief Information Security Manager as a matter of urgency.*

***Staff** - All other personnel are responsible for reading and understanding their obligations in relation to this document in the context of their relevant area of expertise. Staff members are responsible for ensuring they undertake appropriate security measures to protect TBG assets.*

***Operational responsibilities** - All TBG information assets must be kept secure and all of its staff / users are responsible and accountable for its protection. Non-compliance with these responsibilities will be dealt with by appropriate measures ranging from disciplinary to legal action.*

RACI Definition

Responsible: Refers to those who do the work to complete the task.

Accountable: Designates the person who ultimately answers the results of an activity, and also who delegates the work to the people who will execute it.

Consulted: Refers to those who sought to be heard on the related activity, and with whom there is two-way communication.

Informed: Designates those who sought to be kept up to date on the progress of the activity, and with whom there is just one-way communication

VERSION CONTROL

Version	Date	Change Summary	Author/Reviewer	Approved by:
8.0	18/03/2024	ISO 27001:2022 and entity updates	H Jolly	Cyber Security Committee
7.0	05/12/2023	Approved document lifted and reapproved.	Amanda Parsons	Clint Cunningham