



## IT & Cyber Security Policy

The **scope of this policy** includes the provision of a secure IT environment that protects Comstar, our people, customers and other stakeholders from the potential harm posed by cyber security threats. The scope includes:

- Comstar systems operations in Tasmania and Victoria
- Comstar employees, contractors and consultants working for Comstar
- The Comstar IT Network and potential threats to and from other IT networks
- Fixed IT equipment, mobile equipment, confidentiality and intellectual property

Comstar Systems has developed and implemented an integrated management system (IMS), incorporating a quality system aligned to **AS ISO/IEC 27001: 2015**. The IMS provides a framework for establishing and reviewing IT and cyber security objectives. For further information on this process refer to *the Administration Manual - IT and cyber security* and the *QEHS Planning Monitoring Measurement and Reporting Procedure*.

**Our senior management is committed to the IT & cyber security management system and shall:**

- Establish IT & cyber security **objectives** compatible with the **context and strategic direction** of our business.
- Integrate IT & cyber security management system requirements into Comstar processes
- Provide the **resources** needed for the IT & cyber security management system
- Take accountability for the **effectiveness** of the IT & cyber security management system i.e: that it achieves its intended results by:
  - **Communicating to personnel** the importance of effective IT & cyber security management and of conforming to IT & cyber security management system requirements
  - **Engaging, directing and supporting personnel** to contribute to the effectiveness of the IT & cyber security management system and to show leadership as it applies to their respective roles.
- **Promote continual improvement** of our IT & cyber security management system
- Fulfill **compliance obligations** including, statutory, regulatory and customer requirements as well as meeting the requirements of AS ISO/IEC 27001 deemed by management to be applicable to Comstar's needs.

This policy will be communicated to all employees and stakeholders as required and can be accessed on the P drive. Employees and other stakeholders are expected to co-operate and assist in the implementation of this policy. This policy shall be communicated and made available to interested parties:

- By employees through accessing the P/ drive
- By any stakeholder upon reasonable request or by accessing the Comstar website
- By inclusion in employee/contractor inductions and the contractor pre-qualification process.

Policy authorised by:

Catherine Hammersley-Cave  
Managing Director

Date: 3/5/21.

**When printed this document is uncontrolled – refer to Skytrust for the latest version.**