commtel | security

AIO5000

Security Management System Policy

commtelns.com

Internal

Document Control

Document No:	AIO5000	**Document Author:**	Security Manager
Document Title:	Security Management System Policy	**Company Unit Owner:**	Executive Management Team
Document Class:	Internal	**Document Status:**	Approved

Version	Approval	Revised by	Issue Date	Summary
1.1	EA066 / #151	Robert S	18-Aug-17	Adjust text.
1.2	EA066 / #154	Robert S	10-Oct-17	Add 'Management System' to title, removed word 'cyber'.
1.3	EA083 / #267	Alex N	13-Jul-20	Business Objectives and Responsibilities sections added
1.4		Alex N	15-Mar-22	Update to formatting

Distribution

Version	Destination	Upload Date	Location
1.1	Unity	aug-2017	Management Systems > Security Management Systems > Policies
1.2	Unity	feb-2018	Management Systems > Security Management Systems > Policies
1.3	Unity	jan-2021	Management Systems > Security Management Systems > Policies
1.4	Unity	Mar-2022	Management Systems > Security Management Systems > Policies

Company Information

Aus
29 Translink Drive
Keilor Park VIC
Australia 3042

t. (613) 8340 6100
f. (613) 9331 7121
info@commtelns.com
commtelns.com

CommTel Network Solutions Pty Ltd.
acn. 082 646 017
abn. 75 082 646 017

Policy Statement

CommTel Network Solutions ('CommTel') operates both in Australia and internationally delivering market-leading solutions in the communications industry. As an organisation that relies on technology, our responsibility for data protection, information security and infrastructure security is a critical priority to the Executive Management Team.

CommTel is committed to providing a security framework that ensures the protection of its people, information and infrastructure. People, information, information systems, information processing facilities, buildings and supporting infrastructure are all important assets which support the business in achieving its strategic objectives. They must be adequately protected through the application of proportionate and effective controls identified through effective risk management.

CommTel operates and maintains an ISO/IEC 27001-certified Security Management System ('SMS') to protect the identified assets from security risks related to the unauthorised access, loss, misuse or damage of these assets. The SMS contains the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving security within the context of the overall business objectives and risks of CommTel.

Business Objectives

This document, which has been authorised by CommTel's Executive Management Team ('EMT'), reflects the intentions of the EMT with regards to security, establishes related responsibilities and defines the guiding principles that define CommTel's approach to the protection of information assets.

By establishing an organisation-wide approach to security, CommTel aims to:

- Protect CommTel's business and reputation by preventing the compromise of security and the misuse of CommTel's data;
- Effectively manage all security threats in order to ensure business continuity, manage risk and maximise return on investment and business opportunities;
- Provide assurance to customers and other third parties with respect to the security of their information;
- Ensure that CommTel satisfies all of its legal, regulatory, contractual and ethical responsibilities with regard to its handling of sensitive and confidential data;
- Lead a change in the CommTel culture with respect to security by providing a foundation for improving information security within operational environments, greater information security awareness and aptitude and behavioural change within the working environment;
- Ensure the business objectives with regard to security are flowed down to the General Managers and all staff;
- Position CommTel with a competitive advantage by leveraging the ISO/IEC 27001 certification and be recognised as an industry leader.

System Requirements

ISO/IEC 27001 compliance is an important requirement for CommTel, specifically within its industries that include critical infrastructure and associated sensitive information. The key requirements of the SMS are to:

- Define and implement control mechanisms to protect CommTel information against misuse;
- Prescribe an effective mechanism for reporting and responding to information security incidents and real or perceived non-compliance with the Security Management System policies and procedures;
- Ensure that processes are in place to communicate the security framework and underlying principles to new and existing employees, agents, contractors;
- Define the procedures for maintaining the effectiveness of CommTel's security rules;
- Define the procedures for monitoring compliance to the Security Management System (SMS);
- Ensure CommTel's internal networks and systems are compliant with confidentiality, integrity and availability requirements of applicable legislation;
- Ensure that potential or actual breaches of CommTel's security policies are reported externally in line with applicable legislation;
- Ensure accountabilities and responsibilities are visible throughout CommTel.

CommTel takes a risk-based approach to security management by ensuring:

- Security requirements are understood and communicated through policy and procedures;
- Security-related risks are handled in a similar manner to other major business risks such as financial, legal and reputational;
- Risks associated with information assets are known and their impacts minimized within CommTel's risk appetite;
- Monitoring and reviewing is performed to measure the performance and effectiveness of the SMS;
- A process of continual review and improvement is applied based on objective measurement.

Responsibilities

It is the EMT's responsibility to promote the importance of security and risk management.

All CommTel staff, be they permanent, temporary, contract employed or engaged by CommTel, its subsidiaries or any third-party organisations whilst engaged on CommTel business must comply with all Security Policies and highlight any areas of non-compliance to their management.

All staff must report security breaches, whether actual or suspected, in accordance with CommTel's published Incident Management Procedure.

Robert Green
Chief Executive Officer

Gerald Molenkamp
Chief Technical Officer