INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

1.0 Introduction

This policy defines how Management Systems will be set up, managed, measured, reported on and developed within 21st Century.

21st Century has decided to pursue full certification to ISO/IEC 27001:2013 in order that the effective adoption of information security best practice may be validated by an external third party.

The purpose of this document is to define an overall policy with regard to management systems that is appropriate to the purpose of 21st Century, and includes:

- A framework for setting objectives
- A commitment to satisfying applicable requirements
- A commitment to continual improvement of the management systems

This Policy is available in electronic form and will be communicated within the organization and to all relevant stakeholders and interested third parties.

1.1 Reference documents

- ISO/IEC 27001 standard, clauses 4.2.1 (b) and A.15.1.1
- SEC Rules 204
- Information Security Risk Assessment and Risk Treatment Methodology
- Information Security Policy
- Business Continuity Policy
- Incident Management Policy

1.2 Our Policy Statement

21CTL establishes this policy to ensure that Information is protected against unauthorized access by maintaining Confidentiality, Integrity, Availability, Regulatory and legislative obligations, Business Continuity plans, Information security training, and to report and investigate all breaches of information security, actual or suspected.

2.0 ISMS Policy

2.1 Purpose, scope and users

The aim of this Policy is to define the purpose, direction, principles and basic rules that must be adhered to when dealing with all Information pertaining to 21st Century Technologies (21CTL).

The information created, processed and used by 21st Century Technologies Limited as well as non-public consumer information entrusted to 21st Century Technologies by its customers are among the Organization's most valuable assets. Given the competitive nature of 21st Century Technologies' businesses, along with the significant value of the resources it manages, the business and technology organizations/units must take all steps necessary to protect these assets. A compromise of these information assets could severely impact 21st Century Technologies customers, constitute a breach of laws and regulations and negatively affect the reputation and financial stability of the Organization. This Policy will help address these areas and provide the basis for an effective information security program.

This Policy is applied to the entire Information Security Management System (ISMS). Users of this document are all employees of 21CTL, contract workers and third parties contracted to provide services for 21st Century Technologies, as well as all external parties who have a role in the ISMS.

2.2 Requirements

A clear definition of the requirements for the Management Systems will be agreed and maintained with the business so that all activities is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements with regard to the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the 21st Century Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2.3 Top Management Leadership and Commitment

Commitment to the Management Systems extends to senior levels of the

organization and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the management systems and associated controls.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that objectives are being met and issues are identified through the audit programme and management processes. Management Review can take several forms including departmental and other management meetings.

2.4 Framework for Setting Objectives and Policy

The high-level objectives for the information security within 21st Century are defined within the document "Information Security Management System Context, Requirement and Scope". These are fundamental to the nature of the business and should not be subject to frequent change.

These overall objectives will used as guidance in the setting of lower level, more short-term objectives within an annual cycle timed to coincide with organizational budget planning. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the overall business requirements, informed by the annual management review with stakeholders.

ISMS objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on a quarterly basis to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001:2013 the control objectives and policy statements detailed in Annex A of the standard will be adopted where appropriate by 21st Century. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with 21CTL Information Security Risk Assessment and Treatment methodology.

2.5 Roles and Responsibilities

Within the field of Information Security Management, there are a number of key roles that need to be undertaken to ensure successful protection of the business from risk.

Full details of the responsibilities associated with each of the roles and how they are allocated within 21st Century are given in a separate document Roles,

Responsibilities and Authorities.

The Information Security Management System Manager shall have overall authority and responsibility for the implementation and management of the Management Systems, specifically:

- The identification, documentation and fulfilment of applicable requirements
- Implementation, management and improvement of risk management processes
- Integration of processes
- Compliance with statutory, regulatory and contractual requirements in the management of assets used to deliver products and services
- Reporting to top management on performance and improvement

2.6 Continual Improvement Policy

21st Century policy with regard to Continual Improvement is to:

- Continually improve the effectiveness of the ISMS across all areas within scope.
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001:2013.
- Achieve certification to the management systems and maintain them on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to the ongoing management of the ISMS.
- Make processes and controls more measurable in order to provide a sound basis for informed decisions.
- Achieve an enhanced understanding of and relationship with the business units to which the ISMS applies
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings with stakeholders and document them in a Continual Improvement Log
- Review the Continual Improvement Log at regular management meetings in order to prioritize and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be added to the 21CTL Continual Improvement Log and evaluated by the ISMS Manager.

As part of the evaluation of proposed improvements, the following criteria will be used:

- Cost
- Business Benefit
- Risk
- Implementation timescale
- Resource requirement

If accepted, the improvement proposal will be prioritized in order to allow more effective planning.

2.7 Approach to Managing Risk

A risk management strategy and process will be used which is line with the requirements and recommendations of the Management Systems. This requires that relevant assets are identified, and the following aspects considered:

- Threats
- Vulnerabilities
- Impact and likelihood before risk treatment
- Risk Treatment (e.g., reduction, removal, transfer)
- Impact and Likelihood after risk treatment
- Function responsible/Owner
- Timescale and Review Frequency

Risk management will take place at several levels within the ISMS, including:

- Management planning – risks to the achievement of objectives
- Information security and business continuity risk assessments
- Assessment of the risk of changes via the change management process
- At the project level as part of the management of significant business change

High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision. For more detail on the approach to risk assessment please review the documents "21CTL Information Security Risk Assessment and Treatment Methodology".

2.8 ISMS Team

21st Century will ensure that all staff involved in ISMS are competent on the basis of appropriate education, training, skills and experience.

The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill levels within 21st Century. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

2.9 Auditing and Review

Once in place, it is vital that regular reviews take place of how well the ISMS

processes and procedures are being adhered to. This will happen at three levels:

1. Structured regular management review of conformity to policies and procedures
2. Internal audit reviews against the management system standards by the 21st Century Audit Team
3. External audit against the standards in order to gain and maintain certification

2.10 Documentation Structure and Policy

All policies and plans that form part of the ISMS must be documented. This section sets out the main documents that must be maintained in each area.

Details of documentation conventions and standards are given in the Procedure for the Control of Documents and Records document.

A number of core documents has been created and will be maintained as part of the ISMS. They are uniquely numbered, and the current versions are tracked in 21CTL Documentation Log.

3.0 Sanction for Breaches

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to 21CTL assets, or an event which is in breach of 21CTL' security procedures and policies.

All 21CTL employees, operators in the capital market, partners, third Parties and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through an established Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access the Information Systems of 21CTL.

21CTL shall ensure that appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks are in place. In the case of an employee then the matter may be dealt with under the disciplinary procedures.

4.0 Managing Records

Use the table below to manage record kept in line with this policy:

Record name	Storage location	Person responsible for	Controls for record protection	Retention time

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Number of employees and external parties who have a role in the ISMS, but are not familiar with this document;
- Non-compliance of the ISMS policy with the laws and regulations, contractual obligations, and other internal documents of the organization;
- Ineffectiveness of ISMS implementation and maintenance;
- Unclear responsibilities for ISMS implementation.

5.0 Policy Review

This policy shall be reviewed at least annually to ensure effectiveness and continual application and relevance to the Company's business or as may be required.

6.0 Escalation

All policy breaches shall be escalated to the Information Security team for action.

7.0 Policy Exceptions & Retention

A policy exception represents a circumstance whereby an employee of 21CTL knowingly deviates from a requirement of the Policy. All Policy exceptions must be approved by the MD/CEO of 21CTL.

All documentation shall be maintained in accordance with the policy of 21CTL for Retention of Documents and Records or as regulation requires.