



Information Security Management Framework (ISMF) Policy

Version 1.0

February 2019

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
DOCUMENT CONTROL	ERROR! BOOKMARK NOT DEFINED.
DOCUMENT OWNER	ERROR! BOOKMARK NOT DEFINED.
DOCUMENT HISTORY.....	ERROR! BOOKMARK NOT DEFINED.
INTRODUCTION	4
OBJECTIVE	4
SCOPE.....	4
GENERAL RESPONSIBILITIES	4
GLOSSARY OF TERMS.....	4
STATEMENTS	5
MANAGEMENT COMMITMENT	5
CYBER SECURITY	5
INFORMATION SECURITY	6
GOVERNANCE.....	6
ASSET MANAGEMENT.....	7
RISK MANAGEMENT	8
DOCUMENTATION	8
COMMUNICATION	9
CONFORMANCE	10

DOCUMENT CONTROL

This is a controlled document.

All changes must be authorised by the document owner and tracked below.

DOCUMENT OWNER

Owner:	Robert Nathan
Phone:	1800 876 642
Email:	admin@cloudtronics.com.au

DOCUMENT HISTORY

Version	Date	Summary of changes
0.1	7 February 2019	Robert Nathan – Initial version.
1.0	8 February 2019	Approved by Robert Nathan.

INTRODUCTION

OBJECTIVE

This objective of the *Information Security Management Framework (ISMF) Policy* is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

SCOPE

This policy applies organisation-wide including:

- information created or received by the company in hardcopy or electronic form
- systems (e.g. hardware & software) used to store, process or transmit company information
- people accessing company information (employees, contractors and external parties)
- physical assets used to protect company information
- suppliers that store, process or transmit company information on behalf of the company

GENERAL RESPONSIBILITIES

Role	General responsibilities
Executive	<ul style="list-style-type: none">• Approve this policy and monitor performance
ISGC	<ul style="list-style-type: none">• Approve all other policies, standards and procedures
Managers	<ul style="list-style-type: none">• Apply policies and associated procedures on a risk-managed basis
All	<ul style="list-style-type: none">• Conform with company policies such as this and associated procedures• Report suspected or actual deviations to management: (e.g. via security@cloudtronics.com.au)

Further specific responsibilities are assigned in each policy.

GLOSSARY OF TERMS

Refer to the glossary of terms as required.

STATEMENTS


The *Information Security Management Framework (ISMF) Policy* addresses the following topics:

- Management commitment
- Cyber security
- Information security
- Governance
- Asset management
- Risk management
- Documentation
- Communication
- Accreditation
- Compliance

Other topics are addressed in complimentary policies, standards, guidelines and procedures.

MANAGEMENT COMMITMENT

The *Executive*:

Ref	Statement	
ISMF-1	Recognises that in order to achieve business objectives the organisation must ensure appropriate protection of its systems and information. <i>Note: Refer to ISO 27001 6.2.</i>	
ISMF-2	Sets clear business objectives that demonstrate the true value of security to the organisation and review them <u>annually</u> .	

CYBER SECURITY

The *Executive*:

Ref	Statement	
ISMF-3	Recognises digital networks and systems form the backbone of the business and are vital to the ability of the organisation to achieve its objectives.	

Management:

Ref	Statement	
ISMF-4	Deploys cyber security controls in order to operate online within acceptable levels of risk in response to identified threats and risks.	

The *CISO*:

Ref	Statement
ISMF-5	Operates (or ensures the effective operation of) cyber security measures including personnel security, physical security and IT security.

INFORMATION SECURITY

The *Executive*:

Ref	Statement
ISMF-6	Recognises information is vital and is stored, processed and transmitted by information systems that include people, processes and technology.
ISMF-7	Recognises information security involves ensuring information, in what-ever form (hardcopy or electronic), is suitably protected from information risks.

Management:

Ref	Statement
ISMF-8	Deploys information security controls in order to protect information in any form within acceptable levels of risk in response to identified threats and risks.


The *CISO*:

Ref	Statement
ISMF-9	Operates (or ensures the effective operation of) information security measures including personnel security, physical security and information security.


GOVERNANCE

The *Executive*:


Ref	Statement
ISMF-10	Is ultimately accountable for ensuring the organisation has implemented effective cyber and information security measures.
ISMF-11	Establishes an Information Security Governance Committee (ISGC) that concerns itself with the effective operation of cyber and information security.
ISMF-12	Appoints a Chief Information Security Officer (CISO) that helps set the direction for, implement and measure cyber and information security.
ISMF-13	Allocates sufficient resources to assist the CISO with implementing and operating cyber and information security effectively. Note: Sufficient resources includes employees dedicated to security, time for non-security employees to conform to security requirements along with hardware, software and services identified as current risk treatments.

ISMF-14	<p>Receives reporting on the performance of cyber and information security at least <u>quarterly</u> from the ISGC.</p> <p>Note: Reporting includes performance against the stated business objectives along with any notable incidents or issues, threats, risks or other environmental changes.</p>	
----------------	---	---

The *Information Security Governance Committee (ISGC)*:

Ref	Statement	
ISMF-15	<p>Receives reporting on the performance of cyber and information security at least <u>quarterly</u> from the CISO.</p> <p>Note: Reporting includes performance against the stated business objectives along with any notable incidents or issues, threats, risks or other environmental changes.</p>	
ISMF-16	Takes steps to proactively manage the cyber and information security program by recording minutes including actions and tracking progress.	

The *CISO*:

Ref	Statement	
ISMF-17	Prepares the agenda and minutes (or arranges for them to be prepared) for the ISGC at least <u>quarterly</u> .	

ASSET MANAGEMENT

Management:

Ref	Statement	
ISMF-18	<p>Identifies the organisation's critical assets in an Information Asset Register.</p> <p>Note: The Information Asset Register includes:</p> <ul style="list-style-type: none"> • information created or received by the organisation • format (electronic or hardcopy) • the location where the information is stored, processed or transmitted • any relevant suppliers • owner • classifications (in terms of Confidentiality, Integrity and Availability) • retention time 	
ISMF-19	<p>Assigns owners to information assets in the Information Asset Register.</p> <p>Note: Owners are responsible for managing risk associated with the asset and ensuring appropriate cyber and information security measures are in place.</p>	
ISMF-20	<p>Classifies assets in the Information Asset Register in order to know what to protect and how much to protect it.</p> <p>Note: Classification is performed in terms of Confidentiality, Integrity and Availability using a traffic light approach (Low, Medium and High).</p>	

ISMF-21	Reviews the asset register including classifications after significant change or at least <u>annually</u> .
----------------	---



The *CISO*:

Ref	Statement
ISMF-22	Performs (or assists with the performance of) asset management by facilitating asset identification (including owners and locations) along with classification.

RISK MANAGEMENT

Management:

Ref	Statement
ISMF-23	Identifies important risks in an Information Risk Register. Note: The Information Risk Register includes: <ul style="list-style-type: none"> • description • impacted assets (systems or information) • existing controls • initial assessment of likelihood, consequence and risk rating • risk owner • risk treatment decision (i.e. accept, mitigate, transfer or avoid) • risk treatment owner • status
ISMF-24	Identifies, evaluates and treats risks consistent with the industry standard for risk management (i.e. ISO 31000) in order to know how much to protect assets.
ISMF-25	Identifies owners to review and approve the status of associated risks including any treatment plans intended mitigate risk.
ISMF-26	Reviews the status of open risks after significant change (e.g. treatment or changes to the environment) or at least <u>annually</u> .




The *CISO*:

Ref	Statement
ISMF-27	Performs (or assists with the performance of) risk management by facilitating risk identification including owners, assessments and treatment plans.


DOCUMENTATION

The *CISO*:

Ref	Statement
-----	-----------


ISMF-28	Develops information security policies, standards, guidelines and procedures based on ISO 27001 to operationalise the information security program.	
ISMF-29	Maintains control of information security policies, standards and procedures with document owners, change history, reviews and approvals.	
ISMF-30	Reviews and updates as necessary all published policies at least <u>annually</u> .	

The *ISGC*:

Ref	Statement	
ISMF-31	Reviews and approves all published policies at least <u>annually</u> .	

COMMUNICATION


The *Executive*:

Ref	Statement	
ISMF-32	Communicates its commitment to cyber & information security policy by approving the <i>Information Security Management Framework (ISMF) Policy</i> at least <u>annually</u> .	
ISMF-33	Communicates on behalf of the organisation with external parties such as customers, suppliers, regulators and law enforcement when required.	

Management:

Ref	Statement	
ISMF-34	Communicates its management of cyber & information security measures through records rated to ongoing asset management and risk management.	

The *ISGC*:

Ref	Statement	
ISMF-35	Communicates with managers to ensure effective management of cyber & security measures through <u>quarterly</u> ISGC meetings.	

The *CISO*:

Ref	Statement	
ISMF-36	Disseminates relevant security advisories relating to current threats, vulnerabilities, risks, weaknesses and associated mitigation advice as necessary.	
ISMF-37	Incorporates important messages requiring reinforcement into security awareness training activities. Note: This includes the need to report suspected or actual deviations (e.g. via security@cloudtronics.com.au).	

All:

Ref	Statement
ISMF-38	Report suspected or actual deviations to management: (e.g. via security@cloudtronics.com.au)

CONFORMANCE

The *CISO*:

Ref	Statement	
ISMF-39	Maintains artefacts that demonstrate the effective operation of security measures and record any identified gaps as an Issue. Note: Artefacts include 'Statements of Applicability' for relevant standards, Information Asset Register, Information Risk Register, Issue Register along with technical information (configurations and system event logs).	
ISMF-40	Identifies important issues in an Issue Register. Note: Issues may be: <ul style="list-style-type: none"> • relevant vulnerabilities and weaknesses • non-conformances to policies, standards or procedures • measurement results that do not meet defined thresholds • impediments to achieving business objectives • audit results • opportunities for improvement • feedback from interested parties Note: The Issue Register includes: <ul style="list-style-type: none"> • description • impacted assets (systems or information) • reported by and date/time • reported to (ISGC, customer, externally) and date/time • status 	
ISMF-41	Reviews operations including systems and behaviours against compliance requirements (i.e. policies, standards and procedures) at least <u>annually</u> . Note: This include technical review of systems against expected configurations. This may include elements of configuration management, penetration testing, internal audits and external audits.	

The *ISGC*:

Ref	Statement	
ISMF-42	Seeks and receives advice on relevant cyber & information security legislation, regulation and or agreements at least <u>annually</u> . Note: This include privacy, confidentiality and sub-contracting measures.	