



Information Security Issue Management (ISIM) Policy

Version 1.0

February 2019

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
DOCUMENT CONTROL	3
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
PREPARING FOR CYBER SECURITY INCIDENTS.....	5
TRIAGING SECURITY ISSUES	6
RECORDING SECURITY ISSUES	6
REPORTING OF ISSUES	6
CONTAINING SECURITY ISSUES.....	7
RESPONDING TO SECURITY ISSUES	7
REVIEWING SECURITY ISSUES	9

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 Issue Management (ISIM) Policy* is to ensure a consistent and effective approach to the management of information security issues, including incidents.

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 the Information Security Management Framework (ISMF) policy and monitor performance
ISGC	<ul style="list-style-type: none">• Approve this and 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 Issue Management (ISIM) Policy* addresses the following topics:

- Triaging security issues
- Recording security issues
- Reporting of issues
- Containing security issues
- Responding to security issues
- Reviewing security issues

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

PREPARING FOR CYBER SECURITY INCIDENTS

The *CISO*:

Ref	Statement	
ISIM-1	<p>Takes steps to prevent cyber security incidents as described in information security policies, standards and procedures.</p> <p>Note: Steps include:</p> <ul style="list-style-type: none"> • Checking that critical controls necessary to prevent and detect cyber and information security incidents are in place and raise issues and/or risks where they are not • Undertaking the necessary training to ensure skills are maintained for identifying and responding to cyber and information security incidents • Maintaining a list of key contacts that may be required in the event of a cyber and information security • Communicating the requirement for all staff to report information security incidents to the CISO throughout the organisation 	
ISIM-2	Ensures that a test of the cyber & information security incident readiness is carried out at least <u>annually</u> to improve preparedness.	

TRIAGING SECURITY ISSUES

The *CISO*:

Ref	Statement
ISIM-3	<p>Reviews each report of a security issue and confirms whether it is an actual security incident or a 'false positive'.</p> <p>Note: Issues may be:</p> <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

RECORDING SECURITY ISSUES

The *CISO*:

Ref	Statement
ISIM-4	<p>Records all confirmed security issues in the information security Issues Register.</p> <p>Note: The Issue Register includes:</p> <ul style="list-style-type: none"> • description of the incident • type of incident (e.g. malware, leakage, denial of service) • impacted assets (systems or information) • reported by and date/time • reported to (ISGC, customer, externally) and date/time • status

REPORTING OF ISSUES

The *CISO*:

Ref	Statement
ISIM-5	Reports all confirmed and significant security issues to the Executive immediately.
ISIM-6	Reports all confirmed and non-significant security issues to the Executive in quarterly reporting via the ISGC.

ISIM-7	<p>Evaluates the need to notify external stakeholders (e.g. customers, suppliers, OAIC, police, ASD and/or ACORN) in conjunction with the Executive.</p> <p>Note: OAIC – The Office of the Australian Information Commissioner is to be notified of ‘significant’ breaches of personal information.</p> <p>Note: ACORN – The Australian Cybercrime Online Reporting Network may be notified of (potentially) criminal security incidents.</p> <p>Note: Australian Government departments and agencies are obligated to report security incidents to the Australian Signals Directorate.</p>	
---------------	---	--

The Executive:

Ref	Statement	
ISIM-8	Reports all confirmed significant security incidents to external stakeholders (or authorises the CISO or another executive to do so).	

CONTAINING SECURITY ISSUES

The *CISO*:

Ref	Statement	
ISIM-9	<p>Evaluates the possibility of containing security issues by isolating impacted systems.</p> <p>Note: To maintain the availability of critical systems (often servers), it may be necessary to disconnect affected systems from the network (if they are not essential) such as workstations or less critical servers. It may also be possible to logically isolate systems on the network to allow nothing other than remediation.</p> <p>Note: To maintain the integrity of evidence avoid powering down impacted systems unless it is necessary to maintain the availability of critical systems (because this will void the ability to recover evidence from volatile memory).</p>	

RESPONDING TO SECURITY ISSUES

The *CISO*:

Ref	Statement	
ISIM-10	Responds to security issues with management approved actions.	
ISIM-11	Determines whether it is necessary to execute the Business Continuity Plan.	
ISIM-12	Determines whether it is necessary to call in specialist cyber security incident response specialists (including forensic specialists).	

ISIM-13	<p>For a Distributed Denial of Service (DDoS) incident, consider the following steps for inclusion in the response:</p> <ul style="list-style-type: none">• Contact your Internet Service Provider (ISP) to provide information and execute available options for blocking the attack upstream• Determine whether capacity can be added to the service being targeted to meet the demand (more likely in public cloud environments)• If all other options fail, consider changing the IP address of the service, however this will not help if DNS is being used (this is best performed in conjunction with a migration behind DDoS protection services) <p>Note: A Denial of Service (DoS) attack exploits a vulnerability or consumes excessive capacity on the target network or computer system(s) to render it unable to service authorised users. A Distributed DoS (DDoS) relies on a collection of distributed computers, often called a botnet, to assist in consuming excessive capacity on the target network or computer system(s).</p>	ISM
ISIM-14	<p>For a malware incident, consider the following steps for inclusion in the response:</p> <ul style="list-style-type: none">• Transfer audit logs to secure media (for evidence preservation)• Remove (isolate) impacted systems from the network• Disable backup scheduled tasks to avoid backing up corrupted/encrypted files• Scan the network and connected media for malware• Liaise with antimalware vendor to obtain updated signatures• Change passwords potentially accessible to the malware• Communicate appropriate details of the incident to users• Recover files from backup only once the malware has been eradicated• Recover operating systems from known good backups where possible• Reinstate backup scheduled tasks <p>Note: Malicious software (malware) includes viruses, worms, Trojans, spyware and ransomware, and aims to harm the operation of computer systems.</p> <p>Note: It is NOT recommended to pay ransoms because provision of the encryption key is not guaranteed and it encourages the behaviour.</p> <p>Note: Do NOT connect your offline backups to the network until the malware is eradicated or the backups may be corrupted or encrypted.</p>	ISM

ISIM-15	<p>For a data loss, leak or spill incident, consider the following steps for inclusion in the response:</p> <ul style="list-style-type: none"> • Do not immediately delete the information (if it remains accessible), first seek authorisation and consider the need to preserve evidence • Do not unnecessarily copy and proliferate the information (e.g. by printing or emailing records) • Quarantine the system or suspected original files by removing access (this helps to maintain the integrity of evidence such as last modified details) • Assume the information is compromised, conduct damage assessment and mitigate issues likely to result from public disclosure of the information • If the breach relates to cryptographic key material ensure relevant cryptographic key custodians are notified, i.e. SecureWorx CISO and relevant Customer(s) • Engage the <i>Executive</i> if disciplinary proceedings are required <p>Note: A data loss, leak or spill is the unauthorised release or disclosure of information. Typically, this involves the unauthorised transfer of sensitive information outside of the organisations control.</p>	ISM
ISIM-16	<p>Do not allow an intrusion to continue in order to seek further information or evidence unless authorisation has been obtained from legal advisors.</p> <p>Note: The relevant act is the Telecommunications (Interception and Access) Act 1979 (the TIA Act).</p>	ISM
ISIM-17	Maintains documented records of the actions taken and the results.	
ISIM-18	Regularly updates the Executive with the status of any significant security incident and actions.	

REVIEWING SECURITY ISSUES

The *CISO*:

Ref	Statement	
ISIM-19	A week to a month after the closure of a significant security incident, hold a Post Incident Review (PIR) to ensure impacted systems have returned to normal operations and to identify any lessons learnt.	
ISIM-20	Reviews trends with security issues at least <u>annually</u> and takes corrective actions in conjunction with the ISGC.	
ISIM-21	Refines the organisation's approach to cyber and information security to prevent new, evolving and/or reoccurring cyber and information security incidents.	