IT Operations Security (ITOS) Policy

Version 1.0

February 2019

TABLE OF CONTENTS

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 *IT Operations Security (ITOS) Policy* is to ensure the correct and secure operation of information processing facilities.

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	• Approve the Information Security Management Framework (ISMF) policy and monitor performance
ISGC	• Approve this and other policies, standards and procedures
Managers	• Apply policies and associated procedures on a risk-managed basis
All	• 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 *IT Operations Security (ITOS) Policy* addresses the following topics:

- Standard operating procedures
- IT change and capacity management
- Anti-malware controls
- Email security
- Web security
- Backup
- Security event management
- Technical vulnerability management
- Cryptographic key management

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

STANDARD OPERATING PROCEDURES

The *IT Manager*:

Ref	Statement	
ITOS-1	Maintains standard operating procedures to bring consistency and reliability to the delivery of IT services and operation of security controls. Note: IT processes are often based on IT Service Management (ITSM).	
ITOS-2	Reviews and updates as needed standard operating procedures for security activities after major change or at least annually. Note: Security standard operating procedures include procedures for: • Access management • Change management • Anti-malware management • Backup management (including recovery and testing) • Security event management • Vulnerability management • Cryptographic key management • Network, operating system, database and application management • Secure coding • Security testing • Media and information handling • Security incident management	

IT CHANGE AND CAPACITY MANAGEMENT

The *IT Manager*:

Ref	Statement

ITOS-3	Controls changes to systems including documented change requests, effective testing, back-up out plans, authorisation and communication.	
ITOS-4	Reviews and approves documented change requests with consideration to necessity and risk.	
ITOS-5	Reviews the current utilisation of resources (e.g. storage, memory, CPU etc) and forecasts requirements at least annually.	

ANTI-MALWARE CONTROLS

The *IT Manager*:

Ref	Statement	
ITOS-6	Employs anti-malware controls to detect, prevent, contain and recover from malware infections including ransomware.	
ITOS-7	Check the status of anti-malware control deployment to systems including coverage, currency (up-to-date) and any identified threats at least quarterly. Note: This check includes Network Intrusion Prevention Systems (NIPS) and Host Intrusion Prevention Systems (HIPS) in addition to traditional antivirus software.	
ITOS-8	Employs application white-listing to limit the execution of applications on assets to known good (i.e. approved) applications.	***ISM***
ITOS-9	Disables untrusted Microsoft Office macros by allowing only macros from controlled trusted locations and digitally signed macros. Note: For further information refer to the associated advisory from ASD: https://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf	***ISM***
ITOS-10	Applies user application hardening by blocking web browser access to Adobe Flash player (uninstall if possible), web advertisements and untrusted Java code on the internet.	***ISM***

EMAIL SECURITY

The *IT Manager*:

Ref	Statement	
ITOS-11	Enable anti-spam and anti-malware email filtering to protect the corporate email service from junk and malicious emails.	
ITOS-12	Enable Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and DMARC email security protocols. Note: These email security protocols reduce the opportunity for attackers to spoof messages i.e. send email appearing to be on behalf of the organisation.	
ITOS-13	Apply protective markings to email contents (including attachments) that accurately reflect the sensitivity/classification of the contents.	***ISM***

ITOS-14	Enable filtering of inbound emails such that unmarked and unrecognised emails are reviewed, and the intended recipient is notified.	***ISM***
ITOS-15	Enable filtering of outbound emails with a protective marking that exceeds the classification of the path over which the email would be transmitted.	***ISM***
ITOS-16	Make use of opportunistic Transport Layer Security (TLS) when sending or receiving emails over public network infrastructure.	

WEB SECURITY

The *IT Manager*:

Ref	Statement	
ITOS-17	Enable web filtering to protect the corporate web service from websites hosting malicious content.	
ITOS-18	Enable website content filtering by categorising websites and approving/rejecting access to categories as appropriate.	
ITOS-19	Enable Content-Security-Policy to achieve secure HTTP headers for public facing websites. Note: Content-Security-Policy helps to prevent Cross Site Scripting (XSS) attacks.	

BACKUP

The *IT Manager*:

Ref	Statement	
ITOS-20	Performs backup of all important systems and information on a daily basis. Note: Known good standard builds that can be redeployed should be used for operating systems in place of backups of systems where possible.	
ITOS-21	Stores backups securely offline. Note: Offline may be on electronic media which is disconnected from any network, or otherwise isolated in a manner that prevents erasure.	***ISM***
ITOS-22	Checks the status of backups at least quarterly including a test restore.	

ELECTRONIC MEDIA HANDLING

The *CISO*:

Ref	Statement	
ITOS-23	Maintains a register of all electronic storage devices used to store information with a Medium or High confidentiality rating.	

ITOS-24	Approves the use of electronic storage devices used to store information with a Medium or High confidentiality rating. Note: Company issued laptops with whole disk encryption enabled are approved for general use including the storage of information with a Medium or High confidentiality rating. Note: On a case by cases basis portable storage devices will be reviewed and approved to enable a temporary transfer of information. Any devices used to transfer Medium or High confidentiality rating require encryption.	***ISM***

MOBILE DEVICE MANAGEMENT

The *IT Manager*:

Ref	Statement	
ITOS-25	Maintains a mobile device management (MDM) solution to enforce the cyber & information security policies and standards on mobile devices used to store or access corporate information. Note: The built-in MDM for Office365 is considered acceptable to enable access to emails, address books, calendars and documents.	***ISM***

SECURITY EVENT MANAGEMENT

The *IT Manager*:

Ref	Statement	
ITOS-26	Establishes a consistent time source for all systems using the Network Time Protocol (NTP) and reliable internet based (or GPS) time servers.	

ITOS-27	Centrally logs all important system events logs and automatically alerts when acceptable thresholds are exceeded. Note: Important system event logs include: • Authentication (logon) attempts - All successful and failed authentication attempts are logged including system logon and privileged escalation (e.g. "Run as" and "sudo"). • Privileged command execution - The event that occur whereby a user switches from standard to privileged operation (i.e. "Run as" and "sudo") and all subsequent privileged command use. • Access control (user, group) changes - All modification to access control configuration including create, update and delete functions on users, groups and privileges. • Security alerts and failures - All security alerts and failure events produced by the source (e.g. record not found, system failure, bad read/write, out of memory). • Configuration changes - All changes to configuration of operating systems, applications and databases (e.g. file paths, thresholds, allocated disk space, schemas). • Changes to critical files - All changes to critical files (e.g. log files, system files, application code, sensitive documents, sensitive database records or fields). • Information flows - All imports and exports of sensitive information (e.g. source code, classified information, personal information, credit card numbers). • Information correlation - All access to aggregate data that summarises attributes of a sensitive data set or combines data for analytical or research purposes.	
ITOS-28	Configures alerts that notify when acceptable thresholds are exceeded are responded to immediately in accordance with the Information Security Issue Management Policy. Note: When security violations are observed, the Information Security Issue Management Policy is followed.	
ITOS-29	Protects the integrity of the logging system and event information. Note: The integrity of the logging system and events can be protected with: • restricted access • access logging • cryptographic hashing (signing) of events • storage and transit encryption • extraction of reports • other relevant controls documented in policies	
ITOS-30	Retains metadata for 7 years and content for 2 years by default and 7 years if the content forms the basis of an investigation. Note: Metadata is the information associated with a security event (e.g. date and time, description, source, location) and content is 'payload' (e.g. email body or attachment, webpage, document, database record change, audio or video).	

ITOS-31	Checks the status of the security event management system, including acceptable thresholds for security events and trends, at least annually. Note: Event are monitored: • in real-time by the Security Information and Event Management (SIEM) platform in accordance with defined rules and thresholds • by analysts that check the SIEM platform on at least quarterly basis to ensure the rules are sufficient, up-to-date & performing as expected • as a part of scheduled penetration tests • as a part of the security program assessments (IRAP assessments and ISO 27001 internal audits) Note: When security violations are identified, the Information Security Issue Management Policy is followed.	

TECHNICAL VULNERABILITY MANAGEMENT

The *IT Manager*:

Ref	Statement	
ITOS-32	Maintains Standard Operating Environments (SOE) for workstations and servers that incorporate suitable security hardening. Note: The SOE includes up-to-date operating system with all unnecessary features and accounts removed, Macro security, anti-malware controls (including application white-listing), access controls and centralised logging.	
ITOS-33	Subscribes to information that identifies relevant vulnerabilities and available patches associated with hardware, firmware and software (operating systems, databases, applications and libraries). Note: Advisories are available from vendors and CERT organisations.	
ITOS-34	Applies all relevant extreme risk / critical patches within 48 hours. Note: Extreme risk / critical patches are categorised as such by the Cloudtronics CISO and usually relate to publicly accessible systems with a remotely exploitable vulnerability for which public exploit code is known to exist.	***ISM***
ITOS-35	Applies all relevant high-risk patches within 2 weeks. Note: High-risk vulnerabilities and patches are categorised as such by the Cloudtronics CISO and usually relate to publicly accessible or critical internal systems with a remotely exploitable vulnerability.	***ISM***
ITOS-36	Applies all other applicable patches within 4 weeks.	***ISM***

ITOS-37	When patches are not available for security vulnerabilities, implements one or more of the following approaches:
	• resolve the security vulnerability by either:
	  ○ disabling the functionality associated with the security vulnerability
	  ○ asking the vendor for an alternative method of managing the security vulnerability
	  ○ moving to a different product with a more responsive vendor
	  ○ engaging a software developer to resolve the security vulnerability.
	• prevent exploitation of the security vulnerability by either:
	  ○ applying external input sanitisation (if an input triggers the exploit)
	  ○ applying filtering or verification on output (if the exploit relates to an information disclosure)
	  ○ applying additional access controls that prevent access to the security vulnerability
	  ○ configuring firewall rules to limit access to the security vulnerability.
	• contain exploitation of the security vulnerability by either:
	  ○ applying firewall rules limiting outward traffic that is likely in the event of an exploitation
	  ○ applying mandatory access control preventing the execution of exploitation code
	  ○ setting file system permissions preventing exploitation code from being written to disk.
	• detect exploitation of the security vulnerability by either:
	  ○ deploying an intrusion detection system
	  ○ monitoring logging alerts
	  ○ using other mechanisms for the detection of exploits using the known security vulnerability.
		ISM

ITOS-38	Checks the status of software patches at least quarterly through the use of patch management tools.	
ITOS-39	Checks status of software vulnerabilities (infrastructure and applications) at least quarterly through the use of vulnerability management tools.	

CRYPTOGRAPHIC KEY MANAGEMENT

The *IT Manager*:

Ref	Statement	
ITOS-40	Maintains a register of cryptographic key material. Note: Private keys are stored securely in an electronic password vault.	
ITOS-41	Uses automatic key negotiation protocols where possible. Note: This includes managed services such as AWS Certificate Management Services and software such as certbot.	

ITOS-42	Transports commercial grade cryptographic equipment in an unkeyed state where possible. Note: When necessary, commercial grade cryptographic equipment is transported in a keyed state and handled commensurate with its classification.	***ISM***
ITOS-43	Reviews the register of cryptographic key material at least annually in order to identify keys that need to be renewed or revoked.	
ITOS-44	Revokes keying materials or certificates when they are suspected of being compromised.	***ISM***