cloudtronics

Acceptable Use Policy (AUP)

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 *Acceptable Use Policy (AUP)* is to ensure that employees, contractors and supplier users understand their responsibilities.

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 people	• 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 *Acceptable Use Policy (AUP)* addresses the following topics:

- General responsibilities
- Inappropriate content
- Intellectual property
- Information classification
- Information handling
- Media handling
- Computer hygiene
- Mobile devices
- Personal use
- Other unauthorised uses
- Monitoring
- Misconduct
- Suspected or actual issues

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

GENERAL RESPONSIBILITIES

You are expected to:

Ref	Statement	
AUP-1	Maintain professional standards and adhere to all relevant codes of conduct/ethics.	
AUP-2	Participate in an introductory information security awareness program at commencement of employment.	
AUP-3	Participate in an up-to-date information security awareness program at least annually.	⏰

INAPPROPRIATE CONTENT

You are expected to:

Ref	Statement	
AUP-4	Avoid accessing or distributing inappropriate content. Note: Inappropriate content includes: • illegal content • sexual or pornographic content • content that promotes or encourages racism or intolerance • content that appears harassing, degrading, intimidating or threatening • any other objectionable material.	

INTELLECTUAL PROPERTY

You are expected to:

Ref	Statement
AUP-5	Adhere to all relevant software licensing agreements and copyright laws. Note: Do not illegally share copyright protected media.

INFORMATION CLASSIFICATION

You are expected to:

<table>
<tr><th>Ref</th><th>Statement</th></tr>
<tr><td>AUP-6</td><td>Classify business information in accordance with information classification procedures as defined in the following table:
<table>
<tr><th>Type</th><th>Classification</th><th>Description</th></tr>
<tr><td>Confidentiality</td><td>Low</td><td>Unauthorised disclosure could be expected to cause no to insignificant harm/damage to operations or individuals.</td></tr>
<tr><td>Confidentiality</td><td>Medium</td><td>Unauthorised disclosure could be expected to cause limited harm/damage to operations or individuals.</td></tr>
<tr><td>Confidentiality</td><td>High</td><td>Unauthorised disclosure could be expected to cause major harm/damage to operations or individuals.</td></tr>
<tr><td>Integrity</td><td>Low</td><td>Unauthorised modification could be expected to cause no to insignificant harm/damage to operations or individuals.</td></tr>
<tr><td>Integrity</td><td>Medium</td><td>Unauthorised modification could be expected to cause limited harm/damage to operations or individuals.</td></tr>
<tr><td>Integrity</td><td>High</td><td>Unauthorised modification could be expected to cause major harm/damage to operations or individuals.</td></tr>
<tr><td>Availability</td><td>Low</td><td>Unavailability of the system could be expected to cause no to insignificant harm/damage to operations or individuals.</td></tr>
<tr><td>Availability</td><td>Medium</td><td>Unavailability of the system could be expected to cause limited harm/damage to operations or individuals.</td></tr>
<tr><td>Availability</td><td>High</td><td>Unavailability of the system could be expected to cause major harm/damage to operations or individuals.</td></tr>
</table>
</td></tr>
</table>

INFORMATION HANDLING

You are expected to:

<table>
<tr><th>Ref</th><th>Statement</th></tr>
<tr><td><b>AUP-7</b></td><td>Handle business information in accordance with secure handling procedures as described in the following table:
<table>
<tr><th>Type</th><th>Classification</th><th>Description</th></tr>
<tr><td><b>Access</b></td><td><b>Low</b></td><td>Staff approve access or release</td></tr>
<tr><td><b>Access</b></td><td><b>Medium</b></td><td>Manager approves access or release[1]</td></tr>
<tr><td><b>Access</b></td><td><b>High</b></td><td>Executive approves access or release[2]</td></tr>
<tr><td><b>Storage</b></td><td><b>Low</b></td><td>No encryption required</td></tr>
<tr><td><b>Storage</b></td><td><b>Medium</b></td><td>Use AACAs</td></tr>
<tr><td><b>Storage</b></td><td><b>High</b></td><td>Use AACAs</td></tr>
<tr><td><b>Transit</b></td><td><b>Low</b></td><td>No encryption required</td></tr>
<tr><td><b>Transit</b></td><td><b>Medium</b></td><td>Use AACPs and AACAs</td></tr>
<tr><td><b>Transit</b></td><td><b>High</b></td><td>Use corporate VPN service</td></tr>
<tr><td><b>Disposal</b></td><td><b>Low</b></td><td>No sanitisation or destruction required</td></tr>
<tr><td><b>Disposal</b></td><td><b>Medium</b></td><td>Sanitise or destroy prior to disposal</td></tr>
<tr><td><b>Disposal</b></td><td><b>High</b></td><td>Sanitise or destroy prior to disposal</td></tr>
</table>
Note 1: Discuss only in a secure area.
Note 2: Discuss only in a secure area – do not discuss on the telephone.
Note: The AACAs and AACPs can be found in the Australian Government Information Security Manual (ISM) as follows:
https://www.asd.gov.au/infosec/ism
Note: Sanitisation of electronic media will occur through the destruction of cryptographic keys used to decrypt encrypted information.
Note: Destruction will occur via shredding, incineration or Executive approved destruction service provider. Destruction services will hold a National Association for Information Destruction AAA Certification with High security endorsement or Paper/printed media (same day destruction) endorsement</td></tr>
<tr><td><b>AUP-8</b></td><td>Maintain environmental awareness to prevent unauthorised disclosure of sensitive information by avoiding:
• Sensitive conversations being overheard (by visitors or in public)
• Reading sensitive documents in unsecure areas (by visitors or in public)
• Projecting documents or displays such as computer monitors & projector screens outside (or in some cases beyond meeting rooms)
• Projecting documents or displays such as computer monitors & projector screens via webcams used in videoconferencing</td></tr>
</table>

MEDIA HANDLING

You are expected to:

Ref	Statement	
AUP-9	Use only electronic media to store company information with a Medium or High confidentiality classification rating that has been approved by the CISO in accordance with the IT Operations Security Policy.	
AUP-10	Only store information on portable electronic media on a temporary basis and ensure all critical data is backed up regularly.	
AUP-11	Report lost or stolen electronic media to the CISO via email to security@cloudtronics.com.au.	

COMPUTER HYGIENE

You are expected to:

Ref	Statement	
AUP-12	Maintain effective computer hygiene and avoid malware. Note: Good computer hygiene includes: • showing caution and avoiding phishing attacks when reading emails, clicking on links and opening attachments • avoiding the installation, execution or use of software including cloud services unless approved by the Executive • maintaining the physical condition of physical assets and avoiding loss or theft • protecting passwords and tokens	
AUP-13	Lock your computer screen (and mobile devices) when unattended or otherwise not in use.	
AUP-14	Avoid connecting to untrusted networks or inserting unknown removable media. Note: If you need to connect to an untrusted network and communicate, connect to the corporate VPN service.	

MOBILE DEVICES

You are expected to:

Ref	Statement	
AUP-15	Enrol personal mobile devices in the company MDM solution if using them to store or access corporate information with a Medium or High confidentiality rating.	***ISM***

AUP-16	Ensure mobile devices are configured to remain undiscoverable to all other Bluetooth devices except during pairing if using them to store or access corporate information with a Medium or High confidentiality rating. Note: Also ensure Bluetooth pairing is performed so that a connection is only made to the device intended and remove pairings no longer required.	***ISM***
AUP-17	Change all passphrases associated with a mobile device upon returning from overseas. Note: Further information about traveling overseas with an electronic device can be found as follows: https://www.asd.gov.au/publications/protect/electronic_devices_os_travel.htm	***ISM***
AUP-18	Report lost or stolen mobile devices to the CISO via email to security@cloudtronics.com.au. Note: The CISO will remotely erase the device.	***ISM***

PERSONAL USE

You are expected to:

Ref	**Statement**	
AUP-19	Ensure personal use is limited, appropriate and conducted with the consent of your manager. Any personal use must: • be reasonable i.e. not excessively consume resources or occupy time • is appropriate i.e. not relate to inappropriate content or infringe intellectual property laws • not impact your work or the work of others • does not relate to another business unless approved by the Executive • embarrass or in anyway harm the organisation, its staff or assets	

OTHER UNAUTHORISED USES

You are expected to:

Ref	Statement	
AUP-20	Avoid other unauthorised uses of the organisational assets including: • sharing information including credentials or authenticated sessions with unauthorised persons • using credentials that protect the organisational assets for personal or other purposes • using unauthorised hardware for the storage of sensitive organisational information (Medium or High) • connecting unauthorised hardware to the organisational systems unless approved by the Executive to do so • exploiting weaknesses in the organisational assets unless approved by the Executive to do so • intercepting traffic, probing and scanning organisation assets unless approved by the Executive to do so • concealing your identity when using organisational systems unless approved by the Executive to do so • removing assets from approved facilities unless approved by the Executive to do so.	

MONITORING

You are expected to:

Ref	Statement	
AUP-21	Understand and accept that the use of company assets is logged and monitored to aid compliance with policies, standards and procedures.	

MISCONDUCT

You are expected to:

Ref	Statement	
AUP-22	Understand and accept non-conformance with policies, standards and procedures may result in termination of employment or any relevant service contract, and/or referral to law enforcement.	

SUSPECTED OR ACTUAL ISSUES

You are expected to:

Ref	Statement

AUP-23	Report suspected or actual security violations including vulnerabilities and weaknesses to the CISO via email to security@cloudtronics.com.au.	