



Identity and Access Management (IDAM) 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
IDENTITY VERIFICATION.....	5
AUTHENTICATION.....	5
AUTHENTICATION TYPES	6
PASSWORDS.....	6
TWO FACTOR AUTHENTICATION.....	7
ACCESS	7
ACCESS REVIEWS	8
ACCESS REMOVAL.....	8

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 *Identity and Access Management (IDAM) Policy* is to ensure employees, contractors and any suppliers have the right access to information.

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 *Identity and Access Management (IDAM) Policy* addresses the following topics:

- Identity verification
- Authentication
- Regular access
- Remote access
- Privileged access
- Access reviews
- Access removal

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

IDENTITY VERIFICATION

The *Manager*:

Ref	Statement
IDAM-1	<p>Verifies, at commencement of employment, the identify of new staff and contractors using:</p> <ol style="list-style-type: none"> 1. the Australian Government National Identity Proofing Guidelines (to a level 3/High/Silver or level 4/Very High/Gold standard), or 2. the older '100 point check' of identity evidence <p>Note: The National Identity Proofing Guidelines can be found as follows: https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Identity-security-guidelines-and-standards.aspx</p> <p>Note: The older '100 point check' can be found as follows: https://www.homeaffairs.gov.au/Licensing/Documents/100-points-identification-guidelines.pdf</p>

System Managers:

Ref	Statement
IDAM-2	<p>Ensure a standard naming convention is used for all account names that helps to ensure all access is uniquely attributable to a user or automated system function.</p> <p>Note: A standard naming convention can be based on the name of the user or an employee ID or similar.</p> <p>Note: All account names includes both interactive people accounts and non-interactive system accounts.</p>

AUTHENTICATION

System Managers:

Ref	Statement
IDAM-3	Require access to internal systems and information to be controlled through an authentication mechanism that confirms a user is who they say they are. Note: By their very nature public systems and information do not necessarily require authentication but at least require authentication for privileged access.
IDAM-4	Use Single or Simplified Sign On (SSO) or Federation to reduce the number of interactive authentications a user is required to perform is encouraged.
IDAM-5	Configure session and/or screensaver locks (where possible) that activate after 15 minutes of inactivity or upon manually activation by a user.

AUTHENTICATION TYPES

System Managers:

Ref	Statement
IDAM-6	For regular access: Require at least a single-factor (i.e. password) where staff or contractors are using a company-controlled device in a company-controlled (physically secure) location to access assets classified as Medium confidentiality or above.
IDAM-7	For remote access: Require two-factor authentication (2FA or TFA) where staff or contractors require remote access to assets classified as Medium confidentiality or above.
IDAM-8	For privileged access: Require two-factor authentication (2FA or TFA) where staff or contractors require privileged access. Note: Privileged access includes access to supervisory functionality that allows the modification of system or security parameters, e.g. 'root' and 'administrator'.
IDAM-9	For emergency access: Require CISO or Executive written approval to grant emergency access to assets with a High Confidentiality classification where policy requirements have not been met.

PASSWORDS

System Managers:

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

IDAM-10	<p>Where passwords are used as the sole method of authentication:</p> <ul style="list-style-type: none"> • verified for complexity via the use of a strength meter • verified for weak or compromised passwords via lists • throttled to prevent frequency of retries (i.e. to prevent brute force) • do not need to be checked for complexity • do not need to be changed unless suspected of being compromised <p>Note: These practices are based on revised NIST Digital Identity Guidelines found as follows: https://pages.nist.gov/800-63-3/</p>	
IDAM-11	<p>Where IDAM-10 requirements based on the NIST Digital Identify Guidelines cannot be met passwords must instead:</p> <ul style="list-style-type: none"> • be a minimum length of 13 alphanumeric characters with complexity • ensure that passphrases are changed at least every 90 days • prevent passphrases from being changed by the user > once a day • prevent passphrases from being reused within 8 passphrase changes • prevent the use of sequential passphrases where possible <p>Note: These practices are based on traditional controls found in the Australian Government Information Security Manual as follows: https://www.asd.gov.au/infosec/ism/ (pp.192-199)</p>	ISM
IDAM-12	<p>Where password are used they are protected as follows:</p> <ul style="list-style-type: none"> • locked after a maximum of 5 failed logon attempts • be unique when reset and changed upon first logon • be encrypted/hashed while in transit and storage (not in cleartext) • not shown on screen (with residual risk acceptance) <p>Note: The use of an electronic password vault/safe to store passwords is encouraged providing it is stored on a company device (not cloud service). Note: Approved cryptographic techniques are described in the System Acquisition and Development Policy.</p>	

TWO FACTOR AUTHENTICATION

System Managers:

Ref	Statement
IDAM-13	<p>Use reputable One Time Password (OTP) software to achieve two factor authentication where the generating device (such as mobile phone) is “out-of-band” (isolated) from the system being accessed.</p> <p>Note: SMS is no longer an approved method for receiving One Time Passwords Note: Google Authenticator is considered reputable OTP software.</p>


ACCESS

System Managers:

Ref	Statement	
IDAM-14	Ensure all access is supported by a documented and legitimate business requirement including authorisation.	
IDAM-15	<p>Restrict administrative privileges by ensuring that only the staff and contractors requiring administrative privileges have them.</p> <p>Note: Staff and contractors do not run day-to-day applications (particularly email and web browsers) with administrative privileges.</p> <p>Note: Administrators use a separate account (or Microsoft UAC or Linux 'sudo') when requiring elevated privileges for administrative duties.</p> <p>Note: Built-in Administrator account and root accounts should be secured.</p>	ISM
IDAM-16	Assign access to users via groups, roles and/or attributes.	
IDAM-17	Enable access controls to enforce access requirements.	

ACCESS REVIEWS

System Managers:

Ref	Statement	
IDAM-18	Review access to systems and information at least <u>annually</u> to ensure accounts and access levels are current and appropriate.	

ACCESS REMOVAL

System Managers:

Ref	Statement	
IDAM-19	Remove access to systems and information that is no longer required due to termination or change of employment (upon notification from HR Manager).	
IDAM-20	<p>Automatically remove or suspend accounts after <u>one month</u> of inactivity.</p> <p>Note: This control should be automated and not require ongoing performance monitoring via a scheduled task.</p>	