Tasmanian Government

Identity and Access Cybersecurity Standard

VERSION 1.0

MARCH 2020

Department of Premier and Cabinet

Tasmanian Government

Contents

Purpose

This Tasmanian Government Identity and Access Cybersecurity Standard (Standard) describes the minimum requirements for authorising and verifying the identity of individuals that access Tasmanian Government information, systems and services as a part of their employment or volunteering duties, or contractual relationship.

This standard also applies to service accounts involved in the provision of, or access to Tasmanian Government information, systems and services.

Adoption of this Standard ensures that an agency can establish that each individual or service account is authorised, and uniquely identifiable when accessing information, systems and services.

Scope

This Standard applies to Tasmanian Government agencies, as listed in the *State Service Act 2000*. Within agencies, the standard applies to the identity of individuals and service accounts. Individuals include those who are employed, contracted by, or volunteer for an agency.

Public access to Tasmanian Government systems and services is to be risk assessed in accordance with the Identity and Access Management Toolkit 2010 and appropriate controls implemented.

Other Tasmanian Government organisations may choose to adopt this standard as good practice.

Implementation

Implementation of the controls within this Standard are mandatory unless an exception has been approved by an agency risk and audit committee (or equivalent).

Minimum Requirements

1. AUTHORISATION

Rationale: Establishing a formal methodology for authorising, assigning, identifying and revoking access, limits the potential for unauthorised access to agency information, systems and services.

1.1. Access to information, systems and services is limited to authorised individuals and devices.

1.2. Access to information, systems and services is limited, within the extent of the capability of the system, to those privileges required to perform the role or receive the intended service in accordance with the 'least-privilege' principle.

1.3. A documented methodology is implemented to request, authorise, manage and remove access to information, systems and services.

1.4. Verification of identities is to be performed before creation of an account. Verification levels[1] will be in proportion to the sensitivity and criticality of the system or information contained within. Refer to the Identity and Access Management Toolkit for further details. [2]

1.5. A user's access to information, systems and services is authorised by the Business System Owner when access is first requested, prior to access being granted.

2. IDENTIFICATION

Rationale: To make authorised individuals accountable for their access to information, systems and services.

2.1. Authorised individuals, application accounts and service accounts are to be assigned a unique identifier for each authentication system.

2.2. Where privileged access is required to applications, databases, systems or services, users will be assigned a privileged account that is separate from their standard account.

2.3. If shared accounts and/or auto-logon accounts are required, the account details are to be recorded in accordance with agency policy. Additional controls are to be implemented to ensure accountability for actions can be attributed to individuals.

2.4. Anonymous access to information, systems or services not classified PUBLIC is not permitted.

[1] As defined in the *Identity and Access Management Toolkit* 2010
[2] Available from Digital Strategy and Services, Department of Premier and Cabinet

2.5. Contractor and temporary accounts are to have an expiry date and are to be disabled on that date. Extensions are permitted as required by the agency.

2.6. Employee and contractor accounts are to be disabled after inactivity in accordance with agency policy.

2.7. Accounts are disabled, within agreed timeframes or service expectations, after notification is received, specifying the account is no longer required.

2.8. Agencies must ensure that a user's identity has been verified to an appropriate level when resetting their passwords[3].

3. AUTHENTICATION

Rationale: To reduce the likelihood of unauthorised access to ICT systems.

3.1. Users are required to utilise a minimum of one authentication factor to authenticate.

a. Where password or passphrases are used, they are to have a minimum standard defined by agency policy. Reference should be made to the Australian Cyber Security Centre Information Security Manual[4] for appropriate password/passphrase standards.

3.2. Sharing of authentication factors is not permitted unless justified by business requirements and the details are managed in accordance with 2.3.

3.3. Authentication factors are to adhere to agency policy.

3.4. Where password or passphrase based authentication factors are used outside the Networking Tasmania perimeter, multi-factor authentication should be implemented.

3.5. Default, or built-in account, passwords must be changed before commissioning systems or services, where possible.

3.6. Initial passwords and passphrases must be set to change on first login where possible.

3.7. Authentication factors are to be provided in a secure and confidential manner.

3.8. Authentication factors used for disaster recovery, shared or group administrative or non-login accounts (eg root, administrator, service accounts, database accounts, IIS application pools etc) are to be stored securely in an enterprise password manager, physical safe or similar.

a. Access to the password manager or safe is restricted to staff that require it for their role. Access to the password manager or safe is to be audited at least monthly.

[3] As defined in the *Identity and Access Management Toolkit* 2010

[4] Australian Cyber Security Centre *Information Security Manual* – Guidelines for System Hardening available at, https://www.cyber.gov.au/acsc/view-all-content/ism

b. Access to the password manager or safe, is to be available when disaster recovery or business continuity plans are activated.

3.9. Password resets:

a. Where the user is required to change the assigned password after an administrative reset, passwords are to adhere with agency policy; or

b. Where password resets are performed in bulk or the user is not forced to change it, passwords are to be:

3.9.b.1. random and unique for each individual reset; and

3.9.b.2. not based on the user's name, staff id or any other identifier that is uniquely identifiable as belonging to them.

3.10. Authentication information is to be encrypted where possible.

3.11. Primary account authentication is to be performed by a central authoritative source (eg Active Directory) via enterprise or federated authentication.

3.12. Accounts are prohibited from authenticating ('locked out') after a number of failed authentication. The specific criteria are defined in the agency's policy.

3.13. Authentication lockouts are reset in accordance with agency policy.

3.14. Devices and applications are to lock the screen in accordance with agency policy.

4. PRIVILEGED ACCESS

Rationale: Privileged accounts have increased permission to access systems, services and information. These are significant targets for compromise by malicious actors and their permissions should be limited to the minimum necessary to perform their role. Reducing the permissions limits the impact of a compromise of a privileged account on an agency.

4.1. Privileged accounts are to utilise multi factor authentication where possible and practical.

4.2. Privileged access is to be restricted to agency roles that require the permissions.

4.3. Privileged access must be formally authorised and documented in registers.

4.4. Privileged access must be revalidated annually.

4.5. Where technically possible privileged accounts are not to be shared accounts, unless they are for disaster recovery, or emergency access purposes only.

4.6. Highly privileged accounts (see definition) are to be limited to the minimum number of unique individuals required to support business requirements.

4.7. Service account permissions are restricted in accordance with the principle of 'least privilege'.

4.8. Privileged accounts are to be prevented from reading emails or messages, browsing the web and downloading files directly from external sources where possible.

4.9. Privileged account access is to be from authorised devices or networks only.

4.10. Privileged accounts are not authorised to authenticate to remote access services from outside the agency perimeter.

5. AUDITING AND ACCESS

Rationale: Regular reviews of audit logs increase the likelihood that unauthorised or malicious activity is detected and addressed.

5.1. Any action taken to create, delete, remove or update a user account is logged for auditing purposes and the logs are maintained in accordance with the agency disposal schedules.

a. A record is to be maintained that contains the approvals to perform the logged actions.

5.2. Audit logs are maintained in accordance with agency disposal schedule for all system or application authentication.

a. Logs are to include successful and unsuccessful authentications.

5.3. Additions, modifications or removals of privileged and highly privileged accounts and/or the associated permissions are to be reviewed monthly.

5.4. Anonymous access to systems is to be logged and the following access information logged at a minimum.

a. Information accessed

b. Time and date of access

c. Connection source of access

Definitions

Account	A unique user identifier that identifies a user to systems and services. Usually consists of username and authentication factor. Access controls and authorisations are assigned to accounts.
Anonymous access	Access to systems, services and information without verifying identity.
Audit logs	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Authentication	The process of verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system.
Authentication system	A self-contained system that verifies the identity of a user, process or device as a prerequisite to allowing access to resources in a system. It consists of authentication servers and authentication factors.
Authentication factors	A category of credential used to verify a user identifier. Will usually consist of one of the following factors: • Something the claimant knows (password, pin) • Something the claimant has (cryptographic token, smartcard, certificate) • Something the claimant is (biometrics)
Authorisation	Business system owner or delegate expressly deciding level of access for unique users within an information system.
Auto-logon accounts	Accounts used to automatically logon to operating systems without human interaction.
Biometrics	Measurable physical characteristics used to identify or verify the claimed identity of an individual.
Business System Owner	The person who is accountable for the security of the information in the asset and/or service. These are normally senior executives in the State Service (Directors, Deputy Secretaries or Secretaries etc.)
Cryptographic (or security) token	A physical device used to gain access to systems and services.

Enterprise authentication	An authentication method utilising a centralised authentication store.
Federated authentication	A method for using a single identity to authenticate to other organisation services.
Highly privileged accounts (see privileged accounts)	Accounts that have elevated permissions and access to the entire range of agency ICT systems and information. For example: Enterprise and Domain administrators, Global Administrators
Least-privilege	The principle that states that processes, users and programs must only have access to resources needed to perform their role.
Multi-factor authentication	A method of authentication that uses two or more authentication factors to authenticate an account identity.
Passphrase	A password consisting of a sentence or phrase made up of several unique words.
Primary account	The unique account assigned to staff, contractors and volunteers for access to agency networks and email services.
Privileged access	Privileged access is elevated permissions with the ability to: • Change system configurations • Change control parameters • Access auditing and security monitoring information • Circumvent security measures • Access data, files and accounts used by other users
Privileged accounts	Privileged accounts are accounts that have privileged access. For example: service accounts, root, sudoers, database administrators, network administrators, workstation and server administrators etc
Remote access	Access to a system that originates from outside an agency network and enters the network through a gateway, including over the internet.
Remote access services	Combination of hardware and software allowing remote access to agency networks or end-user devices.
Shared accounts	Unique identifier shared by one or more people.
Service accounts	Service accounts are accounts created explicitly to run services or daemons, and/or access databases on behalf of applications.

Smart card	A physical card containing an integrated circuit used to gain access to systems and services.
Unique identifier	A numeric or alphanumeric identifier assigned to a user to uniquely identify them in the context of access, authentication, authorisation and accountability. For example: A username, identification number etc
User	An entity authorised to access an information system.

ATTRIBUTION

REFERENCES

Australian Cyber Security Centre. Australian Government Information Security Manual - Controls. Available at https://www.cyber.gov.au/acsc/view-all-content/ism.

Tasmanian Government. *Identity and Access Management Toolkit*. Available from Digital Strategy and Services.

Tasmanian Government. *Tasmanian Government Cybersecurity Policy*. Available at http://www.dpac.tas.gov.au/__data/assets/pdf_file/0003/476706/Tasmanian_Government_Cybersecurity_Policy.pdf.

DOCUMENT HISTORY

Version	Date	Comments
1.0	03/02/2020	Approved by Deputy Secretaries Digital Services Committee

AUTHOR

Digital Strategy and Services, Department of Premier and Cabinet

STANDARD REPLACES

N/A

STANDARD AUTHORISATION

Deputy Secretaries Digital Services Committee

MONITORING PROGRESS OF STANDARD IMPLEMENTATION

Monitoring will occur through the appropriate digital services governance arrangements.

STANDARD MAINTENANCE

Digital Strategy and Services, Department of Premier and Cabinet

STANDARD ISSUED

03 March 2020

REVIEW DATE

No later than March 2023, it may be updated before that date if required.

COPYRIGHT STATEMENT