Snowy Technical Standards	
SHL-GEN-001	***ICS Computer Security Standard***
Subject Matter Expert *Michael Thornton* *Manager Engineering*	Version Date: January 2014 *Reviewed: 2 July 2019*
	Revision: *A*

1. Executive Summary

Security standards and associated practices play an integral role in the security lifecycle of an organisation through the encapsulation of the currently accepted approaches. These current accepted practices are generally a balance of many factors, including (but not limited to) industry security practices and the context of the organisation.

This document seeks to document the policies (as defined within the framework) that represent the currently accepted practices affecting functionality under ICSs custodianship.

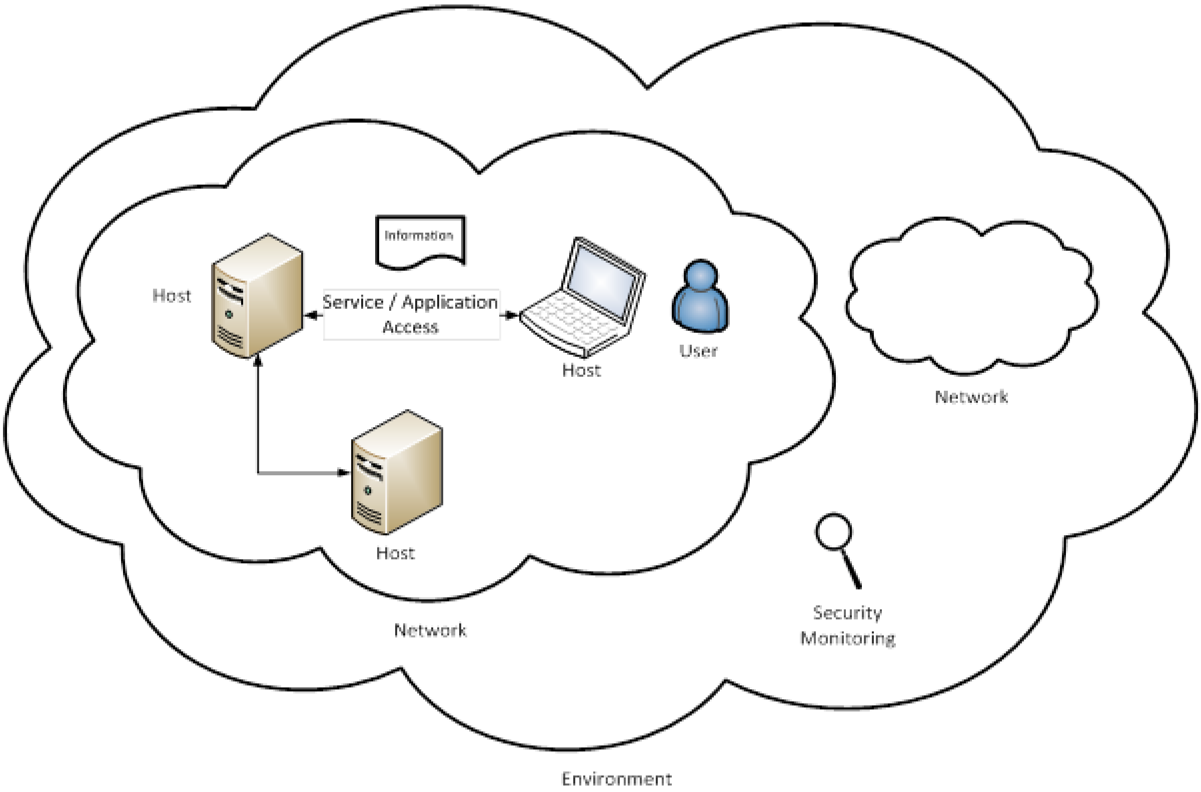
The high-level aims of the policy are:

- Prevent successful attacks against the Snowy Hydro
- Detect and react to successful attacks against Snowy Hydro

It is intended to be primarily used by technical owners, under the direction of business owners, and in conjunction with ICS Security to enhance Snowy Hydro's security posture while minimising the disruption to operations

2. Scope

In order to ensure a holistic approach the following conceptual model is used:



The items in the above diagram represent areas that are to be covered to ensure a comprehensive approach:

- *Network Architecture*
- *Host Management*
- *Information Security*
- *Authentication*
- *User*
- *Security Monitoring and Incident Management*

Physical security is not covered within this document, for the purposes of this document it is assumed that physical locations hosting ICS systems are appropriately secured.

3. Definitions

Credentials	A means to validate that the access being requested is authorised to take place, e.g. password
DMZ	Demilitarised Zone. An intermediate area of the network between less trusted and more trusted environments.
Environment	The combination of related networks, systems, and users.
Event	Anomalous or unexpected activity that may indicate unexpected or unauthorised activity.
Guessing attacks	Attempting each possible credential combination until successful.
Keystroke Logging	Recording a user's activity to capture credentials as they are being entered.

OSI Model	The OSI (Open Systems Interconnection) model of communications
Privilege	The access permitted to an authorised party.
Social Engineering	A form of attack that seeks to fool users into revealing their credentials. Pretending to be an IT professional is a well-known form of this attack.
Zone	A group of networks and systems that are logically grouped.

4. Standard

4.1. Network Architecture

Such an arrangement should be designed to promote similar types of traffic between zones and minimise the amount of activity required for host and authentication management.

Activity between zones must be restricted to only that which is authorised and activity should be denied by default. Where possible intermediate systems (e.g. proxies or jumphosts) should be preferred to direct access.

Bypass of the designated zone controls is not permitted. Examples of bypass include dual-homed systems bridging networks and unauthorised remote access modems.

Controls and inspection must take the full OSI model into account. All controls must be under Snowy Hydro management only.

4.1.1. Remote Access

Systems must be validated to ensure they do not pose risk to the organisation prior to being permitted access to the environment. Access must be restricted in nature.

Access to Snowy Hydro’s environment, including its information and users, must be minimised. Both scope, i.e. what can be accessed, and time, i.e. how long access is permitted, should be taken into account.

All communications are to be secured to ensure that only the authorised user obtains access.

4.2. Host Management

Systems must have a clear and known purpose. Areas that may be covered include the information stored or accessed via this system, the services provided, as well as asset tracking information and ownership.

System configuration hardening and updating must be conducted. These processes should cover BIOS, Operating Systems, Applications, and Information stores among others. Only required functionality should be enabled.

Only authorised parties must be permitted to access functionality on the system. Access to restricted functionality must be via means that ensure that only the authorised party is permitted access, e.g. encryption.

Availability of a known good state should be ensured depending on the value of the system. Examples of mechanisms that may be used include redundant systems, backups or snapshots, etc.

4.3. Information Security

Information is assigned to an individual Owner or an individual representing an Owner team. The owner is deemed to be the subject matter expert in regards to the information under their management and responsible for ensuring that sensitive information is appropriately secured.

ICS, on consultation with owners, provides the necessary advice and tools for owners to secure their information.

Any information deemed to be sensitive to the organisation must be controlled against being revealed to unauthorised parties (confidentiality), unauthorised modification (integrity), and loss (availability). Controls should be based on the potential loss that may incurred by the organisation.

Sensitive information must be protected both in storage and in transit. Intermediate systems may also store data, e.g. multi-function printers, USB drives, etc. and these should be taken into account.

Users authorised to access sensitive information must be granted access via individual authorisation. Such users are expected to take due care with the information they are granted access to, e.g. avoid emailing sensitive documents to third parties, avoiding placing sensitive information outside secure storage.

4.3.1. Data Classification Guideline

Financial & Trading Data – This type of data is of high importance as it can reveal significant information on the company’s inner workings. Trading data is of high importance to the business’ well-being as sensitive information (e.g. trading strategies) may erode the organisation’s competitive advantage or financial position.

Operational Data – Data that pertains to the scheme’s infrastructure and its management is considered sensitive to the organisation.

Personal Data – Data on individuals is of significant value as it is subject to legal regulation (e.g. Privacy Act 1988) and the compromise of such information may lead to regulatory penalties as well as reputational risk.

Other Sensitive Data – Data that is of consequence but does not fall into the above categories, e.g. password repositories

4.4. Authentication

4.4.1. Lifecycle

Credentials must be used only for a single clear purpose. Its purpose must be well known and correspond to one of the standard roles defined (see Predefined Roles). Where a deviation from defined roles is needed an exemption must be documented. In all cases privileges must be minimised.

Credentials must have a single clear assignee. Individual accounts must be tied to a well-known individual, or an individual representing a team (e.g. a team lead) where appropriate. This individual is the owner of the credentials and has full responsibility for activities undertaken via those credentials.

All activity must be tied back to an individual. If processes external to the credentials and associated monitoring are required they should be implemented. Measures should be implemented to detect anomalous activities.

Credentials must only be valid for the duration of their purpose. For access without a set period this is when the purpose is no longer valid, e.g. a user ceases to be employed by the organisation.

Authentication credentials are regarded as sensitive information and must be protected accordingly both in storage and transit

4.4.2. Strength & Longevity

Credential strength needs to be sufficient to invalidate known attacks. Calculations should take into account the possibility of both guessing and reverse engineering via hostile access to the system or credential repository.

Credentials must be refreshed regularly. This refresh period must be based on the expected time calculated for a successful attack and they must not be reused. In the case of credentials being revealed they must be disabled or refreshed.

Credentials must not be shared across different systems or functionalities. Where unavoidable, the credential strength must take into account the potential impact of the shared credentials being compromised, e.g. revealed credentials that are shared across all servers would lead to the compromise of all those servers.

Privileged credential strength must be commensurate to the granted access.

4.4.3. Predefined Roles

Unprivileged User Credentials:

- Normal user credentials that permit restricted access to user environments.
- Remote access must only be granted via strong two-factor authentication.

Privileged Credentials:

- Privileged credentials are those used for accessing restricted environments or conducting administrative activities.
- Privileged credentials must only be used to access privileged systems.
- Privileged credentials must be obviously distinct. There must be no confusion that they are privileged.

Service Credentials:

- Applications and other automated processes at times require an account to fulfil their desired functionality.
- No privileged access should be granted and only the minimum required privileges should be granted.
- Such credentials must be forbidden from interactive access and must not be used by a human.
- The credentials should be very strong as they are not expected to be entered for regular human driven activities. Such credentials should be held in secure storage to ensure they are available when required.

Built-in and Fall-back credentials:

- Applications and systems often have default credentials that are used for initial management. In addition fall-back credentials are often specified as access of last resort.
- These are to be disabled or set to very strong values to ensure they are not used except in case of suitable emergency. Well-known identifiers, e.g. administrator, admin, etc. are forbidden from being used. Credentials must be held under secure storage

4.5. User

Users are deemed to be business owners of functionality. As such it is expected that they bear responsibility for assets and information under their custodianship, e.g. workstations, sensitive information, etc., including the security of those assets. Technical owners, including ICS Security, may assist owners in carrying out those responsibilities.

Users are expected to only access functionality that they are authorised to access. They are also expected to do so in a manner consistent with authorised access, local laws, and keeping the company's best interests in mind.

Monitoring of activity may be undertaken as necessary to ensure that activities comply with authorised activities.

ICS will endeavour to provide users with the necessary resources to carry out their responsibilities. These resources may include tools, education, advice, etc.

4.6. Security Monitoring and Incident Handling

4.6.1. Monitoring

Preventative measures should be prioritised over remediation as the cost-benefit is superior, particularly in terms of manpower and disruption required for remediation.

Monitoring and Detection infrastructure must be in place. Sensors and collectors must be architected so as to provide a comprehensive picture of the environment. Potential points of collection include Network, Operating System, Application, and Authentication among others.

Management processes must be in place for the Monitoring infrastructure. Both regular monitoring and maintenance of the infrastructure must take place.

4.6.2. Incident handling

A security incident is defined to be any situation where undesirable activity has or is likely to take place involving the Snowy Hydro environment. It should be noted that users are also deemed to form part of the environment.

The incident handling team must be authorised by senior management to undertake any monitoring or mitigation activities deemed within scope of the incident handling process. Appropriate escalation must be available for activities that are not authorised.

Well-defined incident handling processes should be in place to ensure consistent activity during an incident, encompassing:

- Incidents should be rated and activities prioritised accordingly.
- Roles and responsibilities are to be defined as part of the process, including those of non-ICS staff involved in the process.
- Forensically sound processes must be used.
- Standardisation of forms and documents should be followed where possible.

5. References

- NIST special publications