Department of Transformation and Shared Services
State Cybersecurity Office

Standard Title: Cloud Security Standard
Standard Version: 1.1
Effective Date: 06/01/2022

---

1. Introduction

Historically, servers and other computing resources were planned, procured, configured, deployed, and maintained within a closed system by trusted network architects with clearly defined roles and responsibilities, and strict security standards, policies, procedures, and oversight.

The cloud changed all that – with only a credit card, anyone can deploy a complete infrastructure in matters of minutes, exposing confidential assets and putting a company's reputation in jeopardy.

1.1 Purpose

This document establishes the necessary security requirements to ensure the security of state data in the cloud.

1.2 Scope

This standard applies to cloud platform(s) managed by DIS.

1.3 Authority

The DIS Director and Chief Information Security Officer (CISO) are the designated authority over state networks and state information assets managed by DIS under TSS. As a result, DIS designates the teams and authorizes the processes necessary to secure cloud platforms and related services in use at DIS.

1.4 Roles and Responsibilities

The following standard outlines the primary role(s) associated with state policy, including responsibilities and expectations.

1.4.1. Cloud Engineer

The Cloud Engineer is responsible for implementing and maintaining the operational controls necessary to support the requirements defined in this document.

2. Standard

2.1. Implementation Priority

Each cloud security requirement has an implementation priority, which is defined in the table below.

Implementation Priority	Requirement(s)
HIGH	These controls MUST be implemented for ALL Cloud Environments. All controls marked as HIGH MUST be implemented and validated before any sensitive data is loaded to the Cloud environment.
MEDIUM	These controls must be implemented in due course of the project, with explicitly defined completion dates that are tracked by the project manager or DIS State Cyber Security Office (SCSO) team.
LOW	These controls are to be addressed in due course of the operating model or project, with explicitly defined completion dates that are tracked by the project manager or DIS SCSO.

2.2. Cloud Security Requirements

The following table identifies the Cloud Security Requirements for implementation:

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-01	The use of a cloud platform root account or like account access with full administration privileges shall be limited. Any use of such credentials shall require multi-factor authentication.	HIGH	The use of root or like account access with full administrative privileges is applied leveraging least privilege practice, limiting the number of employees, and having alert notification when accessed.

		HIGH	All cloud accounts that have elevated privileges are periodically reviewed to ensure utilization of least privilege, that the number of employees with access is limited, and no unauthorized access during the period.
Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
		MEDIUM	Upon creation, any access keys associated with a root or like account access are deleted or disabled. In cases where use of root or like accounts with access keys are required, alerts are generated when active keys are associated with them.
		LOW	Multi-factor authentication (MFA) is enabled and monitored to alert if it is disabled.
		MEDIUM	Security questions are registered for the root account, as necessary to permit emergency recovery.
		MEDIUM	A process is utilized to validate, authorize, and permit usage of the "root" or "Super User" account in the case of emergency. Logging of such access is active and immutable.
		HIGH	MFA is enabled and monitored for all accounts with console access.
DIS-02	Multi-factor authentication (MFA) shall be required for all cloud platform accounts with interactive console access.	HIGH	Access management is governed by automated SSO capabilities and dispositioned through upstream capability.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-03	All cloud platform accounts with interactive console access that have been inactive for more than 90 days shall be removed or deactivated. All access keys shall be rotated at least every 90 days.	HIGH	Access keys are rotated for service accounts.
		HIGH	The password and other credentials configuration for the accounts are examined upon creation, after major system updates, and when changes are made to DIS security policy to ensure compliance with all DIS policies regarding complexity, composition, length, re-use, rotation, and recovery.
DIS-04	The cloud platform password policy for interactive console accounts must enforce complexity that adheres to DIS policy requirements.	HIGH	Inline and other policies are prohibited and prevented from being directly attached to a user. A registry of exceptions of inline policies is maintained and reviewed periodically. Periodic reviews or automated monitoring and alerting of user access is required to ensure that no prohibited access has been attached.
DIS-05	Cloud platform interactive console policies shall only be applied to groups or roles but never directly to individual user accounts	MEDIUM	Sufficient and adequate contact information is made available to the cloud provider and DIS maintains current cloud provider contact information.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-06	All pertinent security and support contact information shall be made available to the cloud platform provider and maintained to ensure current, sufficient information is available in the event of an incident.	MEDIUM	Contact information is available to cloud providers and is kept current and accurate.
		MEDIUM	A responsible group or role is assigned to maintain current and accurate cloud provider contact information.
		MEDIUM	A support role to manage incidents exists and is maintained.
		HIGH	Cloud compute instances utilize roles for authentication and authorization to resources in lieu of stored credentials. Periodic reviews or automated monitoring are employed to ensure compliance. Exceptions are noted and checked periodically for continued visibility.
DIS-07	All access within cloud platform compute instances shall utilize roles for authentication and authorization, in lieu of stored credentials.	HIGH	Logging of all security relevant events is enabled and verified in all regions. Logged information is sufficient to attribute any security relevant action to the responsible individual or entity. Logs are securely retained for a minimum of four years and made readily available to security staff in real-or near-real time.
DIS-08	Logging of all security relevant events and account activity shall be enabled, captured, monitored, and appropriately alarmed for all cloud platform regions in accordance with all applicable policies.	HIGH	Logs are appropriately captured and integrated with a processing sub-system capable of visualizing, identifying anomalies, and generating alerts. Such integration of logs is verified.

		HIGH	Programmatic credentials (i.e., access keys and access secret(s) are not created for user accounts. Machine identities, i.e., service accounts, shall not have interactive console access.
DIS-09	User accounts shall not have access keys and access secrets. Service accounts shall not perform interactive login.	MEDIUM	Evidence demonstrating the effectiveness of this control is periodically reviewed to ensure that interactive users do not have programmatic access and that accounts requiring programmatic access do not have interactive access. Exceptions are noted and checked periodically for continued visibility. Security and administrative personnel are notified when an account violates policy.
		HIGH	Log configuration is periodically checked to validate configuration settings that ensure log security and availability.
DIS-10	Cloud platform logs shall be protected against unauthorized modification and stored in a forensically sound manner.	HIGH	Identity and access management policies are checked programmatically to validate that no policies allow full administrative privileges such as “Effect”, “Allow” with “Action” over “Resource.”
DIS-11	Full administrative privileges shall not be created for any cloud platform Identity and Access Management (IAM) policies.	HIGH	Unauthorized notification of logs is prevented through the restriction of access to the minimum necessary and the required use of robust authentication and authorization.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-12	Public access to cloud platform logs shall be strictly prohibited.	HIGH	Activity logging is enabled and monitored on all log storage mechanisms.

		HIGH	Verification that configuration management and tracking is enabled for all regions is required. Programmatic notification of attempted and successful changes to configuration management settings is required.
DIS-13	Configuration management and tracking shall be enabled for all cloud platform regions	HIGH	Access to configuration management changes and data is restricted based on least privilege. (Programmatic notification of attempted and successful changes to permissions of configuration management settings is required.
		HIGH	Access to log storage media and systems is monitored and reviewed to ensure continued prevention of unauthorized access and modification.
DIS-14	Access to cloud platform log storage media and systems shall be strictly controlled to prevent unauthorized access and modification.	MEDIUM	Verification of log file encryption is required.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-15	All cloud platform log storage media and systems shall employ encryption at rest.	HIGH	Validation of the rotation of keys is required, including symmetric keys used for authentication, encryption keys, and keys used to secure transport protocols.
DIS-16	Cloud platform customer created Customer Master Keys (CMKs) used to protect sensitive and/or confidential data shall be rotated	HIGH	Processes and procedures are employed to monitor, require, and validate the rotation of keys, depending upon the

	in accordance with applicable policy.		implementation and mechanism(s) used to manage encryption. Product owner ensures that contractually the application must support annual key rotation, at a minimum.
		HIGH	Verification of required logging is required.
DIS-17	Logging of security relevant events in all relevant regions shall be enabled for all cloud platform compute resources and virtual networking capabilities, in accordance with applicable policy.	HIGH	Network traffic, including Virtual Private Cloud (VPC) flow logs, is logged and retained in accordance with DIS policy.
		HIGH	Log metric filters and alarms should be identified, collected, validated, and maintained in the preferred state.
DIS-18	Cloud platform log metric filters and alarms shall be established and maintained for all pertinent services, and events shall be monitored appropriately.	HIGH	Unauthorized Application Programming Interface (API) calls, including both external APIs within the control ("endpoints") and API calls within the cloud service/platform.

Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-18 (Continued)		HIGH	Changes in logging mechanisms and processes, such as suspension or disablement, modification, and unauthorized access attempts.
		HIGH	Changes to compute services, including virtual instances and networking, unauthorized actions, or access requests.
		HIGH	Successful and unsuccessful login attempts to interactive resources such as a web console or portal without Multi-Factor Authentication (MFA) and all unsuccessful attempts.

		HIGH	Use of root account
		HIGH	Disablement, scheduled deletion, modification, or permissions related to encryption keys and key management systems.
		HIGH	Changes to policy, including unauthorized actions or access requests.
		HIGH	Changes to storage services, including unauthorized actions or access requests.
		HIGH	Changes to configuration management services, including unauthorized actions or access requests.
Policy Control ID	Requirement(s)	Implementation Priority	Standard Requirement(s)
DIS-18 (Continued)		HIGH	Changes to network access such as network access control lists, security groups, route tables, and network gateways, including unauthorized actions or access requests.
		MEDIUM	Alerts for the above are generated and delivered to the SCSO. All alarms are routinely validated to ensure they are functioning properly.
		HIGH	Network interfaces and security groups restrict inbound access to all interactive services and ports, such as restricting by IP address, ports, and other means.

DIS-19	Inbound access to ports on the cloud platform shall be restricted to the minimum necessary for remote connectivity and administrative access.	HIGH	Inbound connectivity is restricted to not be overly broad, particularly for services that are used for remote interactive connectivity and administration.
		HIGH	Rules are defined to control network traffic in and out of network interfaces and to implicitly deny all other traffic.
DIS-20	Ingress and egress of cloud platform network traffic shall be strictly controlled.	HIGH	Routing tables for peer-to-peer network services restrict to least access.
DIS-21	Cloud platform routing tables for network interface peering shall be set to "least access."	HIGH	Default should be deny.

3. Inquiries

Direct inquiries about this policy to:
Division of Information Systems
State Cybersecurity Office
Little Rock, Arkansas 72201
Email: SCSO@arkansas.gov

4. Revision History

This standard shall be subject to review according to the Regulatory Spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
08/01/2022	Annual Review	State Cybersecurity Office
12/19/2024	Annual Review. Update formatting.	Raymond Girdler, State IT Security Specialist