Policy Title: Cloud Service Provider Security Standard

Approved by: Chief Information Officer

Approval Date: 11/30/2021

Next Review Date: 11/30/2022

Effective Date: 11/30/2021

Policy Number:

Supersedes:

Originating Department: I&T

Contributing Departments: Information Security

Manual: Information Technology Manual

Section:

Revision: 1

Table of Contents

I. Standard 1

II. Purpose 1

III. Scope 1

IV. Standard Details 1

A. General Cloud Security Standards 1

V. Definitions 7

VI. Attachments 8

VII. Related Policies & References 8

VIII. Version Control 8

# Scope

This Bon Secours Mercy Health (BSMH) Information & Technology (I&T) standard applies to all workforce members and governs all data and systems (whether owned by or operated for BSMH business through contractual arrangements).

# Standard

BSMH must implement security controls on BSMH contracted Cloud Platform Technologies (Cloud) that will be utilized by BSMH.

# Purpose

Cloud security encompasses the technologies, controls, processes, and standards which combine to protect BSMH cloud-based systems, data, and infrastructure. It is a sub-domain of information security.

Cloud security is a shared responsibility between BSMH and the cloud service provider. Cloud security is implemented to protect the Confidentiality, Integrity, and Availability (CIA) of data and adhere to regulatory compliance. This in turn protects BSMH from reputational, financial, and legal impacts of data breaches and loss.

# Standard Details

## A. General Cloud Security Standards

## BSMH must choose a trusted cloud service provider. Cloud service providers must provide evidence of their security compliance, cybersecurity insurance, and security certifications (e.g., HITRUST).

## BSMH and the cloud service provider must review and understand the shared responsibility model. BSMH must ensure that the cloud service provider agrees with the stated model responsibilities.

## Example shared responsibility model:



## Workforce members must understand the provider’s security controls and governance process in place for the protection of BSMH assets and information (e.g. using CSA STAR Registry).

## All cloud service provider contracts and Service Level Agreements (SLAs) must be processed by BSMH Supply Chain to include review and approved by BSMH I&T and BSMH Legal. Contracts must include (but are not limited to) the following:

## Contracts and SLAs must state that all data belongs to BSMH.

* + - 1. Contracts and SLAs must state the disposition of data when the contract is terminated (the use of Crypto Shredding of BSMH data is strongly encouraged).
      2. Cloud service providers must provide visibility into security events and report responses to those events to BSMH in a timely manner.
      3. Contract and SLAs must state that the data location for all BSMH data is in a BSMH approved geolocation.
      4. Contracts and SLAs must state timeframe and access mechanism pertaining to providing requested data for the purpose of forensic analysis.

1. BSMH must provide training on secure cloud practices to its workforce members that includes (but is not limited to) the following topics:
2. Spotting malware
3. Identifying phishing e-mail
4. Secure computing practice
5. Password policies
6. Workforce members with Administrative privileges in the cloud must receive training and/or certifications in cloud security.
7. BSMH must ensure the implementation of strong user access control:
   * + 1. Each new cloud solution must be brought to the attention of the Identification and Access Management team prior to implementation to allow for the development of user provisioning process flows.
       2. All user account permissions must be configured using the Principle of Least Privilege.
       3. User permissions must be configured using security groups rather than assigning permissions to individual user accounts. The use of nested groups is prohibited.
       4. User access to cloud resources must be granted through the approved BSMH methodology (See AC-ST-1.0.06-R2.0 Application and Information Access Control and AC-ST-1.0.02-R2.0 Authorized Access to Information Systems).
       5. The BSMH Provisioning team must be utilized as applicable for creating user accounts and access to cloud services.
       6. The root or administrative account used to establish the subscription/tenant must not have programmatic credentials configured (e.g. API keys, access/secret keys).
       7. Users with direct console access that remain inactive for a period of more than 180 days will be disabled. Re-enabling these accounts will follow the same approval process as a new account and will be audited and restricted using Principles of Least Privilege.
       8. All programmatic credentials (API keys, access/secret keys, etc.) will be rotated every 90 days.
8. BSMH must ensure the implementation of threat detection and prevention:
   * + 1. Strong endpoint security must be maintained on managed endpoints following BSMH standards SA-ST-10.0.06-R1.0 and CS-ST-9.0.04-R1.0.
       2. Implementation of data loss prevention mechanisms will be put in place where sensitive data is stored and where applicable.
       3. A mechanism to discover, assess, and prioritize vulnerabilities must be configured for all compute assets.
       4. A redundant system of network traffic inspection for the purpose of intelligent routing and capable of blocking malicious network traffic will be deployed in the cloud environment (e.g. network firewall).
       5. Web applications (static or dynamic) will employ a mechanism for detecting, prioritizing, and blocking malicious traffic and common web application attack vectors (e.g. web application firewall).
9. BSMH must maintain the ability to discover cloud services and applications that interface with BSMH infrastructure. Unapproved cloud solutions must go through a cybersecurity risk assessment and gain approval or be discontinued. New cloud solutions must go through the I&T Governance process prior to contracting with the provider for services.
10. BSMH must ensure the implementation of data encryption:
    * + 1. Data encryption for data in motion must be implemented for data transmission to and from the cloud. BSMH cryptographic controls must be followed (See SA-ST-10.0.03-R1.0 Cryptographic Controls).
        2. BSMH must ensure that data at rest in the cloud is encrypted with an entrusted key and follow BSMH cryptographic controls (See SA-ST-10.0.03-R1.0 Cryptographic Controls).
        3. Avoid encrypting data with a single entrusted key to reduce the impact in the event of a compromised encryption key (e.g. using multiple entrusted keys to encrypt different types of data or systems).
        4. Entrusted key will be rotated regularly and, where possible, automatically (e.g. automatic rotation every 365 days).
        5. Where possible, entrusted keys should not be deleted. Entrusted keys should be disabled or employ a mechanism for retention of the key material for an extended period.
        6. Where possible, network connectivity should be private and encrypted.
11. Strong Password Security Practices
    * + 1. Where possible, all BSMH workforce member user and Administrator accounts must be configured to utilize Single Sign-On (SSO) for authentication to cloud services. Otherwise, user and privileged accounts must comply with BSMH password standards (see AC-ST-1.0.02-R1.0 Authorized Access to Information Systems standard).
        2. An isolated account (not belonging to any one person) must be used in the creation of the subscription/tenant. The creation of this account using a personal (non-BSMH email) is prohibited.
        3. The root or administrator account used to establish the subscription/tenant must comply with BSMH password standards (see AC-ST-1.0.02-R1.0 Authorized Access to Information Systems standard).
        4. Where possible, root account passwords will be stored in the corporate approved BSMH Privileged Access Management platform.
12. Authentication
    * + 1. All non-service accounts with management plane access to the subscription/tenant must also use multi-factor authentication (e.g. hardware token or virtual token).
13. Sensitive Credentials
    * + 1. Sensitive credentials and application information (e.g. database connection strings, API Keys, usernames, passwords, etc.) will be stored securely, encrypted, and rotated regularly (e.g. every 365 days).
14. BSMH must implement a Cloud Access Security Broker (CASB) to enhance and extend security controls into the cloud.
15. Security of Network Connectivity
    * + 1. Outbound network traffic rules should be restricted to BSMH approved ports (See CS-ST-9.0.06-R1.0 Network Security Management and AC-ST-1.0.04-R2.0 Network Access Control Standard). All other ports (outbound) require approval by the approved BSMH Governance Committee.
        2. Inbound network traffic rules require approval by the approved BSMH Governance Committee.
        3. Interconnectivity of internal resources deployed in the cloud should be enabled and network traffic will be restricted to minimum required (e.g. VPC Peering).
        4. Outbound and inbound network traffic will be routed through a redundant system capable of inspecting and blocking malicious network traffic (e.g. network firewall, web application firewall).
16. Public and External Access
    * + 1. Remote access administration will be disabled (e.g. RDP- 3389, SSH -22, etc.). If remote access is required, compensating controls must be put in place (e.g. bastion networks). Deviation from this recommendation must be approved and documented by the approved BSMH Governance Committee.
        2. Storage mechanisms will not have public read/write permissions enabled.
        3. Databases will not have public read/write permissions enabled.
17. Workload Hardening
    * + 1. Compute resources must be hardened to prevent intrusion from malicious actors (e.g. disabling unused services, uninstalling unused default software programs from operating systems).
        2. Serverless compute must be hardened to prevent unsecured communications and runtime environment from becoming an attack vector to malicious actors (e.g. enforce HTTPS, latest version of programming language).
        3. Where possible, storage mediums should employ secure connectivity for read and write access (e.g. enforce HTTPS, SFTP over FTP, etc.).
        4. An identification mechanism for software and hardware security patches must be deployed and operational.
        5. Compute resources must have the latest security patches installed to meet the BSMH patching standards (See SA-ST-10.0.06-R1.0 Technical Vulnerability Management).
18. Asset and Data Classification
    * + 1. Compute resources will be configured with tags for the purpose of classification and identification of assets.
        2. Cloud resources (e.g. VMs, databases, etc.) must be logically grouped according to workload or data sensitivity-level to isolate and reduce the impact in the event of a security incident or system compromise.
19. Security Information Logging
    * + 1. A central repository for the collection of security related logs must be configured. Access (e.g. read, write, and modify) to this repository will be granted using the Principle of Least Privilege.
        2. A data lifecycle policy will be configured to automatically archive security related logs after an acceptable period and in accordance with applicable governance and compliance requirements (e.g. 1 year, 7 years for compliance with HIPAA).
        3. The following log sources (but not limited to) must be enabled/configured to be stored in a central repository:
20. Management plane activity logs
21. Network traffic logs
22. System/application logs (e.g. Windows event logs)
23. BSMH must ensure the implementation of data management:
    * + 1. A data lifecycle management policy will be configured on all applicable storage mediums per applicable governance, compliance requirements, or as best practice (e.g. 1 year, 7 years for compliance with HIPAA).
24. BSMH must ensure the implementation of documentation:
    * + 1. The Cloud environment must be documented to show all components involved and how they interact with each other. Documentation must be readily available, and access will be granted using Principles of Least Privilege.

# Definitions

Underlined words identify terms that are hyperlinked defined in MP-ST-0.0.01-R1.0 Information Security Governance Manual Attachment 1.

# Attachments

NONE

# Related Policies & References

* Communications and Operations Management policy
* Records Retention and Destruction policy
* Malicious Code Protections standard
* Technical Vulnerability Management standard
* Authorized Access to Information Systems standard
* Cryptographic Controls standard
* Network Security Management
* Network Access Control Standard
* Application and Information Access Control

# Version Control

| Version | Date | Description | Prepared By |
| --- | --- | --- | --- |
| 1.0 | 8/5/2021 | Standard created and approved | Luis Leon |
|  | 8/12/2021 | Adjusted formatting to BSMH standard, proofread, grammar check, add TOC | Kara Mueller |
|  | 11/1/2021 | Annual review, Adjusted formatting to BSMH standard | Lara Hayes, Desiree Chumbler, Tracy Griffin |

This policy/procedure/guideline does not establish a standard of clinical care or practice or standard of non-clinical practice to be followed in every case. The policy/procedure/guideline should guide actions with the understanding that departures may be required at times.

Revised 04/01/2021 - Bon Secours Mercy Health adopts the above policy, procedure, policy & procedure, guideline, manual / reference guide / instructions, or principle / standard / guidance document for all Bon Secours Mercy Health entities including, but not limited to, facilities doing business as Mercy Health – St. Vincent Medical Center, Mercy Children’s Hospital, Mercy Health – St. Charles Hospital, Mercy Health – St. Anne Hospital, Mercy Health – Tiffin Hospital, Mercy Health – Willard Hospital, Mercy Health – Defiance Hospital, Mercy Health Allen Hospital LLC, Mercy Health - Lorain Hospital, Mercy Health St. Elizabeth Youngstown Hospital, Mercy Health St. Joseph Warren Hospital, Mercy Health - St. Elizabeth Boardman Hospital, Mercy Health - St. Rita’s Medical Center, Mercy Health – Springfield Regional Medical Center, Mercy Health - Urbana Hospital, Mercy Health - Anderson Hospital, Mercy Health - Clermont Hospital, Mercy Health – Fairfield Hospital, Mercy Health - West Hospital, The Jewish Hospital – Mercy Health, Mercy Health - Lourdes Hospital LLC, Mercy Health – Marcum and Wallace Hospital, Chesapeake Hospital Corporation DBA Rappahannock General, Maryview Hospital, Bon Secours Richmond Community, Bon Secours Memorial Regional Medical Center, Bon Secours – St. Mary’s Hospital, St. Francis Hospital, Inc., Bon Secours St. Francis Medical Center, Bon Secours Mary Immaculate Hospital, Southside Regional Medical Center, Bon Secours Mercy Health Franklin, LLC, and Southern Virginia Regional Medical Center (Emporia).