Status Active PolicyStat ID 15387827

Origination Date	12/2018
Last Approved	03/2024
Effective	03/2024
Last Revised	03/2024
Next Review	03/2025

Owner	Mark Johnson: VP Chief Info Security Offcr
Policy Area	Cybersecurity-ENTERPRISE
Applicability	Hackensack Meridian Health Network
Applies To	Hackensack Meridian Health Network

Cloud Security Policy

Purpose

Hackensack Meridian Health (HMH) and its affiliated entities have adopted this Cloud Security Policy in order to recognize the requirement to comply with applicable administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of data for all HMH entities, including the Hackensack Meridian School of Medicine.

HMH recognizes our responsibility to protect internal, confidential and restricted data, including but not limited to protected health information, personally identifiable information, student protected information, credit card data, and financial information, in electronic form, under applicable industry, state and federal regulations and general professional ethics.

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on. HMH's DTS department remains committed to enabling team members to do their jobs as efficiently as possible through the use of technology. The following policy is intended to establish a process whereby HMH team members can use cloud services without jeopardizing organizational data and computing resources.

This policy pertains to all external cloud services, including cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. for

HMH. All personnel of HMH must comply with this policy. Please direct questions on this policy to the Cybersecurity team.

Policy

- Use of cloud computing services for work purposes should be formally authorized by the SVP, Associate CIO & Chief Technology Officer or designee. The SVP, Associate CIO & Chief Technology Officer or designee will strive to certify that cybersecurity, privacy and all other DTS requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the SVP, Associate CIO & Chief Technology Officer (or designee) as well as the HMH Strategic Sourcing and Legal departments.
- The use of such services should comply with all laws and regulations and HMH policies governing the handling of public, internal, confidential and restricted data or any other data created, received, maintained and/or transmitted by HMH.
- HMH will strive to create procedures that allow for prior approvals, as necessary, for structured data transmissions.
- HMH personnel should label, handle and safeguard the data in accordance with the HMH Data Handling Policy.
- Personal cloud services and/or accounts should not be used for the storage, manipulation or exchange of company-related communications or company-owned data.
- Data transmitted, processed, and/or stored in cloud services should be encrypted.
- Access to cloud services should be controlled through HMH centralized Identity and Access Management systems.
- Cloud services should be monitored for security threats.
- Security incidents should be reported to HMH's Cybersecurity department.

Compliance and Enforcement

All managers and supervisors are responsible for supporting the enforcement of this policy. Executives, team members, contractors, temporary workers, and volunteers must comply with this policy. Team members who violate this policy are subject to discipline up to and including termination in accordance with HMH's Guidelines for Cooperation and Discipline.

Approval Signatures

Step Description	Approver	Date
	Mark Johnson: VP Chief Info Security Offcr	03/2024

Melissa Lawlor: Dir Cybersecurity GRC	03/2024
Matthew Sadler: Dir Cybersecurity Ops	03/2024