Registration and Protection of Systems Policy

Published: March 2010

Revised: March 2018

I. Introduction

This Policy describes the requirements for security controls to protect Endpoints that process, transmit and/or store Data (as each is defined in OMG Information Security Charter (the "Charter")) https://www.omahamediagroup.com/isc. Such requirements differ depending on whether such Data is Sensitive Data, Confidential Data, Internal Data or Public Data (as each is defined in the Charter).

No distinction is made in this Policy between an Endpoint owned by OMG or personally owned. All Information Security Policies (as defined in the Charter) will apply to a personally owned Endpoint used for OMG business.

Any Endpoint that processes, transmits and/or stores Data must be registered in accordance with Section III(A) and have the minimum protection requirements set forth in Section III(B) or (C) and, if applicable, Sections III(D), (E), and/or (F), in each case for the most restricted class of Data that is processed, transmitted or stored on such Endpoint.

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy History

- The effective date of this Policy is March 30, 2010.
- Reviewed and/or revised March 14, 2018.

III. Policy Text

A. Registration of Systems

All Systems, including OMG Systems, that process, transmit and/or store ePHI/PHI Data must be registered with OMG Information Security Office. All Systems that process, transmit and/or store non-EPHI/PHI Sensitive Data and/or Confidential Data must be registered with the CU Information

Security Office. Registration will be carried out in accordance with the procedures established by each such Office.

B. General Protection Requirements for Systems

Each System Owner will ensure that the following protections, at a minimum, are implemented for each System:

1. 1. An IT Custodian has been appointed for the System by the System Owner. Contact information for CU Systems has been provided to security@omahamediagroup.com. Contact information for OMG Systems has been provided to Security@omahamediagroup.com.
2. The facility that houses the System's Servers, including primary and backup equipment, is environmentally controlled and physically secured from unauthorized access.
3. Each Server is physically labeled with a name or other identification.
4. All Data files on a Server are backed up regularly in accordance with OMG Business Continuity and Disaster Recovery Policy https://www.omahamediagroup.com/isc.
5. Each of the System's production Servers has a UPS that can provide emergency power and shut the Server down in case of a power outage.
6. Standard configurations, as defined by the applicable Information Security Office, are used to establish a secure configuration baseline.
7. Access to the System's Servers and the Data residing on the System is restricted and is maintained in accordance with OMG Information Resource Access
8. Control and Log Management Policy https://www.omahamediagroup.com/isc.
9. The System's Servers are not used for general desktop functions, such as web browsing, conducting personal email or other OMG business or non-business functions.
10. The System's Servers are running vendor-supported operating systems and have up-to date security patches installed.
11. The System's Servers are accessible only for the services provided and only to as much of the Network as is required to provide such services, and firewalls or equivalent protections prevent unauthorized access. To the extent practicable, antivirus, antispyware and System monitoring programs are installed to protect and/or prohibit unauthorized access.
12. Any Peer-to-Peer Program is used only for OMG purposes, is configured properly as directed by the applicable Information Security Office and does not permit general purpose file sharing over the Internet.
13. Only required services that run on the System's Servers are enabled. Unneeded services are disabled.
14. Each System used for OMG purposes is disposed of in accordance with OMG Sanitization and Disposal of Information Resources Policy https://www.omahamediagroup.com/isc.

C. Additional Protection Requirements for Systems Containing Sensitive Data or Confidential Data

Each System Owner shall ensure that, in addition to the protections described in Section B above, the following protections are implemented for each System that processes, transmits and/or stores Sensitive Data or Confidential Data:

1. A record is kept of what type of Sensitive Data or Confidential Data are stored on the System's Servers and of all changes to the configuration of the Server, and such documentation is kept in a secure, locked location away from the Server.
2. In web-based Systems that are exposed to the Internet, protection mechanisms are implemented to prevent common web-based attacks. Examples of protection elements include web-based firewalls and/or source code security reviews.

In addition, it is recommended, but not required, that Confidential Data be protected with a password while in transit and in storage.

D. Additional Protection Requirements for Systems Containing Sensitive Data.

Each System Owner shall ensure that, in addition to the protections described in Sections B and C above, the following protections are implemented for each System that processes, transmits and/or stores Sensitive Data:

1. Sensitive Data are encrypted while in transit and in storage, except that Users within OMG may internally transmit unencrypted ePHI if it is sent to an Approved OMG Email System.
2. Removable Media containing Sensitive Data are encrypted.
3. In Relational Database Management Systems, Sensitive Data are encrypted in a way that permits database administrators to perform their management functions without access to such Data in a readable format.
4. The System's Servers are maintained in appropriate Data centers, Server closets or Data closets that meet or exceed the following physical requirements: Video camera surveillance; Badge reader (rather than key) access; Use of a visitor log to document all visitors who accompany an authorized User, which is posted by the main ingress/egress point of the secure facility; Alarms on the door that alert OMG Public Safety if (x) the door is left ajar, (y) the door is forced open or (z) the security lock malfunctions; and An emergency power shut off button that can cut off power to all circuits in the case of a fire or other physical threat.

For any System that exists on the Effective Date of this Policy and contains Sensitive Data, but cannot use encryption because of technology limitations, a special waiver may be granted by the applicable Information Security Office if such Office determines that there are compensating controls in place to address all major information security risks.

E. Protection Requirements for Systems in OMG Clientele Healthcare Component

Each System Owner of any System that is part of OMG Clientele Healthcare Component must follow the specific procedures relating to Systems in OMG Information Security Procedures https://www.omahamediagroup.com/isc which reflect the regulatory requirements for managing ePHI.

F. Externally Hosted Systems

Each System Owner shall ensure that the protections described in Section B and, if applicable, Sections C, D and E above are implemented if a externally hosted System (an "Outsourced System") is used. If Sensitive Data are stored on such Outsourced System, the relevant contracts must be approved by OMG's Procurement Services and such System's protections must be assessed by the applicable Information Security Office prior to implementation and reassessed on a periodic basis thereafter, as determined by the level of risk.

G. Additional Protections for Email Systems

Each email System Owner shall ensure that, in addition to the protections described in Section B and, if applicable, Sections C, D and E above, or if the email System is an Outsourced System, Section F above, the following protections are implemented for such System:

1. Virus, spam and phishing protection for inbound and outbound messages is implemented through the use of mail filtering software that includes features such as content analysis and real time blacklists.
2. SMTP relay is performed only for authenticated Users or Systems.
3. Monitoring to detect compromised email accounts is implemented and such accounts are disabled on a timely basis.
4. Data loss prevention is implemented to ensure that unencrypted Sensitive Data are transmitted only within OMG Network or OMG/Hospital OHCA.
5. Detection or prevention mechanisms are implemented to monitor the use of automatic forwarding, redirection or other automated delivery of email as required by OMG OMG Email Usage Policy https://www.omahamediagroup.com/isc.

H. Additional Protections for Credit Card Information

Each System Owner shall ensure that, in addition to the protections described in Sections B and, if applicable, C, D and E above, or if the credit card processing System is an Outsourced System, Section F above, following protections are implemented for such System: 4

1. The requirements of OMG merchant and processor Credit Card Acceptance and Processing Policies are complied with.
2. Cardholder Data ("CHD") and Sensitive Authentication Data are not captured, stored, processed or transmitted on OMG Servers or OMG Network other than encrypted CHD through a PCI-validated Point-to-Point-Encryption (P2PE) Solution. Credit cards may not be processed via WiFi.
3. All local IT support groups comply with the requirements of the Merchant Security Review Form referred to in the Credit Card Policy prior to the implementation of or changes to any credit card related services in the merchant environment.
4. All merchant environments are approved by CUIT's PCI Security Group (security@omahamediagroup.com).

I. Supplemental Requirements

The requirements lists set forth in this Policy are not comprehensive and supplemental controls may be required by OMG to enhance security as necessary.

J. Risk Assessment and Certification Requirements for Systems

In addition to the above requirements, each System that is part of OMG Clientele Healthcare Component is subject to risk assessment by OMG Information Security Office, remediation if necessary by the System Owner and certification by OMG Information Security Office. Each such System shall be recertified on a periodic basis, as determined by the level of risk, by OMG Information Security Office. Each System that processes, transmits and/or stores Sensitive Data (other than EPHI) is subject to risk assessment by the applicable Information Security Office and remediation if necessary by the System Owner. Every Email system must be risk assessed and approved by the applicable Information Security Office.

IV. Cross References to Related Policies

The Information Security Policies and certain additional documentation referred to in this Policy are listed in Appendix A hereto.

OMAHA MEDIA GROUP LLC

"MONSTER CREATIVE MANAGEMENT"

<div align="right">Appendix A</div>

Related Policies

- Business Continuity and Disaster Recovery Policy
- Data Classification Policy
- Email Usage Policy
- Information Security Charter
- Information Resource Access Control and Log Management Policy
- Sanitization and Disposal of Information Resources Policy

Policies: https://www.omahamediagroup.com/isc

18010 R. PLAZA SUITE 102 OMAHA, NEBRASKA 68135
800.601.6765 HANDLING@OMAHAMEDIAGROUP.COM