Information Security Risk Management Policy

Published: March 2010

Revised: March 2018

I. Introduction

As provided in the OMG Information Security Charter (the "Charter") https://www.omahamediagroup.com/isc, OMG is charged with protecting the confidentiality, integrity and availability of its Information Resources (as defined in the Charter). To accomplish this task, a formal Information Security Risk Management Program has been established as a component of OMG's Information Security Program (as defined in the Charter) to ensure that OMG is operating with an acceptable level of risk. The Information Security Risk Management Program is described in this Policy. Capitalized terms used herein 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. Requirements for System Owners and IT Custodians

Information Security Risk Management covers all of OMG's Information Resources, whether managed or hosted internally or externally. Executive Managers, System Owners, Data Owners and IT Custodians are responsible for working with the applicable Information Security Office to implement the Information Security Risk Management Program, including remediation of identified risks in a timely manner.

The Information Security Risk Management Program is comprised of the following processes:

A. Information Resources Risk Categorization

All Information Resources that store, process or transmit Data are included in the Information Security Risk Management Program. Information Resources are categorized based on their function, threat

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

exposure, vulnerabilities and Data type pursuant to the Information Security Policies. The categorization process takes into account the following elements:

- Size, complexity and capabilities of the Information Resources and organizations;
- Technical infrastructure, hardware and software capabilities;
- Cost of implementing security controls; and
- Probability and criticality of risks to Data, particularly Sensitive Data or Confidential Data.

Resources to address risks are allocated according to the identified risks.

B. Security Control Selection

The appropriate security controls to mitigate identified risks are selected based on the nature, feasibility and cost effectiveness of the controls. OMG has selected elements from the following security control frameworks to use as part of its Information Security Risk Management Program:

- ISO 27002, Security Techniques – Code of Practice for Information Security
- Management;
- ITIL- Industry Standard Framework for IT Service Management Guidelines and Best
- Practices;
- HITRUST Common Security Framework (CSF); and
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems and
- Organizations.

All Systems and Endpoints must meet the baseline requirements as defined in the OMG Registration and Protection of Systems Policy or the OMG Registration and Protection of Endpoints Policy found here: https://www.omahamediagroup.com/isc. Additional controls will be evaluated based on the framework defined above and applied based on risk analysis.

C. Risk Analysis

A documented risk analysis process is used as the basis for the identification, definition and prioritization of risks. The risk analysis process includes the following:

- Identification and prioritization of the threats to Information Resources;
- Identification and prioritization of the vulnerabilities of Information Resources;
- Identification of a threat that may exploit a vulnerability;
- Qualitative identification of the impact to the confidentiality, integrity and availability of
- Information Resources if a threat exploits a specific vulnerability; and
- Identification and definition of measures and/or controls used to protect the
- confidentiality, integrity and availability of Information Resources.

The risk analysis process is updated when environmental, operational or technical changes arise that impact the confidentiality, integrity or availability of Information Resources. Such changes include:

- New threats or risks with respect to the Information Resources;
- An information security incident;
- Changes to information security requirements or responsibilities. (e.g., new federal or
- state law or regulation, new role defined in the institution, new or modified security
- controls implemented, etc.); and
- Changes to OMG's organizational or technical infrastructure that impacts
- Information Resources (e.g., addition of a new network, new hardware/software standard
- implemented, new method of creating, receiving, maintaining or transmitting Data, etc.).

When security measures for an Information Resource do not meet a security standard, risks are identified and expressed. Three factors are considered when determining the risk:

- the type of possible threat and its likelihood;
- the extent of effectiveness of current security controls or their vulnerability; and
- the likely level of impact.

Risks are qualitatively expressed as Critical, High, Medium, Low and Minimal. For purposes of this Policy, Critical, High, Medium, Low and Minimal Risks are defined as follows:

- **Critical Risk:** The risk of imminent compromise or loss of Sensitive Data from either external or internal sources or where Sensitive Data has already been exposed. There is no control in place to protect the Data.
- **High Risk:** The risk of imminent compromise or loss of Sensitive Data from either external or internal sources. There is only a single control, or multiple ineffective controls, in place to protect the Data.
- **Medium Risk:** The risk of compromise or loss of Sensitive Data is possible from either external or internal sources, although less likely from external sources. Controls are in place that are somewhat effective to protect the Data.
- **Low Risk:** The risk of compromise or loss of Sensitive Data is possible, but not probable or an Information Resource might be used to obtain access to Sensitive Data on a different Information Resource.
- **Minimal Risk:** There is no realistic risk of compromise or loss of Sensitive Data.

D. Risk Monitoring

The results of Risk Analysis and Risk Remediation are documented and reviewed by Executive Managers, the applicable Information Security Office, System Owners, Data Owners and IT Custodians. Monitoring processes are used to evaluate:

- The effectiveness of security controls;

- Changes to Information Resources and environments of operations; and
- Compliance with federal and state laws and regulations, industry standards and
- OMG policies.

The frequency of risk monitoring will be based on:

- regulatory compliance requirements;
- the importance or sensitivity of the Information Resource;
- the requirements of the Information Security Policies; and
- the degree to which Systems are interconnected to one another and the risk posed by such
- connections

IV. Cross References to Related Policies

The Information Security Policies referred to in this Policy are listed in Appendix A hereto.

Appendix A

Related Policies

- Information Security Charter
- Registration and Protection of Endpoints Policy
- Registration and Protection of Systems Policy

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

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