



Office of the Comptroller  
May 20, 2011

W. Martin Morics, C.P.A.  
Comptroller

Michael J. Daun  
Deputy Comptroller

John M. Egan, C.P.A.  
Special Deputy Comptroller

Craig D. Kammholz  
Special Deputy Comptroller

To the Honorable Common Council  
City of Milwaukee

RE: IS Security Policy Audit

Dear Council Members: transmittal

As a component of the Comptroller's comprehensive information systems audit work plan, the IS security policy audit was conducted from December 2010 to March 2011 and involved the review of ITMD's IS security policies and guidelines. The audit consisted of the comprehensive review of the entire "Information Security Policies and Standards" document as well as the "Information Security Reference Manual."

A decentralized IT organization can lead to inconsistencies in applying enterprise level policies, procedure and guidelines as they pertain to City wide information systems security controls. Information technology has become increasingly important to the City's ability to function in recent years so ensuring that the City's security policies are current, relevant and adhere to IS security best practices is a necessity.

The "Information Security Policies and Standards" and "Information Security Reference Manual." were originally prepared by the Department of Administration in 1996 as a way to satisfy the need for information security policies and appropriate, measurable standards to be used in safeguarding the City's information and IS infrastructure. These two documents have constituted the core of the City's information security program. The latest review of these two documents was carried out by City's Chief Information Officer in August 2008.

Current IS security policies follow a rigorous and appropriate process for approval before they are published. Policy and guideline drafts are often developed in cross divisional collaborative groups and brought to the CIMC, a subcommittee of the Finance and Personnel Committee, for review, debate and ultimate approval. If the policy is approved by the CIMC, the chairman makes a recommendation to the Finance and Personal Committee to adopt the policy. IS security guidelines are published directly by the Chief Information Officer.

The "Information Security Policies and Standards" document consists of 11 sections covering the Standard IS security control framework. The sections include Security Management, Risk Assessment, Security Awareness, User Access, Authorized Use, Network Access, Security Logging and Tracking, Developmental Activities, Virus Protection, Licenses and Contingency Planning. The "Information Security Reference

Manual" is a companion document to the "Information Security Policies and Standards" which suggest practices and procedures to help implement the guidelines and policies. There were no IS security control sections omitted in the publication of these two documents. Audit conclusions from each section showing deficiencies are discussed below.

- Security Management

*1.0 and 1.1*

The security management section states that "The Information Resource Manager shall be responsible for overall development, coordination, administration and management of the program at the City-level and for establishing standards through which policy compliance will be measured." This position is, in effect, a Chief Information Security Officer. The guidelines also state that each division must appoint an Information Security Officer. The City does not currently have this Information Resource Manager/Chief Information Security Officer and no divisions with the exception of MPD have a dedicated Information Security Officer position. This position must either be filled/designated to carry out the above duties or guidelines must be written to assign security management to appropriate City personnel.

*1.8*

The guideline only offers a generic sentence stating "Each department, division, or agency must provide for the physical security of the information processing infrastructure." A specific physical security guideline should be adopted that lists specific minimum requirements of all City datacenters in protecting the City's information processing infrastructure.

- Risk Assessment

*2.2*

The guideline only offers a generic sentence stating "Each department, division, or agency must submit a written risk assessment update to IRM at least annually as part of an ongoing organizational risk assessment program." This is not currently being done. All City divisions should resume this risk assessment process or update the guidelines to remove this requirement.

- Network Access

*6.1*

The guideline refers to dial up modem connectivity criteria. This is a seldom used and outdated technology within the City and the standard should be updated to reflect the current use of this technology within the City.

- Developmental Activities

## 8.3

The guideline states that for developed software "system administrators and developers must rely on the access controls provided by an operating system or an access control system designed to enhance the operating system." This statement and its further guidelines contradict the best practices of application security leaving application data vulnerable should unauthorized users gain access to the City's network. It is a unanimous industry recommendation to have both operating system authentication controls and application level authentication controls in place to provide for strong data security.

The "Information Security Policies and Standards" and "Information Security Reference Manual" are a comprehensive collection of guidelines to govern the details of the City's information security program. These guidelines are not enforceable and thus, it is not mandatory for City divisions to comply with them. The City's Chief Information Officer is charged with the governance and security of the City's computer environment but has no enforcement authority outside of ITMD. In recent years some guidelines have been enhanced and turned into policies. These Policies are adopted by the Common Council and thus, require full compliance from City divisions.

Five Information Systems policies have been developed and adopted in the last 18 months. These policies include; Email Use Policy, Website Linking Policy, Email Disclaimer Policy, Social Media Policy and Password Policy. These are strong policies that should be incorporated into the City's overall information security program by including them in the "Information Security Policies and Standards" and the "Information Security Reference Manual."

The audit indicates that the City's "Information Security Policies and Standards" and "Information Security Reference Manual" are generally in good operational standing but need to be updated on a more regular schedule. The audit found that four out of eleven IS security control framework sections needed some form of update or improvement. The remaining seven sections did not have any exceptions identified. Recommendations for improvement have been communicated to the appropriate City personnel. A management response to the exceptions is attached to this document.

## **1. IS security polices and guidelines are not updated annually**

**Recommendation:** The CIO should conduct a thorough review of all City IS policies and guidelines on an annual basis. The last review was conducted in August 2008.

**2. There are no formal channels of authority to enforce IS security guidelines.**

**Recommendation:** Per the "Information Security Policies and Standards" document, "Compliance is to be enforced through current administrative procedures and is the responsibility of City managers and appointed Information Security Officers." City Divisions should clearly define the roles of CISO/ISO and hire or appoint qualified personnel to carry out IS security duties and enforce Security Policies and controls. Otherwise, full responsibility and authority to enforce IS security policies and guidelines should be given to the Chief Information Officer as is done in many other organizations.

**3. Annual Information System Risk Assessments are not currently completed and submitted by City divisions.**

**Recommendation:** All City division should resume this risk assessment process or update the guidelines to remove this requirement.

**4. The current Physical Security guideline is vague.**

**Recommendation:** A specific physical security guideline should be adopted that lists specific minimum requirements of all City datacenters in protecting the City's information processing infrastructure.

**5. The Development guideline prohibits the development and inclusion of application level security/authentication controls on custom development applications.**

**Recommendation:** This guideline could lead to a weakness in application level security and should be removed from the guidelines.

All City employees who participated in this audit should be commended for their availability and cooperation throughout the IS Security Policy Audit process. The Comptroller thanks all parties involved in this audit for their enthusiastic cooperation with the auditor.

Sincerely,



W. MARTIN MORICS  
Comptroller



COMPTROLLER

Tom Barrett  
Mayor

2011 MAY 19 AM 11:58  
Department of Administration  
Information and Technology  
Management Division

Sharon D. Robinson  
Administration Director

Nancy A. Olson  
Chief Information Officer

Date: May 11<sup>th</sup>, 2011  
To: Mr. Wally Morics  
From: Nancy A Olson, Chief Information Officer *NAO*  
Re: 2011 IS Security Policy Audit

Dear Mr. Morics:

In response to the findings of the April 29<sup>th</sup>, 2011 DOA/ITMD IS security policy audit, I would first like to highlight two salient points that directly affect the current state of IT security in the City of Milwaukee.

- IT Security is implemented using a decentralized (departmental) approach, not a centralized model.
- No dedicated IT Security staffing exists in ITMD or departments

Given the limitations mentioned above, I offer the following proposals as the best approach, to resolving specific audit findings, and reducing/removing these findings in future audits.

- 1) **IS security polices and guidelines are not updated annually.** As CIO, I will review and update the IS security policy on an annual basis.
- 2) **There are no formal channels of authority to enforce IS security guidelines.**  
Enforcement authority has been given to the Chief Information Officer by City Ordinance Section 310-7-3-a which reads; "All departments and agencies shall comply with the information technology plan, standards, policies, guidelines and systems established by the department of administration. The department of administration may grant exceptions based on unique departmental business needs."  
  
In the future the CIO will inform departments of updates to the IT Security guidelines and advise them of their security-related responsibilities. To facilitate communication with City departments, the CIO will review and update the outdated existing list of Information Security Officers (ISOs). The City Information Management Committee (CIMC) may elect to review the policies and guidelines put forth in this document and create formal policies on specific topic around IT security in the future.
- 3) **Annual Information System Risk Assessments are not currently completed and submitted by City divisions.** The CIO will review this requirement and determine an agreeable and manageable approach for implementation which can be accomplished using existing staff.
- 4) **The current Physical Security guideline is vague.** Templates that outline current "best practices" for disaster recovery plans/physical security that have been developed under the IT Disaster Recovery audit will be included in the IS Security Policy document.

- 5) **The Development guideline prohibits the development and inclusion of application level security/authentication controls on custom development applications.** This statement is incorrect and will be removed from the IT Security Policies and Standards document.

If you have questions or need additional details, please do not hesitate to contact me at extension 8710 or at [Nancy.Olson@milwaukee.gov](mailto:Nancy.Olson@milwaukee.gov) .

C: Sharon Robinson