Legislation Details (With Text)

File #:	14-1481	**Version:** 2	**Name:**	Information Security Ordinance	
Type:	Ordinance		**Status:**	Approved	
File created:	2/10/2014		**In control:**	Technology and Innovation Committee	
On agenda:	2/19/2014		**Final action:**	6/18/2014	
Title:	PROPOSED SUBSTITUTE TO 14-1481				

PROPOSED ORDINANCE

COOK COUNTY INFORMATION SECURITY ORDINANCE
WHEREAS, technology and information resources in the various agencies and departments funded by the Cook County Board of Commissioners are strategic and vital assets belonging to the people of the County and State; and
WHEREAS, Cook County has a responsibility to the citizens of Cook County to ensure that the information entrusted to these agencies is safe, secure, and protected from unauthorized access, use, or destruction; and
WHEREAS, coordinated efforts are encouraged to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information; and
WHEREAS, a strong information security framework should be coordinated, promulgated and implemented throughout agencies funded by the County, including the offices of the separately elected County and State Officials, to ensure the development and maintenance of minimum information security controls to protect technology and information resources that support the operations and assets of said agencies and departments and to enable the protection of the public health, safety, morals and welfare.
NOW THEREFORE BE IT ORDAINED, by the Cook County Board of Commissioners that Chapter 2 Administration, Article XII, Cook County Information Security Ordinance, Sec. 2-960 through 2-967 of the Cook County Code, is hereby enacted as follows:
ARTICLE XII. Cook County Information Security

Sec. 2-960. Short title.

This article shall be known and may be cited as the “Cook County Information Security Ordinance.”

Sec. 2-961. Purpose and Policy.
All separately elected County and State Officials, Departments, Office Institutions or Agencies funded by the Cook County Board of Commissioners, including but not limited to the offices and departments under the control of the County Board President, the Board of Commissioners, Cook County Health and Hospitals System, State’s Attorney of Cook County, Cook County Sheriff, Cook County Public Defender, Illinois Clerk of the Circuit Court of Cook County, Cook County Treasurer, Cook County Clerk, Cook County Recorder of Deeds, Cook County Assessor, Chief Judge of the Circuit Court of Cook County, Board of Review, Cook County Public Defender, Cook County Independent Inspector General, Cook County Veteran’s Assistance Commission and the Public Administrator (collectively, “Agency”) shall take all appropriate precautions to protect the confidentiality, integrity, and availability of information. Such precautions shall be in accordance with applicable Federal and State laws and regulations and take into consideration industry standards and best practices.
Sec. 2-962. Countywide Information Security Working Group.
(a) An Information Security Working Group shall be composed of the directors of the information systems for all Agencies set forth in Section 2-961, or the directors’ designees.
(b) The Bureau of Technology’s Chief Information Security Officer (“CISO”) shall be the chair of the Information Security Working Group.
Sec. 2-963. Definitions.

The following words, terms and phrases, when used in this article shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:
Guideline means a recommendation to assist an Agency employee or contractor in making appropriate decisions or performing a particular task, which allows for latitude in interpretation and implementation.
Plan means a comprehensive document that details strategic direction, which may also provide additional details, such as Standards used and so forth.
Policy means a document that communicates leadership expectations to a business unit or department of an Agency, which may also be considered as mandatory business rules or organization -specific directives and which are communication of management intent.
Procedure means a document stating the manner in which a Policy shall be functionally implemented in an Agency's environment, which may define specific operation steps, manual methods, or instructions for compliance with a Policy.
Standard means a document that contains a specification or describes minimum implementation that satisfies a Policy.
Sec. 2-964. Information Security Framework.
(a) The Information Security Working Group shall assist the CISO in creating, and updating as necessary, comprehensive and written information security Plans, Policies, Procedures, Standards, and Guidelines for the Agencies (collectively, the "Information Security Framework") to reasonably protect the confidentiality, integrity, and availability of Agency information.
(b) In creating and updating the Information Security Framework, the CISO shall seek the advice and recommendations of each Agency in order to ensure that the Information Security Framework addresses unique considerations of said Agency; all Agencies shall advise and collaborate with the CISO in the creation of the Information Security Framework.
(c) The Information Security Framework shall: (1) be in accordance with applicable Federal and State laws and regulations; (2) state all Agencies' minimum requirements and precautions to protect the confidentiality, integrity, and availability of Agencies' information; (3) address the unique considerations of each Agency in a manner that does not unduly interfere with the operations of such Agency or any confidentiality or privilege required for such operations; and (4) take into consideration industry standards and best practices by including critical and necessary components of any such similar framework, for example, risk management processes, information security incident response plans, and data breach notification plans.
Sec. 2-965. Adoption and Compliance
(a) The Bureau of Technology's Chief Information Officer ("CIO") and CISO shall publish and make available the Information Security Framework to all Agencies; said Agencies shall adopt and comply with the Information Security Framework in a reasonable time, except as set forth in subsections (b) and (c) of this section. The CIO, CISO and Agencies shall not otherwise disclose the Information Security Framework except as required to further the security of the various information systems or as required by law.
(b) After publication of the Information Security Framework, Agencies may deviate from the Information Security Framework based on their unique requirements, but only upon the approval of the Information Security Working Group and signing of a mutual agreement that would be executed by the CISO and the Agency following the Information Security Working Group approval.
(c) After publication of the Information Security Framework, any Agency not under the control of the County Board President may elect to not adopt and comply with the Information Security Framework by sending written notice to the CIO, the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners within ninety calendar days after such publication; provided that to the extent that such Agency continues to use or access information systems under the management or control of the CIO, the CIO may only allow such Agency to use and access such information systems in a manner consistent with the use and access conditions of the Information Security Framework.
(1) Any Agency not under the control of the County Board President that elects to not adopt and comply with the Information Security Framework under this subsection may, subsequently and at any time, elect to adopt and comply with the Information Security Framework by giving written notice ninety calendar days' in advance to the CIO, the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners.
(2) The adoption and compliance with the Information Security Framework, or the lack thereof, shall not affect any rights and responsibilities arising under any law, including the Illinois Constitution, the Illinois Counties Code, or the Code of Ordinance of Cook County, Illinois.

(d) Agencies adopting the Information Security Framework shall take all appropriate actions, including completing assigned training and if warranted, initiating disciplinary action, to ensure their employees and contractors adopt and comply with the Information Security Framework.
Sec. 2-966. Review, Remediation and Enforcement
(a) No less than annually, the CISO shall review and determine the status of Agency adoption and compliance with the Information Security Framework and whether an Agency's use and access of County information systems adheres to the use and access conditions of the Information Security Framework.
(b) Where the CISO has determined that an Agency has not fully adopted or complied with, or uses or access County information systems contrary to, the Information Security Framework, the CIO and CISO shall notify the Information Security Working Group and that Agency to remediate such deficiencies in adoption, compliance, use or access in a reasonable time; and the CISO shall assist such Agency with its remediation effort if requested.
(c) The CIO and CISO shall be authorized to take all other appropriate actions to protect the County's network that are consistent with the requirements of the Information Security Framework.
(d) Where an Agency disagrees with the CISO's determination that such Agency has not fully adopted or complied with, or uses or access County information systems contrary to, the Information Security Framework, then such Agency may request that the Information Security Working Group review and determine the status of such Agency's adoption and compliance with the Information Security Framework. The CISO shall follow the Information Security Working Group's determinations.
Sec. 2-967. Reporting.
(a) At least once each calendar year, the CISO shall report to the Information Security Working Group on the Information Security Framework.
(b) At a minimum, the CISO's annual report shall detail: (i) the status of all Agencies' adoption and compliance with the Information Security Framework, and (ii) a summary of all advice and recommendations of each Agency regarding their unique considerations. Based on information provided by the Information Security Working Group, the CISO may modify his or her annual report.
(c) The CIO shall present the CISO's annual report to the Cook County Board of Commissioners following the presentation of that report to the Information Security Working Group.

Effective date: This ordinance shall be in effect immediately upon adoption

Sponsors: JOHN A. FRITCHEY, TONI PRECKWINKLE (President)

Indexes: (Inactive) MARY JO HORACE, Bureau of Technology

Code sections:

Attachments:

Date	Ver.	Action By	Action	Result
6/18/2014	2	Board of Commissioners	approve	
6/18/2014	2	Board of Commissioners	approve	
6/17/2014	1	Technology and Innovation Committee	recommend for approval as substituted	
2/19/2014	1	Board of Commissioners	refer	Pass

PROPOSED SUBSTITUTE TO 14-1481

PROPOSED ORDINANCE

COOK COUNTY INFORMATION SECURITY ORDINANCE

WHEREAS, technology and information resources in the various agencies and departments funded by the Cook County Board of Commissioners are strategic and vital assets belonging to the people of the County and State; and

WHEREAS, Cook County has a responsibility to the citizens of Cook County to ensure that the information entrusted to

these agencies is safe, secure, and protected from unauthorized access, use, or destruction; and

WHEREAS, coordinated efforts are encouraged to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information; and

WHEREAS, a strong information security framework should be coordinated, promulgated and implemented throughout agencies funded by the County, including the offices of the separately elected County and State Officials, to ensure the development and maintenance of minimum information security controls to protect technology and information resources that support the operations and assets of said agencies and departments and to enable the protection of the public health, safety, morals and welfare.

NOW THEREFORE BE IT ORDAINED, by the Cook County Board of Commissioners that Chapter 2 Administration, Article XII, Cook County Information Security Ordinance, Sec. 2-960 through 2-967 of the Cook County Code, is hereby enacted as follows:

ARTICLE XII. Cook County Information Security

Sec. 2-960. Short title.

This article shall be known and may be cited as the "Cook County Information Security Ordinance."

Sec. 2-961. Purpose and Policy.

All separately elected County and State Officials, Departments, Office Institutions or Agencies funded by the Cook County Board of Commissioners, including but not limited to the offices and departments under the control of the County Board President, the Board of Commissioners, Cook County Health and Hospitals System, State's Attorney of Cook County, Cook County Sheriff, Cook County Public Defender, Illinois Clerk of the Circuit Court of Cook County, Cook County Treasurer, Cook County Clerk, Cook County Recorder of Deeds, Cook County Assessor, Chief Judge of the Circuit Court of Cook County, Board of Review, Cook County Public Defender, Cook County Independent Inspector General, Cook County Veteran's Assistance Commission and the Public Administrator (collectively, "Agency") shall take all appropriate precautions to protect the confidentiality, integrity, and availability of information. Such precautions shall be in accordance with applicable Federal and State laws and regulations and take into consideration industry standards and best practices.

Sec. 2-962. Countywide Information Security Working Group.

(a) An Information Security Working Group shall be composed of the directors of the information systems for all Agencies set forth in Section 2-961, or the directors' designees.

(b) The Bureau of Technology's Chief Information Security Officer ("CISO") shall be the chair of the Information Security Working Group.

Sec. 2-963. Definitions.

The following words, terms and phrases, when used in this article shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

Guideline means a recommendation to assist an Agency employee or contractor in making appropriate decisions or

performing a particular task, which allows for latitude in interpretation and implementation.

Plan means a comprehensive document that details strategic direction, which may also provide additional details, such as Standards used and so forth.

Policy means a document that communicates leadership expectations to a business unit or department of an Agency, which may also be considered as mandatory business rules or organization-specific directives and which are communication of management intent.

Procedure means a document stating the manner in which a Policy shall be functionally implemented in an Agency's environment, which may define specific operation steps, manual methods, or instructions for compliance with a Policy.

Standard means a document that contains a specification or describes minimum implementation that satisfies a Policy.

Sec. 2-964. Information Security Framework.

(a) The Information Security Working Group shall assist the CISO in creating, and updating as necessary, comprehensive and written information security Plans, Policies, Procedures, Standards, and Guidelines for the Agencies (collectively, the "Information Security Framework") to reasonably protect the confidentiality, integrity, and availability of Agency information.

(b) In creating and updating the Information Security Framework, the CISO shall seek the advice and recommendations of each Agency in order to ensure that the Information Security Framework addresses unique considerations of said Agency; all Agencies shall advise and collaborate with the CISO in the creation of the Information Security Framework.

(c) The Information Security Framework shall: (1) be in accordance with applicable Federal and State laws and regulations; (2) state all Agencies' minimum requirements and precautions to protect the confidentiality, integrity, and availability of Agencies' information; (3) address the unique considerations of each Agency in a manner that does not unduly interfere with the operations of such Agency or any confidentiality or privilege required for such operations; and (4) take into consideration industry standards and best practices by including critical and necessary components of any such similar framework, for example, risk management processes, information security incident response plans, and data breach notification plans.

Sec. 2-965. Adoption and Compliance

(a) The Bureau of Technology's Chief Information Officer ("CIO") and CISO shall publish and make available the Information Security Framework to all Agencies; said Agencies shall adopt and comply with the Information Security Framework in a reasonable time, except as set forth in subsections (b) and (c) of this section. The CIO, CISO and Agencies shall not otherwise disclose the Information Security Framework except as required to further the security of the various information systems or as required by law.

(b) After publication of the Information Security Framework, Agencies may deviate from the Information Security Framework based on their unique requirements, but only upon the approval of the Information Security Working Group and signing of a mutual agreement that would be executed by the CISO and the Agency following the Information Security Working Group approval.

(c) After publication of the Information Security Framework, any Agency not under the control of the County Board President may elect to not adopt and comply with the Information Security Framework by sending written notice to the CIO, the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners within ninety calendar days after such publication; provided that to the extent that such Agency continues

to use or access information systems under the management or control of the CIO, the CIO may only allow such Agency to use and access such information systems in a manner consistent with the use and access conditions of the Information Security Framework.

(1) Any Agency not under the control of the County Board President that elects to not adopt and comply with the Information Security Framework under this subsection may, subsequently and at any time, elect to adopt and comply with the Information Security Framework by giving written notice ninety calendar days' in advance to the CIO, the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners.

(2) The adoption and compliance with the Information Security Framework, or the lack thereof, shall not affect any rights and responsibilities arising under any law, including the Illinois Constitution, the Illinois Counties Code, or the Code of Ordinance of Cook County, Illinois.

(d) Agencies adopting the Information Security Framework shall take all appropriate actions, including completing assigned training and if warranted, initiating disciplinary action, to ensure their employees and contractors adopt and comply with the Information Security Framework.

Sec. 2-966. Review, Remediation and Enforcement

(a) No less than annually, the CISO shall review and determine the status of Agency adoption and compliance with the Information Security Framework and whether an Agency's use and access of County information systems adheres to the use and access conditions of the Information Security Framework.

(b) Where the CISO has determined that an Agency has not fully adopted or complied with, or uses or access County information systems contrary to, the Information Security Framework, the CIO and CISO shall notify the Information Security Working Group and that Agency to remediate such deficiencies in adoption, compliance, use or access in a reasonable time; and the CISO shall assist such Agency with its remediation effort if requested.

(c) The CIO and CISO shall be authorized to take all other appropriate actions to protect the County's network that are consistent with the requirements of the Information Security Framework.

(d) Where an Agency disagrees with the CISO's determination that such Agency has not fully adopted or complied with, or uses or access County information systems contrary to, the Information Security Framework, then such Agency may request that the Information Security Working Group review and determine the status of such Agency's adoption and compliance with the Information Security Framework. The CISO shall follow the Information Security Working Group's determinations.

Sec. 2-967. Reporting.

(a) At least once each calendar year, the CISO shall report to the Information Security Working Group on the Information Security Framework.

(b) At a minimum, the CISO's annual report shall detail: (i) the status of all Agencies' adoption and compliance with the Information Security Framework, and (ii) a summary of all advice and recommendations of each Agency regarding their unique considerations. Based on information provided by the Information Security Working Group, the CISO may modify his or her annual report.

(c) The CIO shall present the CISO's annual report to the Cook County Board of Commissioners following the presentation of that report to the Information Security Working Group.

Effective date: This ordinance shall be in effect immediately upon adoption