SECOND SUBSTITUTE TO FILE 16-2289
2/8/2017
LEGISLATION AND INTERGOVERNMENTAL RELATIONS COMMITTEE

Sponsored by: LARRY SUFFREDIN, County Commissioner

PROPOSED ORDINANCE AMENDMENT

AN AMENDMENT TO THE COOK COUNTY ETHICS ORDINANCE

BE IT ORDAINED, by the Cook County Board of Commissioners, that Chapter 2 - Administration, ARTICLE XII. - COOK COUNTY INFORMATION SECURITY is hereby amended 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 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 Chief Information Security Officer (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 Chief Information Security Officer (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 Chief Information Security Officer (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.

(5) Include an Acceptable Use Policy compliant with Section 2-965 of this Article.

Sec. 2-965. – Acceptable Use Policy for Information Technology Resources.

(a) On or before April 17, 2017 ~~January 1, 2017~~, the Information Security Working Group shall create, circulate and update as necessary, an Acceptable Use Policy for Information Technology Resources, addressing issues including but not limited to: the use of County-owned or County-leased computers, telephones, software, social media and electronic communication accounts; and, the use of devices, email accounts, and other electronic communications media that are not County-owned or are not official government email accounts but are used partially or entirely for County business (i.e., formalizing or perpetuating knowledge, setting policy, establishing guidelines or procedures, certifying a transaction or issuing a receipt).

(b) Notwithstanding the above, separately elected officials and their designated senior staff as well as designated Cook County Health and Hospitals System senior staff and physicians may use non-

County or non official government email accounts to conduct County business provided ~~provided that the separately elected officials~~ such users (1) cooperate with the County to ensure compliance with applicable law including, but not limited to, the Illinois Freedom of Information Act (5 ILCS 140) and the Illinois Local Records Act (50 ILCS 205); (2) notify the CISO on an annual basis whether non-County or non-official government email accounts are being used for official government business and; (3) notify the Information Security Working Group immediately in the event that a non-County or non-official government email account used to conduct County business or a device used to access such account is lost, stolen, or breached.

(c) Separately elected officials and their designated senior staff as well as designated Cook County Health and Hospitals System senior staff and physicians utilizing non-County or non-official government email accounts partially or entirely for County business shall agree to provide the applicable County Freedom of Information Act Officer any records that may be responsive to Freedom of Information Act requests, including any records and communications pertaining to County business conducted on non-County email accounts promptly upon request by the applicable County Freedom of Information Act Officer for review and/or disclosure to ensure compliance with applicable law.

Sec. 2-96~~5~~6. – Adoption and compliance.

(a) The Bureau of Technology's Chief Information Officer ("CIO") and Chief Information Security Officer (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 Chief Information Officer (CIO), Chief Information Security Officer (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 Chief Information Security Officer (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 Chief Information Officer (CIO), the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners within 90 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 Chief Information Officer (CIO), the Chief Information Officer (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 90 calendar days' in advance to the Chief Information Officer (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. 2-96~~6~~7. - Review, remediation and enforcement.

(a) No less than annually, the Chief Information Security Officer (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 Chief Information Security Officer (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 Chief Information Officer (CIO) and Chief Information Security Officer (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 Chief Information Security Officer (CISO) shall assist such Agency with its remediation effort if requested.

(c) The Chief Information Officer (CIO) and Chief Information Security Officer (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 Chief Information Security Officer's (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 Chief Information Security Officer (CISO) shall follow the Information Security Working Group's determinations.

Sec. 2-96~~7~~8. - Reporting.

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

(b) At a minimum, the Chief Information Security Officer's (CISO's) annual report shall detail:

(1) The status of all Agencies' adoption and compliance with the Information Security Framework; and

(2) 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 Chief Information Security Officer (CISO) may modify his or her annual report.

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

Secs. 2-96~~8~~9—2-999. - Reserved.