File #: Int 0664-2011, **Version:** *

Int. No. 664

By Council Members Brewer, Cabrera, Arroyo, Comrie, James, Rivera, Rose, Van Bramer, Palma, Fidler, Jackson, Lander, Koppell, Vacca, Vann, Koo and Halloran

A Local Law to amend the administrative code of the city of New York, in relation to personal information security.

Be it enacted by the Council as follows:

Section 1. Title 10 of the administrative code of the city of New York is amended by adding a new chapter 9 to read as follows:

Chapter 9 - PERSONAL INFORMATION SECURITY

§10-901 Personal information security

§10-901 Personal information security. a. As used in this chapter, "personal information" shall mean any information concerning an individual which, because of a name, number, symbol, mark or other identifier, can be used to identify that individual.

b. Each agency that maintains a system of records containing personal information shall develop, implement, and maintain a comprehensive security program that contains administrative, technical, and physical safeguards for the protection of such personal information. Such comprehensive security program shall be consistent with federal and state laws and regulations.

c. Where not inconsistent with applicable federal and state laws and regulations, every comprehensive security program shall include, but shall not be limited to, 1. designating one or more employees to maintain the comprehensive information security program;

2. identifying and assessing foreseeable internal and external risks to the security, confidentiality, and/or

integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to, ongoing employee training, employee compliance with policies and procedures, and a means for detecting and preventing security system failures;

3. developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;

4. imposing disciplinary measures for violations of the comprehensive information security program rules;

5. preventing persons whose employment with the agency has been terminated from the agency from accessing records containing personal information;

6. restrictions upon physical access to records containing personal information, including the storage of such records and data in locked facilities, storage areas or containers;

7. regular monitoring to ensure that the comprehensive information security program is operating in a manner calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks;

8. reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may implicate the security or integrity of records containing personal information; and

9. documenting any incident involving a breach of security, responsive actions taken in connection with such incident and performing a mandatory post-incident review of events including changes made, if any, to business practices relating to protection of personal information.

d. Where not inconsistent with applicable federal and state laws and regulations, if an agency electronically stores or transmits records containing personal information the comprehensive information security program of such agency shall include, but not be limited to, 1. secure user authentication protocols

including control of user identification cards and other record access identifiers; a secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; control of data security passwords to ensure that such passwords are kept in a location or format that does not compromise the security of the data they protect; restricting access to active users and active user accounts only; and blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

2. secure access control measures that restrict access to records and files containing personal information to those who need such information to perform their job duties and to assign unique identifications and passwords, which are not vendor supplied default passwords, to each person with computer access, that are designed to maintain the integrity of the security of the access controls;

3. encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

4. encryption of all personal information stored on laptops or other portable devices;

5. encryption of all personal information stored on removable media that is transported or stored by third-party service providers;

6. monitoring of systems for unauthorized use of or access to personal information;

7. for files containing personal information on a system that is connected to the Internet, there must be up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the personal information;

8. up-to-date versions of system security agent software which must include malware protection and up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and

9. education and training of employees on the proper use of the applicable computer security system and the importance of personal information security.

e. Each agency that maintains a system of records containing personal information shall take steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with this chapter and any applicable federal and state laws and regulations, and require such third-party service providers to implement and maintain such appropriate security measures for personal information.

§2. This local law shall take effect one year after its enactment, except that the commissioner or director of each agency shall take such actions as are necessary for its implementation, including the promulgation of rules, prior to such effective date.

jtb
LS# 2212
Cr-6/2/2011 Sv-6/24/2011 12:27:00 PM