The BOARD of ELECTION COMMISSIONERS
for the CITY of CHICAGO

Information Security and Identity Protection Policy

I. Introduction

A. The Board of Election Commissioners (Board) intends to manage its information technology and information assets to maximize their efficient, effective, and secure use in support of the Board's business and its constituents and to prevent unauthorized or unlawful disclosure of Social Security numbers or other personal information.

B. This document, the Information Security and Identity Protection Policy (Policy), defines the governing principles for the secure operation and management of the information technology used, administered, and/or maintained by the Board and for the protection of the Board's information assets and individual identity.

C. Violations of the Board's Information Security and Identity Protections Policy must be reported to the Board's Executive Director.

II. Purpose

A. To define the responsibilities of the Board's officers, employees, vendors, consultants, agents and others with respect to appropriate use and protection of the Board's information assets and technology.

B. To ensure that the Board's information assets and technology are secure from unauthorized access, misuse, disclosure, degradation, or destruction.

III. Scope

A. This Information Security and Identity Protection Policy applies to the Board of Election Commissioners and its officers, employees, temporary employees, interns, vendors, consultants, contractors and agents thereof - collectively referred to as "User(s)". The principles set forth in this Policy are applicable to all information technology and assets, in all formats, used by the Board.

B. This Policy does not create any rights, constitute a contract, or contain the terms of any employment contract or other contract between the Board of Election Commissioners, any employee or applicant for employment, or any other person. Rather, this Policy details certain purposes, procedures, guidelines, responsibilities, and other matters the Board of Election Commissioners deems relevant to its management of information assets. The Board reserves the right to amend this Policy or any part or provision of it.

IV. Definitions

Please familiarize yourself with the definitions in appendix A as part of your understanding of this Policy.

V. Organizing Information Security

A. Information Security. The Department of Electronic Voting Systems is responsible for designing, implementing and maintaining a Board-wide information security program – in conjunction with other departments – and for assisting all Board departments in implementing and maintaining information management practices at their respective locations.

B. Confidentiality Agreements. Employees, consultants, contractors or other persons who use the Board's information technology are required to read, understand, and agree to the Board's Confidentiality and Acceptable Use Agreement regarding their responsibilities and conduct related to the protection of the Board's information assets and technology.

C. Third Parties. The Board often utilizes third parties in support of delivering business services. When, as a result, these arrangements extend the Board's information technology enterprise or business processes into the third parties' computing environments – for example, in cases of Application Service Providers (ASPs) – the third parties must abide by this Policy, as applicable, unless specific additional provisions have been established through contractual agreements.

VI. Asset Management

A. Information Classification. The Board's information, whether in electronic or physical form, can be categorized into three classifications. Due care must be taken to protect the Board's information assets in accordance with the three classifications, as described within this Policy.

1. Confidential. Sensitive personally identifiable information (PII) used for business purposes within the Board which, if disclosed through unauthorized means, could adversely affect registered voters and the Board's personnel, including employees and constituents, and could have legal, statutory, or regulatory repercussions. Examples include: information exempt from disclosure under the Illinois Freedom of Information Act ("FOIA"), information protected from disclosure under the federal Health Insurance Portability and Accountability Act ("HIPPA"), other personnel information including Social Security numbers, driver's license numbers, State identification card numbers, telephone numbers and personal financial information protected by the Illinois Personal Information Protection Act ("PIPA").

2. Internal. Information related to the Board's business that if disclosed, accessed, modified or destroyed by unauthorized means, could have limited or significant financial or operational impact on the Board. Examples include: strategic plans, vendors' proprietary information, responses to Requests for Proposals (RFPs), information protected by intergovernmental non-disclosure agreements or other non-disclosure agreements, and design documents. Other information related to the Board's information technology that is considered Internal includes dial-up modem phone numbers and access point Internet Protocol (IP) addresses.

3. Public. Information intended for unrestricted public disclosure in the course of the Board's business. Examples include: certain voter registration information data, certain election information and records, forms, press releases, public information materials, and competitive bid and employment advertisements.

B. Responsibility for Assets

1. Ownership of Assets. All information stored and processed over the Board's technology systems is the property of the Board. Users of the system have no expectation of privacy associated with the information they store in or send through these systems, within the limits of the federal, state and local laws and, where applicable, foreign laws.

2. Acceptable and Unacceptable Use of Assets

a. To effectively conduct the Board's business and operations, the Board makes available to authorized employees and third parties various information technology resources, including e-mail, the Board's Intranet, the Internet, and other communication and productivity tools. Use of these resources is intended for business purposes in accordance with Users' job functions and responsibilities, with limited personal use permitted only in accordance with

the Board's personnel rules, this Policy, and other applicable Board policies. The limited personal use of information technology resources is not permissible if it creates a non-negligible expense to the Board, consumes excessive time, or violates departmental policy. The privilege of limited personal use may be revoked or limited at any time by the Board or department officials.

b. Board employees are required to use only Board authorized e-mail addresses and servers when communicating with others via e-mail concerning matters of Board business – use of personal or private e-mail addresses to communicate regarding Board business is prohibited.

c. Users must not allow any consultant, visitor, friend, family member, customer, vendor or other unauthorized person to use their network account, e-mail address or other Board-provided computer facilities. Users are responsible for the activities performed by and associated with the accounts assigned to them by the Board.

d. No User may use Board-provided Internet or Intranet access or the Board's Confidential, Internal or Public information to solicit or conduct any personal commercial activity or for personal gain or profit or non-Board approved solicitation.

e. Users must not make statements on behalf of the Board or disclose Confidential or Internal Board information unless expressly authorized in writing by their Department Management. This includes Internet postings, or bulletin boards, news groups, chat rooms, or instant messaging.

f. Users must protect Confidential or Internal information being transmitted across the Internet or public networks in a manner that ensures its confidentiality and integrity between a sender and a recipient. Confidential information such as Social Security numbers and electronic Protected Health Information (ePHI) must be transmitted using encryption software.

g. Internal information such as e-mail lists must not be posted to any external information source, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the prior express written permission of the User's Department Management.

h. Users must not install software on the Board's network and computer resources without prior express written permission from the Department of Electronic Voting Systems. Person-to-person (P2P) applications, Voice over IP (VOIP), instant messenger (IM) applications, and remote access applications pose an especially high risk to the Board and their unauthorized use is strictly prohibited. Board business must not be conducted on any device that allows P2P communication (such as file sharing music applications) without explicit approval from the Department of Electronic Voting Systems.

i. Users must not copy, alter, modify, disassemble, or reverse engineer the Board's authorized software or other intellectual property in violation of licenses provided to or by the Board. Additionally, Users must not download, upload, or share files in violation of U.S. patent, trademark, or copyright laws. Intellectual property that is created for the Board by its employees, vendors, consultants and others is property of the Board unless otherwise agreed upon by means of third party agreements or contracts.

j. Users must not access the Internet, the Intranet or e-mail to use, upload, post, mail, display, or otherwise transmit in any manner any content, communication, or information that, among other inappropriate uses:

i. interferes with official Board business;

ii. is hateful, harassing, threatening, libelous or defamatory, pornographic, profane, or sexually explicit;

iii. is deemed by the Board to offend persons based on race, ethnic heritage, national origin, sex, sexual orientation, age, physical or mental illness or disability, marital status, employment status, housing status, religion, or other characteristics that may be protected by applicable civil rights laws;

iv. impersonates a person (living or dead), organization, business, or other entity;

v. enables or constitutes gaming, wagering or gambling of any kind;

vi. promotes or participates in unauthorized fundraisers;

vii. promotes or participates in partisan political activities;

viii. promotes or participates in unauthorized advertising of Board projects and any advertising of private projects;

ix. compromises or degrades the performance, security, or integrity of the Board's technology resources and information assets;

x. contains a virus, logic bomb, or malicious code;

xi. constitutes participation in chain letters, unauthorized chat rooms, unauthorized instant messaging, spamming, or any unauthorized auto-response program or service.

C. Identity Protection

1. Neither the Board nor any User may publicly post, publicly display or publicly disclose in any manner an individual's e-mail address or telephone number or an individual's Social Security number, driver's license number, or State identification card number, except for the last four digits of such numbers.

2. Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses or telephone numbers, when requested from individuals registering to vote or applying to register to vote, shall be placed in a discrete location on a standardized form and such numbers shall be redacted from such form if the form is required to be released as part of a public records request.

3. Neither the Board nor any User may print an individual's Social Security number, driver's license number, or State identification card number, except for the last four digits of such numbers, on any voter registration card or application form, or on any application for ballot.

4. Neither the Board nor any User may print an individual's Social Security number, driver's license number, State identification card number or telephone number, in whole or in part, on any materials that are mailed to the individual through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless state or federal law requires it and unless enclosed in an envelope so that such numbers are not visible without the envelope having been opened.

5. Neither the Board nor any User may collect a Social Security number, except for the last four digits of such number, from any individual seeking to register to vote.

6. Neither the Board nor any User shall use a Social Security number, driver's license number, State identification number, e-mail address or telephone number for any purpose other than for the purpose for which it was collected.

7. The Board shall identify all Users who may have access to Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses or telephone numbers in the course of performing their duties.

8. The number of Users who have access to information or documents that contain Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses or telephone numbers shall be limited to those who actually need such access as part of their duties.

9. All Users having access to Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses or telephone numbers in the course of performing their duties shall be trained to protect the confidentiality of information and to understand the requirements of the law.

10. Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses or telephone numbers of individuals shall not be disclosed or made accessible to the general public or to anyone other than to the Board's officers, employees, temporary employees, interns, vendors, consultants, or contractors having been given authorized access to such data or information unless required pursuant to court order, warrant or subpoena.

11. Notwithstanding the prohibitions set forth above, Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses and telephone numbers may be disclosed to another governmental entity or its agents, employees, or contractors if disclosure is necessary in order for the entity to perform its duties and responsibilities and if the governmental entity and its agents, employees, and contractors maintain the confidential and exempt status of such data.

12. Documents or data containing Social Security numbers, driver's license numbers, State identification card numbers, e-mail addresses or telephone numbers shall be disposed of only in accordance with procedures approved by the Local Records Commission.

VII. Human Resources Security

A. Prior to Employment. All employees, consultants, and contractors and other persons designated by the Board who use the Board's information technology as part of their job function are required to sign the Board's Confidentiality and Acceptable Use Agreement.

B. During Employment

1. Information Security Awareness, Education, and Training. Security awareness begins during the hiring process and it is the responsibility of the User to remain aware of current security policies. Users should read the security reminders that are periodically distributed.

2. Disciplinary Process. Any violation of this Policy, or any part or provision hereof, may result in disciplinary action, including termination and/or civil action and/or criminal prosecution.

C. Termination or Change of Employment

1. Return of Assets. When a User leaves the Board, all Information Assets remain the property of the Board. A User must not take away such information or take away a copy of such information when he or she leaves the Board without the prior express written permission of the Board.

2. Removal of Access Rights. Upon termination of an employee or vendor, the person who requested access to technology resources must request the termination of that access using the Board's access request procedure. In the event that the requestor is not available, the responsibility is placed upon the manager of the employee or vendor. The Board may automatically disable or delete accounts where termination is suspected even if formal notification was bypassed.

VIII. Communications and Operations Management

A. Protection Against Malicious Code

1. It is the Board's policy to conduct virus scanning of its technology resources to protect them from the threat of malicious code. The Board will intercept and/or quarantine any networking and computer resource that poses a virus threat to its information assets.

2. All servers and workstations (networked and standalone) must have the Board's approved antivirus protection software installed, properly configured, and functioning at all times. Additionally, systems that have not been issued by the Board but that use the Board's network must also be protected by antivirus software.

3. All incoming and outgoing e-mails must be scanned for viruses.

4. Users are responsible for ensuring that software, files, and data downloaded onto the Board's workstations are properly scanned for viruses.

5. Users must conduct virus scans on all external media received or used by the Board.

6. Users must ensure that all workstations (networked and standalone) have the most current antivirus signature files loaded.

B. Back-Up

1. The Board will perform regular backups of User files stored on the Board's file servers and storage media that are centrally managed by the Department of Electronic Voting Systems. This process will be coordinated in conjunction with the Board's User departments based on their individual business needs.

2. The Board will not back up multimedia files in formats including, but not limited to, .mp3, .m4a, .m4p, .avi and .mov, except as needed for Communications Department monitoring of news-media reports, web sites, television or radio interviews and for preparation of commercials, and except as needed by the Community Services Department for preparation and editing of videos for training programs.

C. Media Handling

1. Disposal of Media. Except as otherwise provided by law or court order, electronic information maintained in a department's office may be destroyed by department staff or the Department of

Electronic Voting Systems when the retention period expires, in compliance with the Board's implementation of the State of Illinois Local Records Act.

D. Monitoring

1. Monitoring System Use

a. Users should have no expectation of privacy in their use of Internet services provided by the Board. The Board reserves the right to monitor for unauthorized activity the information sent, received, processed or stored on Board-provided network and computer resources, without the consent of the creator(s) or recipient(s). This includes use of the Internet as well as the Board's e-mail and instant messaging systems.

b. All information technology administrators, technicians and any other employees who by the nature of their assignments have privileged access to networks or computer systems must obtain written approval from the Department of Electronic Voting Systems to monitor User activity.

2. Clock Synchronization. All server clocks must be synchronized in a manner approved by the Department of Electronic Voting Systems in order to provide for timely administration and accurate auditing of systems.

IX. Access Control

A. User Access Management

1. User Account Management

a. Access to Confidential and Internal data must be made using a formal Access Request Form.

b. User accounts that have not been used for 90 days may be disabled without warning. After 180 days of inactivity, these accounts may be deleted without warning.

c. Departments must use the access request process to notify the Department of Electronic Voting Systems of a change in employment status (such as when a User takes a leave of absence, transfers departments, or is terminated). The account of a User on a leave of absence can be retained, suspended, or deleted at the discretion of the User's department.

B. User Responsibilities

1. Password Use

a. All e-mail, network, and domain accounts must be password protected. All new accounts will be created with a temporary password. The temporary password must be changed upon first use.

b. Mobile devices must be password protected; this includes but is not limited to personal digital assistants (PDA), smart phones, laptops, handhelds (e.g. Blackberries) and off-site desktops.

c. Passwords used on the Board's systems and on non-Board systems that are authorized for use must have the following characteristics unless otherwise approved by the Department of Electronic Voting Systems:

i. Passwords must be a minimum of 8 characters in length;

ii. Passwords must contain both alphabetic and numeric characters;

iii. Passwords must not be the same as the username;

iv. Passwords must not contain proper names or words taken from the dictionary;

v. Passwords must be changed at minimum of 90 days; and,

vi. Passwords used for production systems must not be the same as those used for corresponding non-production systems such as the password used during training.

d. Passwords must not be disclosed to anyone. All passwords are to be treated as Confidential Information.

2. Screen Savers. Use of password-protected screen savers is recommended to prohibit unauthorized system access. Screen savers should initiate after 10 minutes of inactivity. Password-protected screen savers are required on workstations that access Confidential information such as electronic Protected Health Information. Password-protected screen savers are also required on workstations that access Internal information if the workstation is not in an area that has restricted access.

C. Mobile Computing and Remote Access

1. Laptops, off-site computers, and mobile media that contain Confidential information must be encrypted using an encryption technique approved by the Department of Electronic Voting Systems. Mobile media that contain Internal information must be protected using an encryption technique approved by the Department of Electronic Voting Systems, a strong logon password, or restricted physical access in order to protect the data. Examples of mobile media include flash drives, DVDs, CDs, and external hard drives.

2. Personal media devices (for example, MP3 players such as iPods) must not be used as peripheral devices on Board-issued workstations.

3. Remote access is provided by the Board as an information conduit to assist in the accomplishment of municipal duties and goals. Any other use is strictly prohibited. Requests for remote access must have a valid business reason and be approved by the Department of Electronic Voting Systems.

4. All remote access connections must be through a secure, centrally administered point of entry approved by the Board. Authorized remote access connections must be properly configured and secured according to Board-approved standards including the Board's password policy. All remote desktop protocol implementations must be authorized by the Department of Electronic Voting Systems. Remote access through unapproved entry points will be terminated when discovered.

5. Non-Board owned computer equipment used for remote access must be approved and must also comply with the Board's standards. The Board will not be responsible for maintenance, repair, upgrades or other support of non-Board owned computer equipment used to access the Board's network and computer resources through remote access services.

6. Users who utilize workstations that are shared with individuals who have not signed a Confidentiality Agreement with the Board must ensure that the Board's data is removed or deleted after each use.

X. Information Security Incident Management

A. Reporting Information Security Events and Weaknesses

1. Violations of the Board's Information Security and Identity Protection Policy or any or all parts or provisions of this Policy must be reported to Department Management or to the Department of Electronic Voting Systems.

2. Users must ensure that a representative of the Department of Electronic Voting Systems is notified immediately whenever a security incident occurs. Examples of security incidents include a virus outbreak, defacement of a website, interception of e-mail, blocking of firewall ports, and theft of physical files or documents.

3. All reports of alleged violations of this Policy, or any part or provision hereof, will be investigated by the appropriate authority. During the course of an investigation, access privileges may be suspended.

XI. Compliance

A. Compliance with Legal Requirements

1. Intellectual Property Rights

a. Intellectual Property that is created for the Board by its employees is property of the Board unless otherwise agreed upon by means of third party agreements or contracts.

b. No User may transmit to, or disseminate from, the Internet any material that is protected by copyright, patent, trademark, service mark, or trade secret, unless such disclosure is properly authorized and bears the appropriate notations.

2. Prevention of Misuse of Information Processing Facilities. Users are prohibited from using the Board's processing facilities – including data centers, network cabinets or closets, and other facilities housing the Board's technology equipment – in any way that violates this Policy, or any federal, state, or municipal law.

3. Compliance with Security Policies and Standards. All Users must read and sign the Board's Confidentiality and Acceptable Use Agreement prior to being authorized to access the Board's information technology and information assets.

Appendix A – Common Terms and Definitions

1. Computer Resources – All related peripherals, components, disk space, system memory and other items necessary to run computer systems.

2. Department Management – A supervisor, manager, director, or other employee of the Board designated by the Board or its Executive Director to be responsible for implementation of this Policy.

3. Electronic Mail (E-mail) – The transmission of messages through electronic means in a body or attachment using the Board's network or other information technology.

4. Information Assets – Information and data created, developed, processed, or stored by the Board that has value to the Board's business or operations.

5. Information Technology or Network and Computer Resources – Computer hardware and software, network hardware and software, e-mail, voice mail, video conferencing, facsimile transmission, telephone, remote access services, printers, copiers, and all other printed and electronic media.

6. Intranet – The suite of browser-based applications and HTML pages that are available for use only with access to the Board's internal network.

7. Internet – The worldwide 'network of networks' connected to each other using the IP protocol and other similar protocols. The Internet enables a variety of information management services, including, but not limited to, e-mail, instant messaging, file transfers, file uploads, file downloads, news, and other services.

8. Internet Services – Any service in which its primary means of communication is the Internet. For example, e-mail, web browsing and file transfers.

9. Mobile Computing Devices – Mobile devices and Mobile media. Mobile data processing devices are used as business productivity tools. Examples include: laptops, personal digital assistants (PDAs), smart phones, handhelds (e.g. Blackberries), and off-site desktops. Mobile media are devices typically used to transport data. Examples include: flash drives, DVDs, CDs, and external hard drives.

10. Network – The linking of multiple computers or computer systems over wired or wireless connections.

11. P2P – Peer-to-Peer network. A network where nodes simultaneously function as both "clients" and "servers" to other nodes on the network, P2P may be used for a variety of uses, but it is typically used to share files such as audio files. Examples of P2P networks includes Napster, KaZaA, and LimeWire. If a node is not properly configured, any file on the device may potentially be accessed by anyone on the network.

12. Protected Health Information – Individually identifiable health information about an individual that relates to the past, present, or future physical or mental health or condition, provision of health care, or payment for health care.

13. Remote Access Services – A service that enables off-site access to the Board information technology and assets. Examples include the Board's telephone exchanges, internal phone switches, wireless access points (WAP), and Virtual Private Network (VPN) connections. Remote access includes, but is not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

14. Security Incident – An event that has an adverse impact on the confidentiality, integrity, and availability of computer systems, computer networks, electronic information assets, or physical information assets.

15. User(s) – The Board's officers, employees, temporary employees, interns, vendors, consultants, contractors, and authorized agents who utilize the Board's information assets and technology.

16. World Wide Web (WWW) – Browser-based applications and HTML pages that are available for access and use across the Internet.