EXHIBIT 2

SCHEDULE OF PRICING

Audit Services Fee Proposal	
Description of Services	*Rate*
Budget Control	
Grant Funding – CARES ACT, CTCL	
Master Data Management	
Cost Allocations	
Policy & Procedures	
Vendor Billing	
Process Improvement	
Internal Control over Financial Reporting	
Other	

	Rate
Other	
Other	
Other	
Other	

APPENDIX 1 - 5

APPENDIX 1

Affidavit of Proposal Submission

The undersigned hereby acknowledges having received and reviewed the RFP and the general conditions, special conditions and specifications herein, and affirms that Proposer shall be bound by all of the terms and conditions contained in said documents, regardless of whether a complete set thereof is attached with this proposal, except only to the extent that Proposer has taken express written exception thereto in the sections of this specification designated for that purpose.

Further, the undersigned, being duly sworn, deposes and says on oath that no disclosures of ownership interest have been withheld and that the information provided herein to the best of its knowledge is current, the prices in the proposal have been arrived at independently without any collusion, consultation, communication or agreement, for the purpose of restricting competition as to any matter relating to such prices, with any other proposer or any competitor; and unless otherwise required by law, the prices which had been quoted in the proposal have not been knowingly disclosed by the Proposer prior to the opening, directly or indirectly, to any other proposer, to any other competitor, or to any Commissioner, officer, employee or agent of the Board.

Further, the undersigned states on oath that no attempt has been made or will be made by Proposer to induce any other person, partnership or corporation to submit or not to submit a proposal.

This proposal, together with all certifications and disclosures, is submitted this _____ day of _____, 20____.

FULL BUSINESS NAME OF PROPOSER: _____

BUSINESS ADDRESS: _____

_____ _____

SIGNATURE OF PROPOSER OR AUTHORIZED PERSON(S)* TITLE

• Note: If this proposal is submitted on behalf of a corporation, then this instrument must be signed by the President of the corporation or such other person authorized by the corporate by-laws or resolutions of the board of directors to bind the corporation (attach a certified copy of appropriate section of by-laws or resolution). This signed instrument must be attested to by the corporation's secretary.
• If this proposal is submitted on behalf of a partnership, all partners must sign this instrument, unless one partner has been authorized to sign for the partnership, in which case, evidence of such authority must be submitted.

Subscribed and sworn to before me by each of the foregoing individuals this _____ day of _____, 20____.

_____ {Seal}

Notary Public Signature

COMPLETE IF SUBMITTED AND SIGNED BY CORPORATION:

**ATTEST: _____

Corporate Secretary Signature

{Affix Corporate Seal}

The attached instrument was acknowledged before me on this _____ day of _____, 20____, by _____ as President (or other authorized officer) and by _____ as Secretary of _____ (Corporation Name)

_____ {Seal}

Notary Public Signature

APPENDIX 2

ECONOMIC DISCLOSURE STATEMENT AND AFFIDAVIT CHICAGO BOARD OF ELECTION COMMISSIONERS

SECTION I -- GENERAL INFORMATION

A. Legal name of Disclosing Party submitting this Statement. Include d/b/a/ if applicable:

_____

Check ONE of the following three boxes:

Indicate whether Disclosing Party submitting this Statement is:

1. [ ] the Applicant OR

2. [ ] a legal entity holding a direct or indirect interest in the Applicant. State the legal name of the Applicant in which Disclosing Party holds an interest OR

3. [ ] a specified legal entity with a right of control (see Section II.B.2.) State the legal name of the entity in which Disclosing Party holds a right of control.

B. Business address of Disclosing Party: _____

_____

C. Telephone: _____ Fax: _____ Email: _____

D. Name of contact person: _____

E. Federal Employer Identification No. (if you have one): _____

F. Brief description of contract, transaction or other undertaking (referred to below as the "Matter") to which this Statement pertains:

_____
_____
_____

SECTION II -- DISCLOSURE OF OWNERSHIP INTERESTS A. NATURE OF DISCLOSING PARTY

1. Indicate the nature of the Disclosing Party:

[ ] Person	[ ] Limited liability company*
[ ] Publicly registered business corporation	[ ] Limited liability partnership*
[ ] Privately held business corporation	[ ] Joint venture*
[ ] Sole proprietorship	[ ] Not-for-profit corporation

[ ] General partnership*	(Is the not-for-profit corporation also a 501(c) (3))?
[ ] Limited partnership*	[ ] Yes [ ] No
[ ] Trust	[ ] Other (please specify)
***** Note B.2. below	_____

2. For legal entities, the state (or foreign country) of incorporation or organization, if applicable: _____

3. For legal entities not organized in the State of Illinois: Has the organization registered to do business in the State of Illinois as a foreign entity?

[ ] Yes [ ] No [ ] N/A

B. IF THE DISCLOSING PARTY IS A LEGAL ENTITY:

1. List below the full names and titles of all executive officers and all directors of the entity. For not-for-profit corporations, also list below all members, if any, which are legal entities. If there are no such members, write "no members." For trusts, estates or other similar entities, list below the legal titleholder(s).

Name Title

_____

_____

_____

_____

2. If you checked “General partnership,” “Limited partnership,” “Limited liability company,” “Limited liability partnership” or “Joint venture” in response to Item A.1. above (Nature of Disclosing Party), list below the name and title of each general partner, managing member, manager or any other person or entity that controls the day-to-day management of the Disclosing Party. NOTE: Each legal entity listed below must submit a Statement on its own behalf.

Name Title

_____

_____

_____

3. Please provide the following information concerning each person or entity having a direct or indirect beneficial interest (including ownership) in excess of 7.5% of the Disclosing Party. Examples of such an interest include shares in a corporation, partnership interest in a partnership or joint venture, interest of a member or manager in a limited liability company, or interest of a beneficiary of a trust, estate or other similar entity. If none, state "None."

Name Business Address Percentage Interest in the Disclosing Party

_____

_____

_____

_____

SECTION III -- BUSINESS RELATIONSHIPS WITH BOARD OFFICIALS

Has the Disclosing Party had a "business relationship" with any Board official in the 12 months before the date this Statement is signed? "Business relationship" shall refer to any contractual or other private business dealing between the Disclosing Party and a Board official, or his or her spouse or domestic partner, or of any entity in which a Board official or his or her spouse or domestic partner has a financial interest, which entitles the Board official to compensation or payment in the amount of $250.00 or more in a calendar year. "Board official" means any Commissioner of the Board of Election Commissioners for the City of Chicago, the Board's Executive Director or the Board's Procurement Officer.

[ ] Yes [ ] No

If yes, please identify below the name(s) of such official(s) and describe such relationship(s):

_____

_____

_____

_____

SECTION IV -- DISCLOSURE OF SUBCONTRACTORS AND OTHER RETAINED PARTIES

The Disclosing Party must disclose the name and business address of each subcontractor, attorney, lobbyist, accountant, consultant and any other person or entity whom the Disclosing Party has retained or expects to retain in connection with the Matter, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Disclosing Party is not required to disclose employees who are paid solely through the Disclosing Party's regular payroll.

"Lobbyist" means any person or entity who undertakes to influence any legislative or administrative action on behalf of any person or entity other than: (1) a not-for-profit entity, on an unpaid basis, or (2) himself. "Lobbyist" also means any person or entity any part of whose duties as an employee of another includes undertaking to influence any legislative or administrative action.

If the Disclosing Party is uncertain whether a disclosure is required under this Section, the Disclosing Party must either ask the Board of Election Commissioners whether disclosure is required or make the disclosure.

Name Business Address Relationship to Disclosing Party Fees (indicate whether (subcontractor, attorney (indicate retained or anticipated lobbyist, etc.) estimated, whether paid or to be retained)

_____

_____

_____

_____

(Add sheets if necessary)

[ ] Check here if the Disclosing party has not retained, nor expects to retain, any such persons or entities.

SECTION V – CERTIFICATIONS

A. CERTIFICATIONS

The Disclosing Party certifies that:

1. The Disclosing Party and, if the Disclosing Party is a legal entity, all of those persons or entities identified in Section II.B. of this Statement:

(a) are not presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from any transactions by any federal, state or local unit of government;

(b) have not, within a five-year period preceding the date of this Statement, been convicted of a criminal offense, adjudged guilty, or had a civil judgment rendered against them in connection with: obtaining, attempting to obtain, or performing a public (federal, state or local) transaction or contract under a public transaction; a violation of federal or state antitrust statutes; fraud; embezzlement; theft; forgery; bribery; falsification or destruction of records; making false statements; or receiving stolen property;

(c) are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state or local) with commission of any of the offenses enumerated in clause A.1.(b) of this Section V;

(d) have not, within a five-year period preceding the date of this Statement, had one or more public transactions (federal, state or local) terminated for cause or default; and

(e) have not, within a five-year period preceding the date of this Statement, been convicted, adjudged guilty, or found liable in a civil proceeding, or in any criminal or civil action, including actions concerning environmental violations, instituted by the State of Illinois or by the federal government, any state, or any other unit of local government.

2. The certifications in subparts 2, 3 and 4 concern:

- the Disclosing Party;
- any "Applicable Party" (meaning any party participating in the performance of the Matter, including but not limited to any persons or legal entities disclosed under Section IV, "Disclosure of Subcontractors and Other Retained Parties");

- any "Affiliated Entity" or “Affiliate” (meaning a person or entity that, directly or indirectly: controls the Disclosing Party, is controlled by the Disclosing Party, or is, with the Disclosing Party, under common control of another person or entity. Indicia of control include, without limitation: interlocking management or ownership; identity of interests among family members, shared facilities and equipment; common use of employees; or organization of a business entity following the ineligibility of a business entity to do business with federal or state or local government, including the Board, using substantially the same management, ownership, or principals as the ineligible entity); with respect to Applicable Parties, the term Affiliated Entity or Affiliate means a person or entity that directly or indirectly controls the Applicable Party, is controlled by it, or, with the Applicable Party, is under common control of another person or entity;
- any responsible official of the Disclosing Party, any Applicable Party or any Affiliated Entity, Affiliate or any other official, agent or employee of the Disclosing Party, any Applicable Party or any Affiliated Entity or Affiliate, acting pursuant to the direction or authorization of a responsible official of the Disclosing Party, any Applicable Party or any Affiliated Entity or Affiliate (collectively "Agents").

Neither the Disclosing Party, nor any Applicable Party, nor any Affiliated Entity or Affiliate of either the Disclosing Party or any Applicable Party nor any Agents have, during the five years before the date this Statement is signed, or, with respect to an Applicable Party, an Affiliated Entity, or an Affiliated Entity of an Applicable Party during the five years before the date of such Applicable Party's or Affiliated Entity's contract or engagement in connection with the Matter:

(a) bribed or attempted to bribe, or been convicted or adjudged guilty of bribery or attempting to bribe, a public officer or employee of the Board, the City of Chicago, the County of Cook, the State of Illinois, or any agency of the federal government or of any state or local government in the United States of America, in that officer's or employee's official capacity;

(b) agreed or colluded with other bidders or prospective bidders, or been a party to any such agreement, or been convicted or adjudged guilty of agreement or collusion among bidders or prospective bidders, in restraint of freedom of competition by agreement to bid a fixed price or otherwise; or

(c) made an admission of such conduct described in (a) or (b) above that is a matter of record, but have not been prosecuted for such conduct.

3. Neither the Disclosing Party, Affiliated Entity or Applicable Party, or any of their employees, officials, agents or partners, is barred from contracting with any unit of state or local government as a result of engaging in or being convicted of (1) bid-rigging in violation of 720 ILCS 5/33E-3; (2) bid-rotating in violation of 720 ILCS 5/33E-4; or (3) any similar offense of any state or of the United States of America that contains the same elements as the offense of bid-rigging or bid-rotating.

4. Neither the Disclosing Party nor any Affiliated Entity is listed on any of the following lists maintained by the Office of Foreign Assets Control of the U.S. Department of the Treasury or the Bureau of Industry and Security of the U.S. Department of Commerce or their successors: the Specially Designated Nationals List, the Denied Persons List, the Unverified List, the Entity List and the Debarred List.

5. If the Disclosing Party is unable to certify to any of the above statements in this Section, the Disclosing Party must explain below:

_____

_____

_____

_____

If the letters "NA," the word "None," or no response appears on the lines above, it will be conclusively presumed that the Disclosing Party certified to the above statements.

SECTION VII -- ACKNOWLEDGMENTS, CONTRACT INCORPORATION, COMPLIANCE, PENALTIES, DISCLOSURE

The Disclosing Party understands and agrees that:

A. By completing and filing this Statement, the Disclosing Party acknowledges and agrees, on behalf of itself and the persons or entities named in this Statement that the Board may investigate the creditworthiness of some or all of the persons or entities named in this Statement.

B. The certifications, disclosures, and acknowledgments contained in this Statement will become part of any contract or other agreement between the Applicant and the Board in connection with the Matter, whether procurement, Board assistance, or other Board action, and are material inducements to the Board's execution of any contract or taking other action with respect to the Matter. The Disclosing Party understands that it must comply with all statutes, ordinances, and regulations on which this Statement is based.

C. If the Board determines that any information provided in this Statement is false, incomplete or inaccurate, any contract or other agreement in connection with which it is submitted may be rescinded or be void or voidable, and the Board may pursue any remedies under the contract or agreement (if not rescinded, void or voidable), at law, or in equity, including terminating the Disclosing Party's participation in the Matter and/or declining to allow the Disclosing Party to participate in other transactions with the Board.

D. It is the Board's policy to make this document available to the public upon request. Some or all of the information provided on this Statement and any attachments to this Statement may be made available to the public in response to a Freedom of Information Act request, or otherwise. By completing and signing this Statement, the Disclosing Party waives and releases any possible rights or claims which it may have against the Board in connection with the public release of information contained in this Statement and also authorizes the Board to verify the accuracy of any information submitted in this Statement.

E. The information provided in this Statement must be kept current. In the event of changes, the Disclosing Party must supplement this Statement up to the time the Board takes action on the Matter. If the Matter is a contract, the Disclosing Party must update this Statement as the contract requires.

The Disclosing Party represents and warrants that:

F. The Disclosing Party has not withheld or reserved any disclosures as to economic interests in the Disclosing Party.

G. The Disclosing Party is not delinquent in the payment of any tax administered by the Illinois Department of Revenue, nor are the Disclosing Party or its affiliates delinquent in paying any fine, fee, tax or other charge owed to the State of Illinois, the County of Cook of the City of Chicago. This includes, but is not limited to, all water charges, sewer charges, license fees, parking tickets, property taxes or sales taxes.

CERTIFICATION

Under penalty of perjury, the person signing below: (1) warrants that he/she is authorized to execute this Statement on behalf of the Disclosing Party, and (2) warrants that all certifications and statements contained in this Statement are true, accurate and complete as of the date furnished to the Board.

Date: _____

_____
(Print or type name of Disclosing Party)

By: _____
(Sign here)

_____
(Print or type name of person signing)

_____
(Print or type title of person signing)

Signed and sworn to before me on (date) _____, by _____, at

_____ City, County and State

_____
Notary Public Signature

Seal Commission expires:

APPENDIX 3

BOARD OF ELECTION COMMISSIONERS 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 Protection 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 ("HIPAA"), 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, and 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. 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.

c. 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.

d. 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.

e. 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.

f. Internal information such as email 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.

g. 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.

h. 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.

i. 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 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 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 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 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 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 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 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 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 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 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 a-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 a dictionary;

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

vi. Passwords used for production systems must not be the same as those used for corresponding nonproduction system 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 email, 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.

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, email, 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 include Napster, KaZaA, and LimeWire, if a node is not property 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.

ADOPTED: JULY 29, 2008

BOARD OF ELECTION COMMISSIONERS
CITY OF CHICAGO

Confidentiality and Acceptable Use Agreement

PURPOSE

Information security, confidentiality, and copyright protection are matters of concern for Board of Election Commissioners for the City of Chicago (the "Board"), employees of the Board and for all other persons who have access to Board computer files, information and records, whether they are employees, vendors, consultants, or others. The Board maintains information in the form of computerized files. The Board also utilizes computer software and methodologies created internally and by third parties that may be protected by intellectual property, patent, copyright and trade secret laws. As such, the Board is contractually obligated to prevent any and all unauthorized disclosure or use of these information assets.

RECIPIENT'S OBLIGATIONS

A position of trust has been conferred upon every authorized person who, as part of their job function, comes in contact with confidential information to keep this information secure and private. Board employees, contractors and others who gain access to confidential information in the possession of or under the control of the Board are obligated to recognize and adhere to these responsibilities while on or off the job. Therefore, an employee of the Board or a person authorized to access Board data files and information agrees:

- To follow the Board's privacy and security policies, standards, and guidelines including the Information Security and Identity Protection Policy;
- If a Board employee, to use only a Board authorized e-mail address and server when communicating with others via-email concerning matters of Board business- use of personal or private e-mail addresses to communicate regarding Board business is prohibited;
- Not to expose voters' or employees' confidential information (such as social security numbers, driver's license numbers, State identification card numbers, telephone numbers or other sensitive information) as mandated by Illinois Personal Information Protection Act;
- Not to expose health information (such as an individual's diagnosis or treatment) as protected by HIPAA privacy and security rules;
- Not to engage in or permit unauthorized use of any information in files or programs maintained by the Board;
- Not to seek to benefit personally or permit others to benefit personally through the release of confidential information which has come to him/her by virtue of their job function or assignment;
- Not to copy, alter, modify, disassemble, reverse engineer or decompile any intellectual property. 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

- Not to exhibit or divulge the contents of any Board record to any person except in the conduct of his/her work assignment or in accordance with the policies of the Board;

- Not to disclose the specifics of non-public Board related business to unauthorized personnel;

- Not to remove or cause to be removed copies of any official record or report from any file from the office where it is kept except in the performance of his/her duties;

- Not to use or request others to use the Board's information technology for personal reasons beyond limited personal use as described in the Information Security and Identity Protection Policy;

- Not to conduct Board business on devices that allow P2P communication (such as music file sharing) without explicit approval from the Board;

- To password protect mobile devices issued by the Board or those authorized to connect to the Board's information technology resources. Examples include but are not limited to: personal digital assistants (PDA), smart phones, laptops, handhelds (e.g. Blackberries) and offsite desktops;

- Not to aid, abet, or act in conspiracy with another to violate any part of this
- Confidentiality and Acceptable Use Agreement or of the Information Security and Identity Protection Policy;

- To report any violation of this Confidentiality and Acceptable Use Agreement or of the
- Information Security and Identity Protection Policy by anyone to his/her supervisor immediately.

I have read, understand, and agree to follow the Board's Confidentiality and Acceptable Use Agreement and Information Security and Identity Protection Policy regarding my responsibilities to the security and privacy of the Board's information and technology assets.

I understand that any violation of this Agreement, or of the Information Security and Identity Protection Policy may result in disciplinary action, including termination and/or civil action and/or criminal prosecution.

_____ _____

Employee/Recipient Signature Date

_____

Employee/Recipient Name (Printed)

_____

Company Name (Printed)
if not a Board employee

APPENDIX 4:

Insurance Certificate of Coverage

Named Insured:_____

Address _____ RFP: Audit Services

(Number and Street)

_____

(City) (State) (ZIP)

Description of Operation/Location	

The insurance policies and endorsements indicated below have been issued to the designated named insured with the policy limits as set forth herein covering the operation described within the contract involving the named insured and the Board or Elections Commissioners. The Certificate issuer agrees that in the event of cancellation, non-renewal or material change involving the indicated policies, the issuer will provide at least sixty (60) days prior written notice of such change to the Board of Elections Commissioners at the address shown on this Certificate. This certificate is issued to the Board of Elections Commissioners in consideration of the contract entered into with the named insured, and it is mutually understood that the Board of Elections Commissioners relies on this certificate as a basis for continuing such agreement with the named insured:

Type of Insurance	Insurer Name	Policy Number	Expiration Date	Limits of Liability All Limits in Thousands
General Liability [ ] Claims made [ ] Occurrence [ ] Premise-Operations [ ] Explosion/Collapse Underground [ ] Products/Completed-Operations [ ] Blanket Contractual [ ] Broad Form Property Damage [ ] Independent Contractors [ ] Personal Injury [ ] Pollution				CSL Per Occurrence $ _____ General Aggregate $ _____ Products/Completed Operations Aggregate $ _____
Automobile Liability				CSL Per Occurrence $ _____
[ ] Excess Liability [ ] Umbrella Liability				Each Occurrence $ _____
Worker=s Compensation and Employer=s Liability				Statutory/Illinois Employers Liability $ _____
Builders Risk/Course of Construction				Amount of Contract
Professional Liability				$ _____
Owner Contractors Protective				$ _____
Other				$ _____

a) Each Insurance policy required by this agreement, excepting policies for worker's compensation and professional liability, will read: The Board of Elections Commissioners is an additional insured as respects operations and activities of, or on behalf of the named insured, performed under contract with or permit from the City of Chicago.

b) The General, Automobile and Excess/Umbrella Liability Policies described provide for severability of Interest (cross liability) applicable to the named insured and the Board of Elections Commissioners.

c) Workers Compensation and Property Insurers shall waive all rights of subrogation against the Board of Elections Commissioners.

d) The receipt of this certificate by the Board of Elections Commissioners does not constitute agreement by the Board of Elections Commissioners that the insurance requirements in the contract have been fully met, or that the insurance policies indicated by this certificate are in compliance with all contract requirements.

Name and Address of Certificate Holder and Recipient of Notice
Certificate Holder/Additional Insured
Board of Elections Commissioners, City of Chicago
Procurement Department
69 West Washington, #800
Chicago, IL 60602

Signature of Authorized Rep. _____
Agency/Company: _____
Address _____
Telephone _____