TORONTO

THIS AGREEMENT made in quadruplicate as of this 31st Day of March, 2014
BETWEEN

CITY OF TORONTO
(hereinafter called the "City")

OF THE FIRST PART

- and -

SCYTL CANADA INC.
(hereinafter called the "Vendor" or "Scytl")

OF THE SECOND PART

WITNESSES THAT:

WHEREAS the City issued Request for Proposals No. 3405-13-3197, dated November 4, 2013 together with:

1) Addendum 1, dated November 7, 2013;
2) Addendum 2, dated November 13, 2013;
3) Addendum 3, dated November 22, 2013;
4) Addendum 4, dated November 25, 2013;
5) Addendum 5, dated November 26,2013; and
6) Addendum 6, dated November 27, 2013

for the development, supply, implementation, training, support and maintenance of an Internet Voting Solution for Persons with Disabilities for the 2014 regular Municipal Election for the City Clerk's Division of the City of Toronto;

WHEREAS in response to the said Request for Proposals, Vendor submitted a Proposal dated December 2, 2013;

WHEREAS the City Council at its meeting on February 19 and 20, 2014 selected the Vendor as the Preferred Proponent following a competitive evaluation process; and

WHEREAS this Agreement for the provision of the Service by Vendor, pursuant to the Request for Proposal has been entered into in accordance with the City Council Award CC48.4 adopted on February 19 and 20, 2014.

NOW THEREFORE IN CONSIDERATION OF the mutual covenants and other terms and conditions of this Agreement and the sum of One Dollar ($1.00) of lawful money of Canada now paid by each of the Parties hereto to the other (the receipt and sufficiency whereof is hereby acknowledged), the Parties hereby covenant, promise and agree each with the other as hereinafter set forth.

1.0 INTERPRETATION

1.1 References to Labeled Provisions

Each reference in this Agreement to a numbered or lettered “section”, ”subsection“, “paragraph, “subparagraph”, “clause” or “sub-clause” shall, unless otherwise expressly indicated, be taken as a reference to the correspondingly labelled provision of this Agreement.

1.2 Definitions

Throughout this Agreement, unless inconsistent with the subject matter or context:

“**Acceptance**” means (i) in the case of any Deliverable that is to be subject to an Acceptance Test hereunder, the completion of such Acceptance Test to the reasonable satisfaction of the City in accordance with this Agreement; and (ii) in the case of any other Deliverable to be provided by Vendor to the City hereunder, the determination that any such Deliverable has been provided to the City in a form which appears to meet all requirements set out in the Agreement unless immaterial or inconsequential;

“**Accepted**” means, with respect to a Deliverable, the City has provided Notice of Acceptance to Vendor;

“**Affiliate**” means a party that partially (at least 50%) or fully controls, is partially or fully controlled by, or is under partial (at least 50%) or full common control with, another party;

“**Agreement**” means this Agreement entered into between the City and the Vendor setting out the respective undertakings by the City and Vendor to perform their respective duties, responsibilities and obligations as prescribed in this Agreement and includes the RFP, and all Addenda, appendices, schedules, drawings, the Proposal and such other documents as may be listed in the Agreement and any change orders and other amendments to the Agreement and the Proposal. It is used interchangeably with “Contract” and "Agreement";

"**Approval Process"** means the acceptance process of all Deliverables, as agreed upon between the Vendor and the City, during Phase 1 – Project Initiation of the IVS Project.

"**Business Day**" means any working day, Monday to Friday inclusive, excluding statutory and other holidays, namely: New Year's Day; Family Day; Good Friday; Easter Monday; Memorial Day; Independence Day, Victoria Day; Canada Day; Civic Holiday; Labour Day; Thanksgiving Day; Remembrance Day; Christmas Day; Boxing Day and any other day which the City has elected to be closed for business. Also see Business Hours defined below;

"**Business Hours**" or **"Normal Business Hours"** means 8:30 AM to 5:00 PM EST of any Business Day (local time in the City of Toronto, Ontario);

"**Change Order**" has the meaning set out in subsection 10.1(1) of this Agreement;

"**Change Order Response**" has the meaning set out in subsection 10.1(1) of this Agreement;

"**Change Order Request**" has the meaning set out in subsection 10.1(1) of this Agreement;

"**Change**" means a change to the Services or Goods to be provided by Vendor pursuant to any SOW or a change to the tasks to be performed or materials to be provided by the City pursuant to any SOW;

"**City**" means the City of Toronto;

"**City Content**" means Content provided by the City;

"**City Data**" means proprietary or personal data (including Personal Information) regarding the City or any of its users under this Agreement. For clarification, City Data is considered Confidential Information;

"**Confidential Information**" means any and all information and materials disclosed by either Party, which:

(1) are designated in writing, as confidential at the time of disclosure;

(2) if disclosed orally or visually, are designated (in the same manner) as confidential at the time of disclosure;

(3) the City is obliged not to or has the discretion not to disclose pursuant to law or statute such as the *Municipal Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act*, or any other municipal, provincial and federal legislation;

(4) the City is required to keep confidential, including any information of third parties, such as but not limited to any suppliers of any products or services provided to the City;

(5) relate to Intellectual Property rights including copyright, trade secrets, processes, formulae, techniques, plans and designs, computer programs, computer codes whether source code or object code, and all related documentation and financial information related hereto which is proprietary to or in the possession of a Party to this Agreement, and that the other Party to this Agreement may have access to for purposes of this Agreement;

(6) comprise the databases of the City or the procedures and operational protocols and information relating to the operations of the City and that Vendor may have access to for purposes of this Agreement;

(7) include all data, formulae, preliminary findings, and other material developed in the performance of the Services;

(8) is Personal Information; or

(9) a reasonable person, having regard to the circumstances, would regard as confidential;

(10) whether recorded or not, however fixed, stored, expressed or embodied.

“Configuration” means a set of tasks required in order to activate functionality without any Customization. Support for Configuration shall be included in the Vendor’s standard support and maintenance service;

“**Content**” means each and all of the following: course, learning object, certification, quiz, test, material, instructor-led session, or document;

“**Contract**” means Agreement (as defined above);

“**Council**” means the City Council for the City;

“Customization” means any required software change(s) that the Vendor must make that results in a modification or creation of any proposed application source code in order to meet the City’s Functional Requirements;

“**Deliverables**” means the Project deliverables to be provided by Vendor to the City pursuant to this Agreement, including the deliverables described in Section 5 of SCHEDULE “A”;

"Demonstration Environment" means website as well as a functional IVR phone number that demonstrates the full functionality and accessibility of the final production environment for the internet and telephone voting service of the IVS;

“**Dispute**” means any dispute or controversy between the City and Vendor arising out of or relating to the Agreement;

"**Documentation**" means any communicable material provided by Vendor to City that is used to describe, explain or instruct regarding attributes of an object, system or procedure, such as its parts, assembly, installation, maintenance and use;

"**Fee(s)**" and "**Fixed Fee**" has the meaning set out in Section 13.0 of the Agreement;

"**Final Acceptance**" means Acceptance of the Services as a whole;

"**Final Notice of Acceptance**" "Notice of Final Acceptance" means a final written notification by the City to Vendor confirming that the City has accepted the completeness and adequacy of all Deliverables specified in such notice by the City;

"Functional Requirements" means the requirements set out in Appendix F.2 of the RFP, SCHEDULES "H" and "I" of this Agreement, and any additional proposed functional requirements in the Proponent's Proposal if accepted by the City;

"**Implementation**" means the configuration, training, testing, and transfer of City Data related to the Solution;

"**Initial Term**" is the initial term of the Agreement, as set forth in the initial Order;
"**IT**" means information technology in general;

"**I&T**" means the City's Information & Technology Division and any successor to that division;

"**Intellectual Property Rights**" means all the intellectual property, industrial and other proprietary rights, protected or protectable, under the laws of Canada, any foreign country, or any political subdivision thereof, including, without limitation, (i) all trade names, trade dress, trademarks, service marks, logos, brand names and other identifiers; (ii) copyrights, moral rights (including rights of attribution and rights of integrity); (iii) all trade secrets, inventions, discoveries, devices, processes, designs, techniques, ideas, know-how and other confidential or proprietary information, whether or not reduced to practice; (iv) all domestic and foreign patents and the registrations, applications, renewals, extensions and continuations (in whole or in part) thereof; and (v) all goodwill associated therewith and all rights and causes of action for infringement, misappropriation, misuse, dilution or unfair trade practices associated with (i) through (iv) above;

"**Interactive Voice Response**" or "**IVR**" means the type of system used in which a voter casts a ballot using a number pad on a touch-tone or mobile telephone, following automated instructions or prompts to move through the voting process.

"Knowledge Transfer" means the process by which the Vendor provides training, in accordance with the Agreement and the applicable Statement of Work, with respect to the Services that augments the knowledge and experience of the City Personnel and user groups, including access to reports, information sessions and meetings and

includes a thorough, hands on review of the methodologies and tools employed by the Vendor with the appropriate City Personnel for the purpose of City Personnel acquiring the skills to manage the ongoing day to day operations, improvements and future implementations;

"**MEA**" means the *Municipal Elections Act, R.S.O. 1996, c. 32*, as amended.

"**MFIPPA**" means the Ontario *Municipal Freedom of Information and Protection of Privacy Act;*

"Non-Functional Requirements" means the requirements set out in Appendix F.2 of this RFP and any additional proposed Non-Functional Requirements in the Proponent's Proposal if accepted by the City;

"**Notice of Acceptance**" means a written notification by the City to Vendor confirming that the City has accepted the completeness and adequacy of the Deliverable(s) specified in such notice by the City;

"Out-of-the-Box" means features that are available as part of the Solution immediately on installation and require no Configuration or Customization;

"**Party**" means either the City or Vendor and "Parties" means both of them;

"**Personal Information**" means any personal information which is required to be protected pursuant to MFIPPA, PHIPA, PIPEDA or any other laws or regulations pertaining to the protection of personal information. For clarification, Personal Information is a subset of Confidential Information;

"**Personnel**" with respect to either Party, means the Party's employees, contract personnel, representatives, invitees, members, volunteers, officials and agents. In the case of Vendor, it includes its directors, partners, subcontractors, sub-consultants and third party service providers and in the case of the City, it includes its Members of Council, the Mayor and officers;

"**PIPEDA**" means the *Personal Information Protection and Electronic Documents Act*, and the regulations there under, as amended from time to time. (For greater clarity, PIPEDA is federal privacy legislation initially passed in 2004 that protects personal information in the hands of certain private sector organizations and provides guidelines for the collection, use and disclosure of that information in the course of commercial activity);

"**PHIPA**" means the *Personal Health Information Protection Act, 2004*; provincial (Ontario) legislation that governs the collection, use and disclosure of personal health information within the health care system;

"**Proceedings**" means any action, claim, demand, lawsuit, or other proceeding;

“Products” means any and all Scytl Canada Content, Services, work product resulting from Services, Documentation and Solution, excluding the Documentation as provided for in section 12.0 of this Agreement;

“Production Environment” means the set of processes, software and physical infrastructure required to operate the Solution on an ongoing basis;

“**Project**” means a work assignment described in a SOW attached to this Agreement as a Schedule;

“**Project Manager**” means main contact person at the City or Vendor, as applicable, for all matters relating to the project. Manager of a team of City staff or Vendor Personnel assigned to the Project;

“**Project Plan**” means, with respect to any Project, a detailed plan approved by the City as a Deliverable setting out the dates by which various activities related to the Project are required to be completed;

"**Project Working Group**" has the meaning set out in Section 3.0 of the SOW.

“**Proposal**” means the Proposal dated December 2, 2014 submitted by Vendor.

“Public Engagement Service” means a demonstration website and functional IVR phone number that is substantially in the same form as the demonstration provided in the original RFP . The Service is to include both Internet and Telephone Voting Services.. The City will use the Public Engagement Service for communication, education and outreach purposes;

“Requirements” means the Requirements requirements set out in Appendices F.1 and F.2 of the RFP No. 3405-13-3197 and any additional proposed Requirements in the Proponent’s Proposal if accepted by the City and set out in SCHEDULES "H" and "I".

“**Request for Proposals**” or “**RFP**” means the Request for Proposals No. 3405-13-3197 in its entirety, inclusive of all appendices, bulletins, or addenda issued by the City which is incorporated by reference and form part of the Agreement;

“**Services**” means any service required to be provided by Vendor to the City, as set out in this Agreement and in any SOW including, but not limited to: (i) hosting of the Solution; (ii) hosting, delivery, and/or distribution of Content; (iii) provision of customer and/or technical support for the Solution; (iv) Implementation; (v) development of Solution functionality specially requested by the City; and/or (vi) any consulting service;

“Solution” means any and all of Scytl Canada’s proprietary web-based applications, including, without limitation, all updates, revisions, bug-fixes, upgrades, and enhancements thereto, as well as applications that have been modified in any way by Scytl Canada at the request of the City in connection with an Internet and Telephone

Voting System including any Deliverables and Services meeting the City's Functional, Technical and Non-Functional Requirements, as set out in this Agreement;

"Staging Environment" means an environment that mirrors the functionality of the Production Environment, on all the same hardware (including high availability systems) in order to demonstrate all live features (including disaster recovery, encryption mechanisms, ability to handle anticipated voter/data volume, fail-over and intrusion detection) before deployment to the Production Environment;

"**Statement of Work**" or "**SOW**" means any Schedule to this Agreement made between the City and Vendor, as amended from time to time, describing the specific items of goods and Services to be provided to the City by the Vendor in accordance with the terms and conditions of this Agreement. "Statement of Work" or "SOW" also includes any other documents that are expressly referenced in and form part of such SOW;

"Technical Requirements" means the Technical Requirements requirements set out in SCHEDULE "H" and "I" of this Agreement and any additional proposed Technical Requirements in the Proponent's Proposal if accepted by the City.

"**Term**" means the Initial Term plus all Renewal Terms;

"User Acceptance Testing" or "UAT" has the meaning set out in Phase 4 – Internet Voting Service Configuration, Implementation and User Acceptance Test and SCHEDULE "F"

"Vendor" means the successful Proponent with whom the City enters into an Agreement, including any sub-contractors or third-party service providers engaged by the successful Proponent;

"Voter-Facing Components" means the components of the Internet Voting Service that a voter could potentially use either via telephone, internet or postal mail.

1.3 Headings

Headings in this Agreement appear for convenience of reference only and shall not affect its construction or interpretation.

1.4 Number, Gender, Person

Unless inconsistent with the subject matter or context, in this Agreement:

(1) words importing gender shall include the masculine, feminine, and neuter genders;

(2) words importing the singular shall include the plural and vice versa; and

(3) words importing persons shall include individuals, consortia, partnerships, associations, trusts, municipal corporations, government agencies, unincorporated organizations and corporations and vice versa.

1.5 Grammatical Variations

Grammatical variations of any expressions defined in this Agreement shall have similar meanings to such defined expressions.

1.6 Legislative Reference

Any reference in this Agreement to all or any part of any statute, regulation, by-law or rule shall, unless otherwise stated, be a reference to that statute, regulation, by-law or rule or the relevant part thereof, as amended, replaced or re-enacted from time to time.

1.7 Order of Precedence

In the event of any conflict or inconsistency between the different parts of this Agreement which cannot be reasonably reconciled, the order of precedence shall be, in descending order of priority:

(1) This Agreement, exclusive of the Schedules;
(2) The Schedules to this Agreement;
(3) Any Exhibits, Appendices, Attachments, etc. to the Schedules:
(4) The RFP; and
(5) The Proposal.

2.0 THE SERVICES AND DELIVERABLES

2.1 Vendor shall perform the Services and provide the Deliverables in a careful, professional and workmanlike manner and in accordance with this Agreement.

3.0 TIMING

3.1 The Vendor shall carry out the Services and shall submit each Deliverable in accordance with the applicable Statement of Work.

3.2 In the event of a delay in or failure of performance under this Agreement by either party that is not mala fide, and arises by reason of force majeure, including without restriction an act of God, an act of any government or any governmental body, an act of war or terrorism, the elements, a strike, a lockout or a labour dispute, or any cause beyond the reasonable control of such party:

(1) Such party shall not thereby be in default; and

(2) Both parties shall use commercially reasonable efforts to mitigate the effect of such *force majeure*, but nothing in this clause shall require a party to settle a labour dispute in order to render performance.

4.0 VENDOR'S RESPONSIBILITIES

4.1 Personnel and Performance

(1) The Vendor must make available appropriately skilled workers, consultants or subcontractors, as appropriate, and must be able to provide the necessary materials, tools, machinery and supplies to carry out the Project.

(2) The Vendor shall be responsible for its own staff resources and for the staff resources of any subcontractors and third-party service providers.

(3) The Vendor will ensure that its personnel (including those of approved sub-contractors), when using any City buildings, premises, equipment, hardware or software shall comply with all security policies, regulations or directives relating to those buildings, premises, equipment, hardware or software.

(4) Personnel assigned by the Vendor to perform or produce the Services or any part of it, (including those of approved subcontractors) may, in the sole discretion of the City, be required to sign non-disclosure Agreement(s) satisfactory to the City before being permitted to perform such Services.

4.2 Sub-Contractors

(1) The Vendor shall be solely responsible for the payment of every sub-contractor employed, engaged, or retained by it for the purpose of assisting it in the performance of its obligations under the Agreement. The Vendor shall coordinate the services of its sub-contractors in a manner acceptable to the City, and ensure that they comply with all the relevant requirements of the Agreement.

(2) The Vendor shall be liable to the City for all costs or damages arising from acts, omissions, negligence or wilful misconduct of its sub-contractors.

5.0 CITY'S RESPONSIBILITIES

5.1 The City shall make available for use by the Vendor adequate workspace and office facilities;

5.2 The City shall, subject to section 15.0 (Confidential Information), make available all data, drawings, plans and any other materials in its possession that are relevant to the Services; at reasonable times, its Personnel for the purpose of any necessary consultation, including room and meeting booking support, required in the view of City Personnel, for the proper performance of the Services, but the City will not provide facilitation, scribing or documentation maintenance support.

5.3 The City shall assign and identify its own Project team members and roles, with suitable business and technical expertise to facilitate efficient progress of the Services;

5.4 Give due consideration to all plans, drawings, specifications, reports, proposals and other information provided by Scytl Canada and make its best efforts to arrive at any decisions which it is required to make in connection therewith so as not to delay the work of the Services.

6.0 INDEMNITY

6.1 The Vendor shall from time to time, and at all times hereafter, well and truly save, keep harmless and fully indemnify City of Toronto and any of its Members of Council, Mayor, officers, employees, agents, representatives, invitees, members, volunteers, successors and assigns from and against any and all manner of claims, demands, losses, costs, charges, actions and other proceedings whatsoever which may be brought against or made upon any of them and against any loss or damages suffered or incurred by the City arising from or relating to any physical injury, including death, or any loss of or damage to tangible property, caused by the Vendor, its employees, agents or subcontractors or any entity for whom it is in law responsible, or arising from or arising from or relating to any statutory obligations of the Vendor; and

6.2 The Vendor shall also fully defend, save harmless and indemnify the City from and The Vendor shall also fully defend, save harmless and indemnify the City from and against any loss or damages suffered or incurred by the City from or arising out of Vendor's performance or rendering of, or Vendor's failure to perform or render, or the failure to exercise reasonable care, skill or diligence in the performance or rendering of the Services save and except that to the extent that any liability arising pursuant to this section is not covered by proceeds of the insurance required to be maintained by the Vendor pursuant to Section 11 of this Agreement, the Vendor's liability to the City shall not exceed an amount equal to the total amount payable hereunder by the City to the Vendor and in no event shall the Vendor be liable to the City for any indirect or consequential damages. The limitation of liability in this section does not apply to the indemnities required by Sections 6.1, 7.0 and 8.2 of this Agreement or to a breach of any obligations of the Vendor relating to confidentiality as set out in Section 15.0.

6.3 The City will not provide any indemnity under any circumstances.

7.0 INTELLECTUAL PROPERTY INDEMNITY

7.1 The Vendor shall indemnify and save harmless the City of Toronto, its Mayor, Members of Council, officers, employees, and agents from and against any losses, liens, charges, claims, demands, suits, proceedings, recoveries and judgments (including legal fees and costs) (collectively, "Damages") arising from infringement, actual or alleged, by the Solution, its use or misuse, or by any of the deliverables developed or provided or supplied under or used in connection with the Services (including the provision of the Services themselves), of any Canadian, American or other copyright, moral right, trade-mark, patent, trade secret or other thing with respect to which a right in the nature of intellectual/industrial property exists. The foregoing provisions of this section shall not apply to the extent the Damages relate to or arise out of: (i) City Data; (ii) City Content; or (iii) unauthorized or negligent use and/or alteration of the Products by the City.

7.2 Indemnification Procedures: To obtain indemnification, the City shall: (i) give written notice of any claim as soon as is practicable to the Vendor; (ii) the Vendor shall assume sole control of the defense and settlement of such claim, provided that the Vendor may not, without the prior consent of the City (not to be unreasonably withheld), settle any claim unless it unconditionally releases the City of all liability; (iii) provide to the Vendor all available information and assistance; and (iv) not take any action that might compromise or settle such claim.

7.3 Infringement Cures. Should the Products or any part thereof become the subject of a claim for infringement of a third party Intellectual Property Right, then Scytl Canada shall, at its sole expense: (i) procure for the City the right to use and access the infringing or potentially infringing item(s) of the Solution free of any liability for infringement; or (ii) replace or modify the infringing or potentially infringing item(s) of the Solution with a non-infringing substitute otherwise materially complying with the functionality of the replaced system. If (i) and (ii) are not commercially reasonable, Scytl Canada may terminate the Agreement in which case the City shall receive a refund of all prepaid, unearned fees for Services paid to Scytl Canada.

8.0 THIRD PARTY SOFTWARE

8.1 Where the City is in possession of software containing or constituting confidential proprietary information belonging to third parties, the Vendor shall not, except in the usual incidental manner genuinely necessary for the intended use of such software on the equipment of the City:

(1) Analyze, copy, decompile, disassemble, translate, convert, reverse engineer or duplicate any physical embodiment or part thereof, or permit any person to do so; or

(2) Divulge to any unauthorized person the ideas, concepts or techniques, or make any other improper use, of such software.

8.2 The Vendor shall fully defend, save harmless and indemnify the City from and against any loss or damages suffered by the City as a result of any failure by the Vendor and/or its Personnel or any of them to comply with the provisions hereof.

8.3 Should the Vendor include third party confidential proprietary information within the Deliverables, the Vendor must secure the rights to use and repackage third party components and pass on those rights to the City without additional charges.

9.0 VENDOR'S REPRESENTATIONS, WARRANTIES AND COVENANTS

9.1 The Vendor represents, warrants and covenants to the City (and acknowledges that the City is relying thereon) that the Services to be supplied under this Agreement will be in substantially in accordance with the City's Functional, Non-Functional and Technical requirements (as set out in the RFP), and, if applicable, will function or otherwise perform in accordance with such RFP response.

9.2 The Vendor warrants, that to its knowledge, (i) no Councillor, official or employee of the City has any direct or indirect beneficial interest, whether financial or otherwise, in the Vendor or its subcontractors or suppliers or in their performance of the Services; and (ii) the Vendor is not engaged in any other projects nor is it providing services to any other client that would give rise to an actual or potential conflict of interest.

9.3 If an actual conflict of interest exists or arises pursuant to this section during the term of this Agreement, the City may, at its discretion, suspend any Services being performed until the matter is resolved. If the conflict of interest is incapable of remedy, the City may terminate this Agreement.

9.4 The Vendor acknowledges and agrees that it is responsible for becoming familiar with, and shall comply with, the City's Purchasing By-law (chapter 195 of the Municipal Code) and City policies respecting MFIPPA, Non-Discrimination, Canadian Content, Fair Wage, Labour Trades Contractual Obligations in the Construction Industry, Re-employment of Former Employees after Reorganizing, Environmentally Responsible Procurement Statement, Purchase of Products Manufactured in Factories Where Children Are Used As Slave Labour or Other Exploitative Circumstances Which Impedes Child Development, Conflict of Interest Policy, Inter-provincial Fairness Legislation, Occupational Health and

Safety Statutory Declarations, Former Metro Toronto or Area Municipality Senior Management Employees Working for Firms on City Contracts Policy, and other City Policies provided to Vendor via website or otherwise. These policies are available to the Vendor on the following website: http://toronto.ca/calldocuments/policy.htm#policy.

9.5 In compliance with the City's policy on Re-Employment of Former Employees after Reorganizing, the Vendor shall not in providing the Services make use of the services of any former City employee who received from the City a separation package, within two (2) years of such employee's termination of employment with the City.

9.6 The Vendor acknowledges that there are no actions, claims, suits or proceedings pending or to its knowledge threatened against or adversely affecting it or any of its subcontractors in any court or before or by any federal, provincial, municipal or other government department, commission, board, bureau or agency, Canadian or Foreign, that might affect the Vendor's or its proposed subcontractor's financial condition or ability to perform and meet any and all duties, liabilities and obligations as may be required under this Agreement.

9.7 TO THE EXTENT PERMITTED BY APPLICABLE LAW, SCYTL CANADA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT (EXCEPT FOR THE INFRINGEMENT INDEMNIFICATION PROVIDED HEREUNDER) AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

10.0 CHANGE CONTROL PROCEDURES AND DISPUTE RESOLUTION

10.1 Change Control: The City shall have the continuing right to request in writing that Vendor make or permit changes, modifications or enhancements to the Services described in this Agreement in accordance with the procedures hereinafter set out. Nothing in this section shall prevent any such request from being made as a result of a Change suggested by Vendor.

10.2 To request a Change, the City will issue a written Change Order Request to Vendor, in the form attached as SCHEDULE D ("Change Order Request"), or Vendor will send a Change Order Request to the City as the case may be, specifying the proposed Change and the purpose or objective sought with such proposed Change.

10.3 Within two (2) Business Days or a timeframe mutually agreed to in writing, after the Change Order Request is received by Vendor or presented to the City, as the case may be, the Vendor shall deliver to the City a written Change Order Response ("Change Order Response") which shall include, at a minimum, the

following information:

(1) The reason for Change where Vendor suggested the Change to the City;

(2) Sufficient information for a Statement of Work;

(3) Task definition and detailed statement of work specifying how the proposed Change would be implemented;

(4) Any deliverables;

(5) Performance schedule and the effect, if any, that such Change will have on the performance of Vendor's obligations under the Statement of Work;

(6) Any additional or reduced costs to the City that will result from the implementation of such Change and, if additional costs, the cost estimate on a fixed price basis; and

(7) Recommended action.

10.4 If the Change Order Response is acceptable to the City and if the approval of the Deputy City Manager, a standing committee or City Council is not required, the Parties will execute a mutually agreed Change Order ("Change Order") to authorize the making of the Change and thereafter the Services shall be deemed to include the services described in such Change Order, provided that the City's Project Lead as identified in the applicable Statement of Work may provide written approval to the Change Order Response if it does not involve or result in any increase in the Fixed Fee. The City reserves the right to accept or reject any Change Order Response, in whole or in part, and, if dissatisfied with the Change Order Response received, the right to request a new one. Despite any other provision in this Agreement, Change Orders signed by both Parties shall be deemed to be a duly authorized amendment to the applicable Statement of Work. Each Change Order shall be attached to the applicable Statement of Work and shall form part of this Agreement as if originally set out herein and have effect accordingly.

10.5 Upon receipt of the fully executed Change Order, Vendor will be authorized to commence the Change.

10.6 Execution by the parties of the process provided for in this section shall not be considered a *force majeure* event for the purposes of section 3.2 and, as a result, shall not excuse or absolve a party from any delay in or failure of performance by it under this Agreement including any Statement of Work. Any claim by Vendor for extension or reduction of time (if applicable) resulting from such changes or additions to any Services shall be considered by the City, and if the City allows such claim, in its sole discretion, this Agreement shall be adjusted by the City as at the time of the City ordering such change in accordance with the City's policy.

10.7 Dispute Resolution: Except where expressly excluded from the provisions of this section, the parties shall endeavour to resolve any Dispute (other than a dispute with respect to the commencement of an action for injunctive relief or a declaration to restrain or prevent the improper use or misappropriation of Confidential Information) arising between the parties. A Dispute shall be resolved by employing the procedures provided for below in this section.

10.8 All Disputes which may arise with respect to any matter governed by this Agreement shall, to the extent possible, be resolved by City's Project Manager and Vendor's Project Manager or any persons designated by them in writing to deal with any category of Dispute as soon as practicable.

10.9 The following constitutes the escalation process to resolve a Dispute:

(1) If City's Project Manager and Vendor's Project Manager, or the persons designated as their representatives, are unable to resolve a Dispute within ten (10) Business days of its referral, either one of them can escalate the matter of the Dispute to their respective managers. If these persons are unable to resolve a Dispute within a further ten (10) Business days, either one of them can escalate the matter further or designate for resolution who shall make reasonable efforts to resolve the Dispute within fifteen (15) Business days of its escalation. Each Party shall ensure that its representatives have the necessary authority to resolve any Dispute on its behalf.

(2) If the parties are unable to resolve a Dispute in accordance with the provisions of Section 10.2, 10.3 or 10.4(1), above, then either Vendor or the City may in writing request that City Council be requested to approve the submission of the Dispute to arbitration on terms acceptable to both parties. Arbitration requires the consent of both parties.

10.10 Subject to the terms of this Agreement, unless requested or otherwise agreed to by the City, Vendor shall not stop or suspend its performance under this Agreement pending the resolution of any nominal or immaterial Dispute unless the performance cannot reasonably be continued until the Dispute is resolved, as contemplated in this Section 10.0. At any time prior to the resolution of a Dispute under Sections 10.2, 10.3 or 10.4(1), above, the Parties may agree as to the manner in which to proceed while the resolution of the Dispute is pending and the Parties shall proceed as agreed**.**

11.0 INSURANCE

11.1 The Vendor shall purchase and maintain in force, at its own expense (including the payment of all deductibles) and for the duration of this Agreement, the following policies of insurance, which policies shall be in a form and with an insurer acceptable to the City. A certificate of these policies originally signed by

the insurer or an authorized agent of the insurer must be delivered to the City prior to the commencement of the Services:

11.2 Commercial General Liability provided that the policy:

(1) Is in the amount of not less than Two Million Dollars ($2,000,000), per occurrence;

(2) Adds the City of Toronto as additional insured;

(3) Includes Non Owned Automobile Liability, Employer's Liability and/or Contingent Employer's Liability, and any other provision relevant to the services;

(4) Includes a clause which will provide the City with thirty (30) days' prior written notice of cancellation or material change in coverage.

11.3 Professional Liability (errors and omissions coverage) for the performance of Services by the Vendor providing that the policy:

(1) Is in the amount of not less than One Million Dollars ($1,000,000);

(2) Will extend to infringement of copyright and other intellectual property, including misuse of trade secrets, if appropriate.

11.4 Notwithstanding anything to the contrary contained in this Agreement, kept in full force and effect for a period of time ending no sooner than TWO YEARS after the termination or expiry of this Agreement, as the case may be.

11.5 Automobile Liability insurance with a minimum limit of $1,000,000 for all owned or leased licensed motorized vehicles used in the performance of services.

11.6 It is understood and agreed that the coverage and limits of liability noted above are not to be construed as the limit of liability of the Vendor in the performance of Services. It is also agreed that the above insurance policies may be subject to reasonable deductible amounts, which deductible amounts shall be borne by the Vendor. At the expiry of the policies of insurance, original signed Certificates evidencing renewal will be provided to the City without notice or demand.

11.7 The Vendor is responsible for any loss or damage whatsoever to any of the its materials, goods, equipment or supplies and will maintain appropriate all-risk coverage as any prudent owner of such materials, goods, supplies and equipment. The Vendor shall have no claim against the City or the City's insurers for any damage or loss to its property and shall require its property insurers to waive any right of subrogation against the City.

11.8 No limitations of liability apply to this section 11.

11.9 This section shall survive the termination or other expiry of this Agreement.

12.0 OWNERSHIP OF PROJECT DOCUMENTATION

12.1 As between the parties, Vendor will and does retain all right, title and interest (including, without limitation, all Intellectual Property Rights) in and to the Products. Except as set out above, the City retains all ownership rights to City Data and City Content. Subject to article 12.2, below, all information, data, plans, specifications, reports, estimates, summaries, photographs and all other Documentation prepared by the Vendor in the performance of the Services under the Agreement, whether they be in draft or final format, shall be the property of the City.

12.2 The City acknowledges that the Vendor shall retain all right, title and interest its pre-existing intellectual property. The Vendor will grant to the City a fully paid-up, royalty free, perpetual, non-transferable and non-exclusive license to use the Documentation described in article 12.1 above for internal business purposes only and the purposes of the specific project(s) or services for which the Deliverables were provided.

13.0 FEES AND BILLING

13.1 The City and Vendor agree that the Fixed Fee set out in any applicable Statement of Work is the all-inclusive total amount that may be charged by Vendor to the City for the Deliverables and Services identified in such SOW and is exclusive of all applicable taxes. Without written amendment, the cumulative amount of the Fixed Fees set out in any Schedule to this Agreement shall not exceed the amount of nine hundred and fourteen thousand, three hundred and forty two dollars and sixty cents ($914,342.60 (CDN) net of HST) plus applicable taxes.

13.2 The City is not required to pay to the Vendor under this Agreement any sums in excess of the Fixed Fee for the provision of the Deliverables and Services set out in any applicable Order or SOW. The City is only obligated to pay additional amounts if, and only if, there is an amendment to this Agreement, including Change Orders, approved in writing by the City and Vendor. The parties acknowledge that there are no such signed amendments or Change Orders as at the date of signing of this Agreement.

13.3 No fees or expenses of any kind whatsoever, including any travel or transportation costs, shall become payable to Vendor pursuant to the Agreement other than pursuant to one or more Schedules appended to this Agreement by amendment, and, subject to any increases authorized by the City or its authorized representatives.

13.4 When submitting an invoice, the relevant Purchase Order or Blanket Contract number, City Project Manager's name and location, along with the approved Deliverables/ location/Services being billed and any separate document evidencing approval by the City of such Deliverables will be attached to such invoice. Vendor will also provide the cost per hour, per consultant (if applicable) for the City's information purposes only.

13.5 Payment of such invoices will be net sixty (60) days from receipt of the invoice.

13.6 Vendor shall submit invoices in the detail set out above, and the City reserves the right to reasonably require further proof or documentation from Vendor in respect of the Deliverables and Services provided or performed or expenses incurred by Vendor and Vendor shall provide, without unreasonable delay, such further proof or documentation. If the City disputes an amount pertaining to the Services which are the subject of the invoice, the City shall advise the Vendor in writing of the reasons for disputing the charges and the Vendor shall remedy the problem at no additional cost to the City before the City shall be obliged to pay the disputed portion of the invoice. Vendor shall issue no invoices for any Deliverable or Services prior to the issuance of a Notice of Acceptance from the City for the Deliverable or Services being invoiced.

13.7 If any charge owing by the City is 30 days or more overdue, Vendor may, without limiting its other rights and remedies, suspend the Services until such amounts are paid in full, provided Vendor has given the City at least 10 days' prior written notice that its account is overdue. Vendor shall not exercise its rights under the foregoing sentence if the City is disputing the applicable charges reasonably and in good faith and is cooperating to resolve the dispute.

13.8 The Vendor shall be solely responsible for the payment of all of its Personnel costs including statutory and otherwise (including without limitation subcontractors and suppliers and their respective Personnel) made available by it and used for performance of any of the Services.

14.0 TERMINATION

14.1 Upon giving the Vendor not less than thirty (30) days' prior written notice, the City may, at any time and without cause, cancel this Agreement, in whole or in part or a Statement of Work under this Agreement in whole or in part. In the event of such cancellation, the City shall not incur any liability to Vendor apart from the payment for the goods, material, articles, equipment, work or services that have been satisfactorily delivered or performed by the Vendor at the time of cancellation.

14.2 If the Vendor is unable to correct any major or minor deficiencies within three (3)

of the UAT period(s), or if more than three (3) deficiencies of the same type (excluding cosmetic) occur within the UAT Period, the City may deem the Solution to be a total failure and at its option may terminate the UAT period and terminate the Agreement. In such event, the Solution shall be returned to the Vendor and the Vendor shall forthwith repay to the City all payments it has received pursuant to the Agreement (plus interest commencing on the day of the termination at a rate of prime plus two (2) percent per annum).

14.3 Conversely, if the Vendor does correct any deficiencies and if more than three (3) deficiencies of the same type do not occur within the City Acceptance Testing Period, or in the event that the City elects not to exercise its right of termination as set out herein, then the Vendor shall be entitled to receive a notice of waiver of the termination rights set out in this Section from the City in respect of such UAT period and the Project will proceed to Phase 6 – Go Live – Registration and Voting.

14.4 If the Vendor is unable to meet the critical Milestones or is unable to fulfill the Requirements detailed in this SOW, or if the City has reason to believe that any of the principles of the *MEA* are at risk of being compromised, thus impacting the security, integrity or privacy of the election, the City will halt the Project and may terminate the Agreement. In such event, the IVS will be returned to the Vendor and the Vendor shall forthwith repay to the City all payments it has received pursuant to the Agreement (plus interest commencing on the day of the termination).

14.5 Failure of a Party to perform its obligations under this Agreement shall entitle the other Party to terminate this Agreement upon thirty (30) calendar days' written notice describing such breach in reasonable detail if a breach which is remediable is not rectified in that time or within such time as the parties may agree. The Vendor agrees to continue the Services until such time as the City, acting expeditiously, can transition to another solution or twelve (12) months, whichever is earlier. The City will continue to pay for such Services.

14.6 All rights and remedies of a Party for any breach of the other Party's obligations under this Agreement shall be cumulative and not exclusive or mutually exclusive alternatives and may be exercised singularly, jointly or in combination and shall not be deemed to be in exclusion of any other rights or remedies available to the City under this Agreement or otherwise at law.

14.7 No delay or omission by a Party in exercising any right or remedy shall operate as a waiver of them or of any other right or remedy, and no single or partial exercise of a right or remedy shall preclude any other or further exercise of them or the exercise of any other right or remedy.

14.8 Upon termination, all originals and copies of data, plans, specifications, reports, estimates, summaries, photographs, and other documents that have been

accumulated and/or prepared by Vendor in performance of this Agreement shall be delivered to the City in a clean and readable format.

14.9 Immediately following termination of this Agreement, the City shall cease using all Products. Upon request, at no additional charge, Vendor will return City Data to the City via City's secure FTP site in the same format in which the City Data was originally inputted into the Solution. Alternatively, City Data can be returned in a mutually agreed format at a scope and price to be agreed. Unless otherwise requested by the City, Vendor will maintain a copy of City Data for no more than six (6) months following termination of the Agreement, after which time any City Data not retrieved will be destroyed.

15.0 CONFIDENTIAL INFORMATION

15.1 Each party to this Agreement and its Personnel (the "Receiving Party") will treat as confidential all financial, statistical, Personnel, technical and general data related to the operations of the other party to this Agreement (the "Disclosing Party"), including (without restriction) any pertaining to third parties, which come to the attention of the Receiving Party in the course of carrying out the Services under this Agreement and any Schedule or Statement of Work, and which are not or do not subsequently become public knowledge through no fault of Receiving Party, and will not disseminate same for any reason whatsoever without the express written permission of the Disclosing Party.

15.2 At the request of the City, Vendor will sign a non-disclosure agreement and will require any Personnel to sign such agreement.

15.3 Despite the foregoing, a Receiving Party shall not be required to keep confidential any data which (i) is or becomes publicly available through no fault of The Receiving Party; (ii) is already rightfully in possession of the Receiving Party and not subject to any pre-existing obligation of confidentiality; (iii) is independently developed by the Receiving Party outside the scope of this Agreement; (iv) is rightfully obtained from third parties; or (v) is required to be disclosed by operation of law.

(1) At the request of Disclosing Party, or upon the expiry or cancellation of the Services or the termination of this Agreement, as the case may be, each Receiving Party, agrees to return to the Disclosing Party, no later than three (3) Business Days thereafter, all such data, and all written or descriptive matter, including but not limited to drawings, prints, descriptions or other papers, documents or any other material which contains any Confidential Information, regardless of the media on which it is resident or stored and regardless of the form in which it may then appear, and including without limitation all such data and all written or descriptive matter, including but not limited to drawings, prints, descriptions or other papers, documents or any other material which contains any Confidential Information, held by any of its

Personnel, or partner, subcontractor or agent of the Receiving Party, and including all copies thereof;

(2) Destroy all electronic versions of the Disclosing Parties' Confidential Information in its possession or in the possession of any of its Personnel, or in the possession of any of its partners, subcontractors or agents; and

(3) Certify to the Disclosing Party that this has been done.

15.4 This section 15.0 is subject to MFIPPA and PHIPA and shall survive the termination or expiry of this Agreement.

16.0 NOTICES

16.1 Any notice required or permitted to be given under this Agreement shall be delivered as follows:

(1) If to the City:

Attn: John Meraglia

CITY OF TORONTO
City Clerk's Office, Elections and Registry Services Unit
89 Northline Road
Toronto ON M4B 3G1

Phone Number: (416) 395-1303
Fax Number: (416) 395-1300
Email: jmeragli@toronto.ca

With a copy to:

Susie Mahendran
Supervisor, Contract Administration, Coordination & Approvals
Information & Technology Division
55 John Street
Metro Hall, 15th Floor
Toronto ON M5V 3C6

Phone Number: (416) 338-1240
Fax Number: (416) 696-4161
Email: smahend@toronto.ca

(2) If to the Vendor:

Attn: Richard Catahan

SCYTL CANADA INC.
1155 North Service Road West, Unit 11
Oakville ON L6M 3E3

Phone Number: (289) 795-3252
Fax Number: (289) 291-4001
Email: richard.catahan@scytl.com

16.2 Any notice delivered to the party to whom it is addressed as provided above under this section shall be deemed to have been given and received on the day it is delivered at that address, provided that if that day is not a Business Day then the notice shall be deemed to have been given and received on the first Business Day next following that day.

16.3 Any notice mailed under this section shall be deemed to have been given and received on the third business day next following the date of its mailing.

16.4 Any notice transmitted by facsimile or other form of recorded communication under this section shall be deemed given and received on the first Business Day after its transmission (provided such transmission is confirmed with the other party).

16.5 In the event of postal disruption, a notice under this section must either be delivered personally or sent by facsimile or other form of recorded communication. Any Notice of Termination under section 14.0 must be delivered personally.

17.0 GENERAL

17.1 This Agreement constitutes the complete and exclusive statement of the agreement between the parties, which supersedes all proposals, oral or written, and all other communications between the parties, relating to its subject matter. Purchase orders submitted by the City are for the City's internal administrative purposes only, and the terms and conditions contained in those purchase orders will have no force and effect.

17.2 If one or more of the phrases, sentences, clauses, paragraphs, sections or subsections contained in this Agreement is declared invalid by the final and unappealable order, decree or judgment of any court of competent jurisdiction,

this Agreement shall be construed as if such phrase(s), sentence(s), clause(s), paragraph(s), section(s) or subsection(s), had not been inserted.

17.3 This Agreement may be changed only by a written amendment signed by authorized representatives of both parties, by a Change Order pursuant to the provisions of section 10.0, or by a court order pursuant to section 17.2 hereof.

18.0 ENUREMENT/ASSIGNMENT

18.1 This Agreement shall inure to the benefit of and be binding upon the parties and their respective successors and, subject to subsection 18.2 hereof, assigns only.

18.2 Neither party shall assign this Agreement or any interest in it without the prior written consent of the other; provided, however, that the Vendor, without the consent of the other City, may transfer this Agreement to an Affiliate or to a successor (whether direct or indirect, by operation of law, and/or by way of purchase, merger, consolidation or otherwise) where, unless otherwise agreed in writing, the responsibilities or obligations of the other party are not increased by such assignment and the rights and remedies available to the other party are not adversely affected by such assignment, and for the purposes of this Agreement, such transfer of this Agreement shall include any transfer in the majority ownership or controlling interest in the Vendor, whether through the sale of shares, direct acquisition of assets or otherwise. The Vendor shall notify the City by letter from Vendor's lawyer, promptly of such an event and provide the City with the necessary confirming documentation that all actions completed have been done as required by law in the jurisdiction as applies.

19.0 AUDIT

19.1 The City may audit all financial and related records associated with the terms of the contract including timesheets, reimbursable out of pocket expenses, materials, goods, and equipment claimed by the Vendor. The Vendor shall at all times during the term of the contract, and for a period of two (2) years following completion of the Contract, keep and maintain records of the work performed pursuant to this Contract. This shall include proper records of invoices, vouchers, timesheets, and other documents that support actions taken by the Vendor. The Vendor shall at his own expense make such records available for inspection and audit by the City within 90 days from the date of request.

20.0 OCCUPATIONAL HEALTH AND SAFETY

20.1 The Vendor shall comply with all federal, provincial or municipal occupational health and safety legislative requirements to which it is subject, including, and

without limitation, the Occupational Health and Safety Act, R.S.O., 1990 c.0.1 and all regulations thereunder, as amended from time to time (collectively the "OHSA").

20.2 Nothing in this section shall be construed as making the City the "employer" (as defined in the OHSA) of any workers employed or engaged by the Vendor for the either instead of or jointly with the Vendor.

20.3 The Vendor agrees that it will ensure that all subcontractors engaged by it are qualified to perform the Services and that the employees of subcontractors are trained in the health and safety hazards expected to be encountered in the Services, if any.

20.4 The Vendor acknowledges and represents that:

i. The workers employed to carry out the Services have been provided with training in the hazards of the Services to be performed and possess the knowledge and skills to allow them to work safely;

ii. The Vendor has provided, and will provide during the course of the agreement, all necessary personal protective equipment for the protection of workers;

iii. The Vendor's supervisory employees are competent, as defined in the OHSA, and will carry out their duties in a diligent and responsible manner with due consideration for the health and safety of workers;

iv. The Vendor has in place an occupational health and safety policy in accordance with the OHSA; and

v. The Vendor has a process in place to ensure that health and safety issues are identified and addressed and a process in place for reporting work-related injuries and illnesses.

20.5 The Vendor shall provide, at the request of the Chief Information Officer or his designate, the following as proof of the representations made in Section 20.4(i) and (iv):

i. documentation regarding the training programs provided or to be provided during the Services (i.e., types of training, frequency of training and re-training); and

ii. the occupational health and safety policy.

20.6 The Vendor shall immediately advise the Chief Information Officer or his designate in the event of any of the following:

i. A critical injury that arises out of Services, while on the City's premises, that is

the subject of this agreement;

ii. An order(s) is issued to the Vendor by the Ministry of Labour arising out of the Services that is the subject of this agreement;

iii. A charge is laid or a conviction is entered arising out of the Services that is the subject of this agreement, including but not limited to a charge or conviction under the OHSA, the Criminal Code, R.S.C 1985, c. C-46, as amended and the Workplace Safety and Insurance Act, 1997, S.O. 1997, c. 16, Sched. A, as amended.

20.7 The Vendor shall be responsible for any delay in the progress of the Services as a result of any violation or alleged violation of any federal, provincial or municipal health and safety requirement by the Vendor, it being understood that no such delay shall be a force majeure or uncontrollable circumstance for the purposes of extending the time for performance of the Services or entitling the Vendor to additional compensation, and the Vendor shall take all commercially reasonable steps to avoid delay in the final completion of the Services without additional cost to the City.

20.8 The parties acknowledge and agree that employees of the City, including senior officers, have no authority to direct, and will not direct, how employees, workers or other persons employed or engaged by the Vendor do work or perform a task that is the subject of this agreement.

21.0 WORKPLACE SAFETY AND INSURANCE ACT

21.1 The Vendor shall be in good standing with the Workplace Safety and Insurance Board ("WSIB") throughout the term of this Agreement. If requested by the Chief Information Officer or his designate, the Vendor shall produce certificates issued by the WSIB to the effect that they have paid in full their assessment based on a true statement of the amount of payrolls. If the Vendor is considered by WSIB to be an independent operator without coverage, the Vendor shall provide a letter to that effect from the WSIB.

22.0 ACCESSIBILITY STANDARDS FOR CUSTOMER SERVICE TRAINING REQUIREMENTS

22.1 The Vendor shall require all applicable personnel (including those of its subcontractors) to fulfill the training requirements set out in the City's policy on Accessible Customer Service Training Requirements for Contractors, Consultants and other Service Providers.

23.0 NON-SOLICITATION

23.1 The Vendor shall not actively recruit for employment any member of the City's staff, but nothing herein shall prevent the Vendor from hiring or retaining at any time any such member who has responded to a public advertisement for such employment or engagement.

23.2 The City shall not actively recruit for employment any member of the Vendor's staff prior to the expiry of the provision of the last of the Services most recently supplied by such member, but nothing herein shall prevent the City from hiring or retaining at any time any such member who has responded to a public advertisement for such employment or engagement.

23.3 This section 23.0 shall survive the termination or expiry of this Agreement for a period of twelve months.

24.0 INDEPENDENT CONTRACTOR

24.1 The relationship of the City and the Vendor is one of owner and independent contractor and not one of employer-employee. Neither is there any intention to create a partnership, joint venture or joint enterprise between the Vendor and the City.

25.0 PUBLICITY

25.1 Subject to the provisions of this Agreement, neither party nor any of its affiliates, associates, third-party service providers, and subcontractors, shall make any public announcement or release for publication any information in connection with this Agreement or its subject matter, without the prior written consent of the other which shall not be unreasonably withheld.

26.0 NON-EXCLUSIVITY

26.1 The Vendor acknowledges and agrees that the entering into of this Agreement by the City is not a guarantee or promise of exclusivity, and that the City in its discretion may arrange for performance of any Services by entities other than the Vendor.

27.0 COMPLIANCE WITH LAWS

27.1 Each Party shall comply with all federal, provincial and municipal laws and regulations to which it is subject in performing its obligations under this Agreement, including, without limitation, the *Occupational Health and Safety Act and the Workplace Safety and Insurance Act,* 1997, or any successor legislation,

as applicable.

28.0 GOVERNING LAW

28.1 This Agreement shall be governed by the laws of the Province of Ontario, and of Canada. Any dispute arising out of this Agreement will be determined by a court of competent jurisdiction in the Province of Ontario unless otherwise agreed to in writing by the City.

29.0 SCHEDULES

The following schedules are attached to and from a part of this Agreement in the same manner and with the same effect as if they were included in the body hereof:

SCHEDULE "A-1" – Statement of Work
SCHEDULE "B" – List of Base Software and Base Software Pricing
SCHEDULE "C" – Schedule of Forms
SCHEDULE "D" – Change Order Form
SCHEDULE "E" – Hourly Rates
SCHEDULE "F" – Testing: Quality Assurance Plan/Quality Assurance Details
SCHEDULE "G" – Training
SCHEDULE "H"– Requirements
SCHEDULE "I" – IVR Telephone Voting Service Requirements
SCHEDULE "J" – Quality Level Metrics
SCHEDULE "K" – Key Project Milestones and Dates
SCHEDULE "L" – Internet Voting Service Process Diagrams
SCHEDULE "M" – The City's Existing I&T Infrastructure
SCHEDULE "N" – Service Level Agreement
SCHEDULE "O" – Escrow Provisions

IN WITNESS WHEREOF the parties hereto have hereunto affixed their corporate seals attested to by the hands of their respective proper signing officers in that behalf duly authorized.

CITY OF TORONTO
Per:

Name:
Title:

CITY OF TORONTO
Per:

Name: Ulli S. Watkiss

Title: City Clerk

SCYTL CANADA INC.

Per:

Name: Richard Catahan
Title: Director of Operations, Canada

I have authority to bind the company

Authorized by CC48.4 adopted by City Council at its meeting on February 19th and 20th, 2014.	Authorized pursuant to Purchasing Policy number FS-PMM-14 – Computer Related Purchases	APPROVED AS TO FORM
Marilyn M. Toft Ulli S. Watkiss City Clerk	Rob Meikle Chief Information Officer	Anna Kinastowski City Solicitor

SCHEDULE "A-1"

STATEMENT OF WORK

to the Master Agreement (the "Master Agreement") dated the ___day of March, 2014,

between

CITY OF TORONTO (the “City”)

- and -

Scytl Canada Inc. (“Scytl” or “Vendor”)

Statement of Work – Internet Voting Services for the 2014 Municipal Election

THIS STATEMENT OF WORK has an effective date of the 1st day of April, 2014 (the “Effective Date”).

GENERAL

This Statement of Work ("SOW") forms part of the Agreement for the supply, delivery, implementation and support of an Internet and Telephone Voting Service for persons with disabilities between the parties dated as of the Effective Date (the “Agreement”). Hereafter, the Service for Internet Voting, Telephone Voting, the Voter Contact Centre and the Centralized Electronic Voters’ List management system (CEVL) will be collectively referred to as an "Internet Voting Service" or "IVS."

Any capitalized term not defined herein shall have the definition provided for in the Master Agreement. The paramount provisions set out in Article 1.7 of the Master Agreement shall apply in the event of any inconsistency or conflict between the terms of this SOW and any other part of the Master Agreement.

This SOW includes contracted terms regarding the Project Management, Project Team Members, Scope of Work, Deliverables, Payment Milestones, Payment Schedules, and Cost of Services for the Deliverables as identified in this SOW.

The Vendor is expected to provide the Deliverables detailed in this SOW, at a minimum. The Vendor should consult the RFP for any Deliverables and Milestones not specified in this SOW.

DETAILED STATEMENT OF WORK

1.0 GENERAL PROJECT MANAGEMENT

The Parties each agree to designate a Project Manager from their respective organizations with adequate authority and full technical competence to deal with matters relating to the Services to be provided under the Agreement (each, being a "Project Manager"). The Project Managers will, on behalf of their respective Parties and in accordance with the provisions of the Agreement, use all reasonable efforts to co-ordinate the timely supply, delivery, and performance of the Services identified in the Agreement. Scytl will require approval from the City Project Manager for the assignment and substitution of any and all Scytl resources, in accordance with the Agreement. The City Project Manager is Jerry Liu and the Vendor Project Manager is Richard Catahan. The Project Managers are authorized to deal with the day-to-day matters related to the delivery of the Services pursuant to this SOW.

2.0 SPECIFIC PROJECT MANAGEMENT

Scytl's Project Management Team will be responsible for quality assurance, timeliness, formal progress reporting and clear communications with the City contacts during the implementation of the Internet Voting Service. Scytl's Project Management Team will also be responsible for providing the Services consistent with this SOW, a detailed Project Plan with specific timelines, the Scope of Work, the Deliverables and all of Scytl's resource assignments for the Project. Scytl's resource assignments for the Project will be reviewed, modified and accepted by the appropriate City resource(s) as may be determined by the City in accordance with the Approval Process. Scytl will also provide detail related to use of subcontractor services, including but not limited to, the location of the Service, the scope and the details of the service. Scytl will require approval from the City Project Manager for change of scope, location and provider of any in-scope services. Scytl's Project Management Team has overall responsibility for the planning and delivery of the Services. It is understood that the City of Toronto has responsibilities that affect the ability of Scytl to deliver the Services to be provided under the Agreement, and the success of this Project will be determined through the partnership of the City's and Scytl's combined team.

2.1 City Responsibilities

1) The City Project Manager will be responsible for:

   a) Serving as the key contact for the Vendor;

   b) Approving the Vendor's Project Plan;

   c) Providing clarifications and instructions to the Vendor throughout the Project;

d) Monitoring the Vendor's delivery of the Services; and

e) Providing overall direction, management and leadership of the Project for the City.

2) The City has a Project Management Office ("PMO") that will be responsible for:

a) Assigning City Staff to the Project to facilitate the achievement of the outcome;

b) Approving all Deliverables in accordance with the Approval Process, and assuming responsibility for the overall direction of the Project;

c) Acting as the primary decision-making body to oversee and to provide overall strategic direction for the Project Working Group;

d) Acting as the primary authority for all decisions relating to the IVS's design, methodology, architecture and implementation, as required;

e) Acting as primary liaison with senior City representatives, senior Vendor representatives through the City Project Manager, and with senior representatives of outside community agencies and organizations, as required;

f) Acting as the primary authority for approval of Change Orders and amendments to the Master Agreement; and

g) Acting as the primary authority, and providing approvals for all outgoing publications or communications regarding the Project.

3) The City will have a Project Working Group that, under the coordination of the City Project Manager, will be responsible for:

a) Acting as liaison with the Vendor for the purpose of configuring, developing, training, integrating and implementing the IVS, and coordinating all Vendor activities and results;

b) Acting as liaison during Test planning and IVS Performance tests and User Acceptance Tests (UAT) between the Vendor and the third-party Quality Assurance (QA) Testing Firm engaged by the City;

c) Making recommendations to the Project Management Office regarding changes to business practices affected by the implementation of the IVS;

d) Assisting the Vendor in determining the impacts of the IVS on the City, City staff, and/or any other impacted community agencies, organizations or individuals;

e) Assisting in the implementation of the IVS and ensuring a smooth transition of all affected business practices and protocols; and

f) Reviewing and making recommendations to Project Management Office regarding all aspects of the IVS and its impact on the Division and/or the City as a whole.

2.2 Vendor Responsibilities

1) The Vendor's Project Manager will coordinate the delivery of the Services with the City's Project Manager, and will be responsible for:

   a) Submitting a detailed, initial Project Plan satisfactory to the City within two (2) weeks of the Effective Date of the Master Agreement;

   b) Providing regular written progress reports to the City Project Manager at a minimum of once a week and more frequently if, at the City's or the Vendor's discretion, the situation so warrants, including meeting/interviewing with City staff throughout the Project as required;

   c) Coordinating the delivery of the Services, and identifying City resources that may be required to work on the Project, specifying skill sets, dates and work hours;

   d) Updating the Project Plan as required for the approval of the City's Project Manager; and

   e) Ensuring that all Vendor activities remain on track and that the Services and Deliverables are completed within the timeframes and boundaries described by the approved Project Plan, in alignment with the Scope of Work in Section 4.0 – SCOPE OF WORK.

2) The Vendor will take direction from the City's Project Manager throughout the Project;

3) The Vendor will be responsible for managing and/or replacing their Project staff when so requested by the City, as the City deems necessary, based on the expert opinion of the City's Project Manager. No Vendor staff assigned to, or working on the Project will be removed by the Vendor from the Project without the City Project Manager's prior written unless the removal is beyond the control of the Vendor or if the removal is necessary in order to facilitate Vendor's performance of the Services and Deliverables specified in the Agreement. The replacement of staff shall not entitle the Vendor to any increase in the Fixed Fee of the Project;

4) The Vendor will require written Notice of Acceptance from the City for each implementation phase of the IVS before proceeding to the next phase in the Project.

3.0 TEAM MEMBERS

3.1 City Project Team Members

Name	Title
Project Management Office	
Bonita Pietrangelo	Director, Elections and Registry Services
Jerry Liu	Project Manager, I&T Division, Project & Resource Management Office
John Meraglia	Manager, Elections and Registry Services
Project Working Group	
Tammy Milekovic	Project Coordinator (I&T)
Tiffany Lam	Election Coordinator, Elections and Registry Services (Alternative Election Strategies)
Ian Smith	Election Coordinator, Elections and Registry Services (Alternative Election Strategies)
TBA	TIS Technical Coordinator
Eddie Ng	Security/Risk Mgmt. Specialist, I&T Division, Strategic Architecture & Planning, Risk Management & Information Security
Brent Lanteigne	Senior Systems Integrator, I&T Division, Application Services, Solutions Development
TBA	Manager , 311 Toronto, Operations
TBA	Consultant, Equity, Diversity & Human Rights Division

3.2 Scytl Canada Key Project Team Members and Rates

The Vendor Project Team listed below will be committed as required in the Project Plan in the roles that they are performing for the duration of the Project. Any substitutions must be pre-approved by the City in accordance with Article 4.0 of the Master Agreement. The Vendor Project Team members are: s. 14(1) applied s. 10 applied

Vendor Core Resources	Title	Hourly Rate
Gerard Cervello Garcia	Executive Sponsor	-
Richard Catahan	Project Director	[redacted]
Carlos Vega	Infrastructure SME	[redacted]
Daniel Cheng	Subject Matter Expert	[redacted]
Eric Cottreau	Support Lead	[redacted]
Danny Barbeau	Senior Support Manager	[redacted]
Stephen Sutherland	Senior Data and Program Support Manager	[redacted]
Jesus Choliz	Director of Security & Compliance	[redacted]
Amil Hasanbegovic	Accessibility SME	[redacted]
Glenn Foote	Subject Matter Expert	[redacted]
Davi Bosch	Account Manager	-
Alina Zugulova	Project Manager (Off-Site)	[redacted]
Juan M Caicedo	Project Manager (Local)	[redacted]
Ruben Salvador	Technical Manager	[redacted]
Marcel Arrufat	Development Team Lead	[redacted]
Roger Castells	IT Infrastructure	[redacted]
Mariano Hedrosa	Architecture Infrastructure	[redacted]
Rodrigo Rojas	Business Analyst	[redacted]
Dimitrios Kapanidis	Quality Assurance Manager	[redacted]
Hortense Harvey	DataFix Project Manager	[redacted]
Geoff Day	DataFix Technical Lead	[redacted]

Derrick Leahy	DataFix Development Lead	[redacted]
Jim Stewart	DataFix Subject Manager Expert	[redacted]

Note: The hourly rate has been included for information purposes only. Scytl will be responsible for delivering the Services in accordance with the payment milestones identified in the Payment Schedule of this SOW. The hourly rate will only be used in the event that additional services are required by the City during the Term of the Master Agreement.

4.0 SCOPE OF WORK

The IVS is to meet the objectives described in Section 4.1 of this SOW and the Requirements described in SCHEDULE "H" and SCHEDULE "I" of the Agreement.

The IVS must provide the following high level deliverables:

1) A secure and functional IVS for persons with disabilities for the City's 2014 Municipal Election Advance Vote, which includes:

    a) An **Internet Voting Service and Telephone Voting Service** for use by persons with disabilities in the City's 2014 Municipal Election Advance Vote, from October 14 to October 19, 2014, inclusive;

    b) A **Voter Contact Centre** which is capable of processing Internet voting registrations and initial processing and mailing out of Voters' List Amendment Applications and Personal Information Number (PIN) packages, and which can handle the call volumes specified in the Functional and Capacity Requirements outlined SCHEDULE "J" – QUALITY LEVEL METRICS. Voter Contact Centre agents must be trained and knowledgeable in providing accessible customer service; and

    c) A **Centralized Electronic Voters List management system** (CEVL) that provides real-time synchronization of the voters' list during the Internet Voting Registration period and across all Advance Vote voting channels (Internet Voting, Telephone Voting and in-person Advance Vote).

2) WCAG 2.0 Level AA compliancy on all voter-facing components, including training and support tools.

3) A demonstrated understanding of accessibility and accommodation requirements of Persons with Disabilities in the delivery of the Service.

4) The Registration Go-Live date of September 8, 2014 and the Advance Vote period from October 14 to October 19, 2014 (inclusive) and the October 27, 2014 Election Day, are fixed, immovable targets. Therefore, the Vendor must execute the implementation of the IVS with high agility, meeting or beating all the deadlines set out in the agreed Project Plan. The City Project Team will strive to work collaboratively with the Vendor in the most efficient manner.

4.1 Objectives

The main objective of the Internet Voting Project for 2014 Municipal Election is for the Vendor to deliver a Commercial Off–the-Shelf (COTS) Solution which will allow persons with disabilities to cast a vote from any location, provided they have access to a computing device and the Internet, the assistive technology that they may require to use the computing device or a touchtone telephone. The IVS must verify the voter's identity and their eligibility to vote using a randomly-generated, unique Personal Identification Number and personal password to authenticate. The IVS must then display or read the appropriate online or over the phone using an Interactive Voice Response (IVR) system. In addition to the objectives stated above, the City requires that the Internet Voting Project also satisfy the following objectives:

1) The IVS must be accessible to persons with all types of disabilities and must adhere to the following principles of the *MEA*:
    - The secrecy and confidentiality of an individual's vote is paramount;
    - The election is fair and must not favour one candidate over another;
    - The election is accessible to all voters;
    - The integrity of the process is maintained throughout the election;
    - Voters and candidates are treated fairly;
    - There should be certainty that the results of the election reflect the votes cast; and
    - The proper majority vote governs by ensuring that valid votes are counted and invalid votes are rejected so far as reasonably possible.

2) The IVS must also:
    - Ensure the secrecy of the vote;
    - Be accessible to all voters;
    - Provide a method of voter authentication;
    - Be secure;
    - Be auditable; and
    - Be scalable, to accommodate increased demand.

3) Voter-facing components of the IVS must be compliant with the *Accessibility for Ontarians with Disabilities Act, 2005 (AODA),* the *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990 Chapter M.56 (MFIPPA),* and *Web Content Accessibility Guidelines (WCAG) 2.0 Level AA*, to allow persons with disabilities to vote independently and secretly, without requiring assistance from another person;

4) The IVS must allow a voter to print or record a secure ballot receipt number once their vote has been cast electronically, to serve as ”proof" that their ballot has been cast;

5) The IVS must accommodate the potential up-take rates of fifty thousand (50,000) votes as outlined in SCHEDULE "J", as well as be scalable and flexible to

accommodate any increase in demand. The IVS is to be sized, at a minimum, according to the following:

	Unit	Size
Total number of Voters in Solution	Electors	1,600,000
Total Internet Voting registrants	Electors	50,000
Total Internet Votes cast	Electors	50,000
Design Capacity (minimum)	Electors	100,000
Projected Concurrent Internet Usage	Electors	6,000
Mean voting session length	Minutes	5
Maximum voting session length	Minutes	30

6) The IVS must integrate with the City's existing Toronto Election Information System (TEIS) application, using the City's specifications as defined in Phase 2 of the Project;

7) The IVS must Go Live on the voter registration start-date of September 8, 2014 to enable persons with disabilities to use a computing device or telephone to cast a ballot during the Advance Vote period from October 14 to October 19, 2014, inclusive.

8) The IVS must successfully pass a full audit. The City will engage an Independent External Auditor in parallel with all phases of the Project. The Auditor will provide the necessary security assessment, privacy assessment, or as required, other review, audit or assessment of the services. The Vendor will provide assistance when required, and the relevant and accurate information or documentation related to the audit activities; and

9) During Phases 1, 2 and 3 of the project, and with advance notice of seventy-two (72) hours to the Vendor, the City will schedule an on-site visit(s) to any of the service locations including but not limited to the Primary Office, Data Centre, Telephone Voting IVR and Voter Contact Centres.

10) After the completion of Phase 4 of the project, at any time without advance notice to the Vendor, the City will schedule an on-site visit(s) to any of the service locations including but not limited to the Primary Office, Data Centre, Telephone Voting IVR and Voter Contact Centres.

5.0 Business Requirements

In addition to those Requirements outlined in this SOW, including Attachment 2 (Training Schedule), the IVS will meet the Requirements listed below:

1) Overall, the IVS must provide for seven (7) separate processes:

   a) **Public Engagement Service:** The Public Engagement Service will be available to the City no later than May 2 2014, and be available according to the Service Level Agreement levels identified in SCHEDULE "J" The Public Engagement Service will consist of a demonstration website and functional IVR phone number that is substantially in the same form as the demonstration provided in the original RFP The City will use the Public Engagement site for communication, education and outreach purposes;

   b) **Demonstration Service:** The Demonstration Service will be available to the City no later than August 11, 2014, and be available for 24 hours each day until August 21, 2014, inclusive. The Demonstration Service will consist of a demonstration website as well as a functional IVR phone number that demonstrates the full functionality and accessibility of the final production environment for the internet and telephone voting service of the IVS;

   c) **Internet and Telephone Voter Registration**: This will last approximately six (6) weeks, beginning at 10:00 AM EST on September 8, 2014, ending 7:00 PM EST on October 19, 2014, inclusive;

   d) **Internet and Telephone Voting:** This process will last six (6) days, and will run concurrently with the in-person Advance Vote period, beginning at 10:00 AM EST on October 14, 2014, and ending at 8:00 PM EST on October 19, 2014, inclusive;

   e) **A Centralized Electronic Voters' List management system (CEVL):** The voter's list must be synchronized on a real-time basis with the in-person Advance Vote voters' list and on a nightly basis throughout the Internet and Telephone Voter Registration and Voting periods. An updated voters' list of who has voted must also be provided to the City on a nightly basis in an .CVS/comma delimited format to allow the City to provide Candidates with an updated list of who has voted in their ward(s);

   f) **Final Results Reporting:** Results from the votes cast using the IVS will be made available after 8:00 PM EST on Election Day, October 27, 2014; and

g) **Disposition of Records:** All IVS configuration data, software or hardware related to the production of results, collected data, activity logs and records must be stored in a secure, encrypted format, for 120 days following the declaration of final results as required by the *MEA* section 88(1). When directed by the City, this data, software or hardware will be destroyed and/or returned to the City, after the 120 day period, providing a Certificate of Destruction (COD), in a hard and soft-copy format.

6.0 Project Phases

1) The Vendor will implement the IVS in the following phases described below:

- Phase 1 – Project Initiation
- Phase 2 – Interface, Configuration and Integration Requirements Validation
- Phase 3 – Customize, Integrate and Test Interface
- Phase 4 – IVS Configuration, Implementation and User Acceptance Test
- Phase 5 – Demonstration and Final Acceptance
- Phase 6 – Go Live – Registration and Voting
- Phase 7 – Project Closure

Note: Dates are to be determined and documented in the Project Plan, however the Vendor's Demonstration Site, which will be used to test the functionality of the IVS, must be completed no later than August 11, 2014, and be available each weekday until August 21, 2014, inclusive. In addition, Phase 6 – Go Live must be completed no later than September 8, 2014 for the commencement of the IVS Registration period.

2) See SCHEDULE "K" for a summary table of key dates and deliverables.

6.1.1 Phase 1 – Project Initiation

The main objectives of this phase are to confirm the project objectives and overall Scope of Work, develop a draft Project Plan consisting of implementation, resource, training, migration, interface and integration requirements, Communication, Security and Test Plans, and to develop processes on Quality Management, Issue Management, Risk Management, Monitoring and Reporting, and Change Management. An initial Project Kick-Off meeting will be held to review the overall Project implementation strategy, roles and responsibilities and timelines. All Plans are living documents that are subject to change, as approved by the City, throughout the Project.

6.1.2 Phase 1: Vendor Responsibilities

In Phase 1 – Project Initiation, the Vendor will, at a minimum:

1) Prepare and conduct the Project Kick-Off meeting;

2) Provide the City with signed Non-Disclosure Agreement forms for all Vendor Project staff, including subcontractors and third-party service providers;

3) Confirm the City's business objectives and overall Statement of Work (SOW);

4) Conduct discovery activities and gap analysis;

5) Develop and deliver a detailed Project, Resource and Deployment Plan ("Project Plan"), which contains the detailed tasks/Work Breakdown Structure (WBS) and timelines to complete the Services in accordance with the specifications and Requirements of the Agreement. The Project Plan, as well as this SOW, will define the Acceptance Criteria for the Deliverables for each Phase.

    a) The Project Plan will include, at a minimum:

        i. A consolidated view of the Project management organization and hierarchy of the assigned City and Vendor resources and the effort required to carry out all of the related activities, tasks, Services and Deliverables for the Project;

        ii. Information for all Project resources to ensure that they have a clear understanding of the activities and tasks that they are responsible for performing to ensure timely completion of the Project;

        iii. A detailed Implementation Plan, Migration Plan, Training Plan, Test Plan, a Support plan, and a schedule of key dates, including dates for Deliverable submissions and Milestones;

iv. A high level Security Plan as related to the service, including any subcontractors. The Security Plan, at a minimum, includes:

    a. A list of all locations where the Services will be provisioned, including any subcontractor locations where information will be processed or accessed;
    b. A high level access model for resources;
    c. A high level Disaster Recovery Plan;
    d. A high level overview of the physical architecture of the complete IVS at all locations;
    e. Recommended security configurations and controls; and
    f. Secure handling of sensitive information.

v. Quality Management, Issue Management, Risk Management, Monitoring and Reporting, and Change Control processes;

vi. A Work Breakdown Structure (WBS) which includes staffing structure, breakdown by activity, task and subtask, including duration (in hours or days) for the entire Project;

vii. A high level overview of the hosting infrastructure, including but not limited to the data centre, Voter Contact Centre and facilities where monitoring of the IVS operations will take place; and

viii. A complete Deployment and Execution Plan for each IVS component, including, but not limited to, the CEVL and the Voter Contact Centre.

b) The Project Plan must identify the activities, tasks and subtasks, including a timeline with duration for each task, for the integration and migration of data between the IVS and the City's adjacent systems, and for executing these integration points with minimal disruption to City resources.

c) The Project Plan must include sufficient time for the City to review each Deliverable. The Vendor must include up to two (2) business days per Deliverable in the Project Plan, for City staff to complete a review and to document their findings. Based on the review findings, the City may approve, reject portions of, or reject the entire Deliverable; and/or request that the Vendor make revisions. If a Deliverable is rejected, the Vendor will have up to two (2) business days, or a time frame mutually agreed upon by both parties, to revise the Deliverable.

d) The Project Plan must be delivered to the City in a Microsoft Project 2007-compatible format. Any supporting documentation should be provided to the City in Microsoft Word/Excel or Adobe PDF format.

6) Work with a third-party QA Testing Firm to develop and deliver a Test Plan. This includes identifying all tools and services required to execute the test(s);

7) Develop and deliver a Communication Plan. Consultations will be set up with key Project Team members and/or stakeholders throughout the implementation process to ensure the Services and Deliverables include all tasks and Requirements the City has identified in Phase 1.

   The Communication Plan must:

   a) Describe how the Project will establish a reliable means of ensuring transparency and co-operation, by communicating status and updates on a weekly basis at a minimum;

   b) Identify the processes, methods, and tools required to ensure timely and appropriate collection, distribution, and management of project information for all project participants; and

   c) Have a detailed timeline for implementation, and target execution dates for each Deliverable, Milestone or Phase of the Plan,

8) Develop and deliver a Training Plan for the variety of roles within the City and the Voter Contact Centre as required by this Project which, at a minimum, includes:

   a) Developing and providing WCAG 2.0 Level AA compliant voter training and education materials on the use of the IVS;

   b) Developing and executing the "Election Official" training plan provided in response to the Requirements;

   c) Developing and executing the "System Administrator" training plan provided in response to the Requirements;

   d) Providing all training manuals, system manuals, testing scripts and results for the City's review, and once approved, for the City's use; and

   e) Provide accessibility training to Voter Contact Centre on meeting AODA compliancy and how to appropriately handle calls from the disabilities community.

9) Provide a high level Service Level Agreement ("SLA"), which includes the Services provided by the Vendor and all third-party subcontractors that will deliver any component of the IVS.

6.1.3 Phase 1: City Responsibilities

In Phase 1 – Project Initiation, the City will:

1) Participate in the Project Kick-Off meeting;
2) Provide the Vendor with the City Non-Disclosure Agreement form;
3) Assist in the review of the business objectives and overall SOW;
4) Assist in the creation of the Project Plan;
5) Provide feedback on the Project Plan;
6) Assemble the City Project team;
7) Approve the Project Plan;
8) Review and approve the Communication Plan;
9) Review and approve the Test Plan;
10) Assist the Vendor in identifying content and data integration and migration requirements;
11) Initiate the Approval Process to be implemented at the end of each Phase; and
12) Visit Vendor hosting and Voter Contact Centre facilities, if required.

6.1.4 Phase 1: Vendor Deliverables

The minimum required Deliverables for Phase 1 – Project Initiation, are:

1) A Project Kick-Off meeting;
2) Signed Non-Disclosure Agreement forms;
3) A preliminary detailed Project Plan;
4) A Communication Plan;
5) A Training Plan.
6) A Test Plan;
7) A high level Security Plan

8) A high level overview of infrastructure and hosting architecture

9) A high level SLA; and

10) Host City site visits to Vendor/IVS hosted and Voter Contact Centre facilities.

6.2 Phase 2 – Interface, Configuration and Integration Requirements Validation

The main objectives of this Phase are for the Vendor to validate the integration and migration requirements, develop and document the Configuration Requirements for the interoperability and data extraction of adjacent City systems, design and map the integration points, and to provide the configuration and integration plan to the City.

6.2.1 Phase 2: Vendor Responsibilities

In Phase 2 – Interface, Configuration and Integration Requirements Validation, the Vendor will, at a minimum:

1) Work with the City to develop the Configuration Requirements that will be implemented. This will include and account for the interoperability required to access/read/write/update or extract data on adjacent systems within the IVS. This will also include and account for the interoperability required to read/write/update or extract data on TEIS and adjacent systems within the City's infrastructure;

2) Document the details of the Configuration;

3) Work with the City to document and map integration points;

4) Plan and document the migration strategy between the IVS and any of the City's TEIS and adjacent systems, as identified in Phase 2;

5) Have the City to confirm the Configuration and Integration Plan;

6) Identify and validate the Requirements that will be implemented. This will include and account for the interoperability required to access/read/write/update or extract data on adjacent systems within the City's infrastructure;

7) Deliver the Requirements documentation to the City. Documentation must be provided as detailed in section 7.0 - Documentation Requirements;

8) Develop the full Execution Plan for the CEVL service, which includes details on hardware and software requirements;

9) Develop the Integration Plan and Communications Plan for the Voter Contact Centre to the City; and

10) Develop and provide the business process mapping for the Internet and telephone voting service flow, and Election Night results decryption, for the City to validate;

11) Provide a preliminary design mock-up of the web interface that is customized to City image and web design standards;

12) Advise the City on establishing an Electoral Committee, and provide an Election Night Results Decryption procedure; and

13) Present a summary of findings to the City.

6.2.2 Phase 2: City Responsibilities

In Phase 2 – Interface, Configuration and Integration Requirements Validation, the City will:

1) Assist the Vendor in identifying systems which require integration(s);

2) Assist the Vendor in identifying stakeholders for integration requirements gathering;

3) Coordinate with all stakeholders of the Project to facilitate the gathering of information by the Vendor;

4) Assist the Vendor with the creation of the Interface Requirements document;

5) Assist the Vendor to define the Configuration and Integration Requirements;

6) Assist the Vendor in identifying content and data migration requirements;

7) Participate in the development of the Voter Contact Centre deployment plan;

8) Assist the Vendor in the design of the integration of the Voter Contact Centre to the City;

9) Validate the business process mapping for the Internet Voting process and Telephone Voting service flow, and an Election Night Results Decryption Procedure.

10) Approve the Requirements document;

11) Approve the Final Project Plan; and

12) Establish the City's Electoral Committee.

6.2.3 Phase 2: Vendor Deliverables

The minimum required Deliverables for Phase 2 – Interface, Configuration and Integration Requirements Validation, are:

1) An approved Final Project Plan (with an updated schedule based on findings from Phase 2 activities) with a detailed and comprehensive set of validated interface requirements that describe all aspects of how the Vendor's Internet Voting Service will be implemented and its integration points with the City's internal systems;

2) Document detailed and comprehensive set of validated Configuration Requirements and Integration Requirements;

3) Document the detailed, validated integration map;

4) Document the detailed business process map including the Internet Voting process and Telephone Voting Service flow, and Election Night Results Decryption;

5) Confirm the hardware/software configuration required to access City approved CEVL solution at in-person Advance Vote;

6) A validated Content and Data Migration Strategy;

7) A preliminary design mock-up of the web interface; and

8) A Presentation of summary of findings to the City.

6.3 Phase 3 – Customize, Integrate and Test Interface

The main objectives of this Phase are for the Vendor to define the final hardware and software infrastructure, set up the QA, Staging, Public Engagement, Demonstration and Production Environments, as well as design, develop and test all the integration points between the IVS and the City's TEIS and adjacent systems. All voter-facing components must also be AODA and WCAG 2.0 Level AA compliant.

6.3.1 Phase 3: Vendor Responsibilities

In Phase 3 – Customize, Integrate and Test Interface, the Vendor will, at a minimum:

1) Confirm the hardware and software infrastructure, if any, required by the City to support the IVS based on a vendor-hosted COTS implementation model;

2) Conduct, as required, sessions with City staff (stakeholders, business development leads) in order to confirm, document and test the Interface and any Integration points between the Vendor system and City system(s);

3) Update the Interface and Integration design document as required;

4) Create QA, Staging and Production Environments; and,

5) Develop a Go Live Implementation Plan and a Contingency Plan to assist the City Project Team and divisional staff in the implementation of the IVS;

6) Deliver the detailed Security Plan for the IVS including all subcontractor locations and operations:

    a) A detailed description of all primary and support systems including boundary and physical location, components;

    b) A detailed Disaster Recovery Plan;

    c) A detailed internal and external security access model, including a detailed description of identification, authentication, responsibility, expected use of system and expected behaviour of all resources;

    d) A Staging Environment that is suitable for security testing and assessment;

    e) A detailed list of security controls, which can be technical, or operational to ensure the confidentiality, integrity and availability of the services, at a minimum, includes:

        - Personnel Security
        - Physical and Environmental Protection
        - Contingency Planning
        - Configuration Management
        - Maintenance
        - Media Protection
        - Incident Response
        - Security Awareness and Training
        - Logging and Monitoring
        - Systems and Network Protection

7) Develop a Service Level Management process to support the performance, maintenance and delivery of the IVS;

8) Provide the full CEVL Execution Plan;

9) Provide testing scripts, tools and services to ensure the City or a third-party QA Testing Firm may either run or view convincing results of Service Performance tests and UAT to be performed in Phase 4. In addition to functional user testing, this includes, but is not limited to, testing:

a) Turnaround times (including for loading the candidate lists);
b) Security detection and escalation;
c) The interface between the IVS and TEIS to ensure resilience to temporary network outages between the IVS and the City's data centres;
d) Limited bandwidth or congested network connection;
e) Simulation of web users at the upper planned limit, peaked and sustained; and
f) System backup and recovery.

10) Confirm the voter-facing components are AODA and WCAG 2.0 Level AA compliant; and,

11) Customize the user interface to City web design standards, and,

12) Provide a fully functional Public Engagement Service, by the end of Phase 3, which will closely mirror the Production Environment's look and feel and demonstrates the full functionality and accessibility of the IVS. The Public Engagement Service will include both the Internet and Telephone Registration and Voting voter-facing interfaces and will be used by the City for communication, education and outreach purposes;

6.3.2 Phase 3: City Responsibilities

In Phase 3 – Customize, Integrate and Test Interface, the City will:

1) Provide the Vendor with all necessary information for integration of the IVS with existing City systems;

2) Test the system integration;

3) Participate in and validate the IVS customization specifications;

4) Review the hardware requirements and configuration;

5) Review the Implementation Plan and Contingency Plan;

6) Review the Service Level Management process;

7) Review the full CEVL Execution Plan;

8) Review the testing scripts and test results;

9) Review the Security Plan;

10) Review that voter-facing components are AODA and WCAG 2.0 Level AA compliant;

11) Confirm that the user interface is customized to City web design standards; and,

12) Confirm the Public Engagement Service meets the City's public engagement initiatives.

6.3.3 Phase 3: Vendor Deliverables

The minimum required Deliverables for Phase 3 – Customize, Integrate and Test Interface are:

1) A completed and customized Interface that is ready for testing;

2) A Technical Design Document detailing the Interface and Integration components and functionality;

3) A detailed workflow outlining the IVS Customization process, as required;

4) A validated hardware and software architecture document;

5) A customized Internet Voting Service administration guide;

6) Test scripts and/or tools for review by the City and an external third-party QA Testing Firm. This includes, but is not limited to, Disaster Recovery, stress tests; system administration, business user and accessibility testing;

7) An Implementation and Contingency Plan;

8) A Monitoring Plan;

9) A Service Level Management process;

10) A user interface customized to City web standard designs that is AODA and WCAG 2.0 Level AA compliant; and,

11) A Public Engagement Service for communication, education and outreach purposes.

6.4 Phase 4 – Internet Voting Service Configuration, Implementation and User Acceptance Test

The main objectives of this Phase are for the Vendor to prepare and setup the QA, Staging and Production Environments, customize the IVS, migrate content and test the portal, execute User Acceptance Testing (UAT) for the IVS, and provide training and support to designated City staff, the Accessibility Subject Matter Expert and the Auditor, if necessary.

6.4.1 Phase 4: Vendor Responsibilities

In Phase 4 – Internet Voting Service Configuration, Implementation and User Acceptance Test, the Vendor will, at a minimum:

1) Implement the Internet Voting Service, which, at a minimum, includes:

    a) Working closely with dedicated City technical staff during the entire Project to provide skill and knowledge transfer for all aspects of the integration of the IVS with the City’s existing infrastructure, while ensuring the City's business needs are captured and reflected during the installation and integration of the IVS;

    b) A customized City-branded web interface that adheres to City image and web design standards.

2) Perform Data Migration including:

    a) Migrating all data between the IVS and the City's systems from the existing TEIS Voters' List to the Vendor's IVS; and

b) Execute Data Migration Strategy as outlined in Phase 2.

3) Perform Content Migration including:

a) Migrating all content (for example - City Wards, School Board Wards, voting subdivisions, candidates, electoral offices, etc) from the City to the IVS; and

b) Execute the Content Migration Strategy as outlined in Phase 2.

4) Test the IVS, which, at a minimum, includes:

a) Deploying and configuring the IVS in the QA environment to ensure proper Quality Assurance, Integration, Load and Stress Testing prior to the IVS migration to the Staging and Production Environments;

b) Delivering the QA Environment, separate from the Production Environment that will enable the City to test the interface without impacting the IVS Production Environment. The Environment should be preloaded with demonstration data;

c) Within the Staging Environment, completing functional testing of the required business features based on use cases approved by the City in collaboration with the Vendor;

d) Providing a Staging Environment that mirrors the functionality of the Production Environment, on all the same hardware (including high availability systems) to demonstrate all live features (including disaster recovery, encryption mechanisms, ability to handle anticipated voter/data volume, fail-over and intrusion detection);

e) In addition to testing the functionality of the required business features, there must be provision to include a full Security Assessment of the IVS where security findings can be assessed, risk levels assigned and mitigation measures addressed. The Vendor will be prepared to work with a third-party Independent External Auditor engaged by the City;

f) The Vendor will be prepared to work closely with the Auditor and provide full access to ALL elements of the IVS in order for the Auditor to complete, at a minimum, the following evaluations specific to the IVS's functions: Threat Risk Assessment (TRA); Vulnerability Assessment (VA); Penetration Test (PT); Privacy Impact Assessment (PIA); Code Review; and provide:

i. Change control process and accompanying documentation;
ii. Accuracy and completeness of votes cast via the IVS;
iii. End of polling, and decryption and mixing of votes; and
iv. Destruction of the City's Internet Voting data 120 days following the election.

g) The Vendor will be prepared to work closely an external Quality Assurance Testing Vendor engaged by the City in order to independently verify that all elements of the Testing Plan are executed according to the Agreement and ensure all of the Functional, Technical and Non-Functional Requirements and Integration of Interface have been met and that the IVS functions properly;

h) Ensuring that, prior to integration of the proposed IVS, it is thoroughly tested in the QA and Staging Environments to ensure acceptable functionality and performance;

5) User Acceptance Testing of the IVS which at a minimum, includes:

a) Implementing a phased approach for the UAT, of the different modules within the IVS, following the table shown below:

IVS Module	UAT Completed By
Registration	June 30, 2014
Voting	June 30, 2014
Results Reporting	July 15, 2014

Note: The successful integration of each module with existing City systems is an integral part of the UAT process;

b) Ensuring UAT is successfully completed and approved by the City a minimum of two (2) weeks prior to the 'Go Live' date for all the Deliverables and provided in time for the Go/No-Go Live dates:

IVS Module	Go/No-Go Live Date
Registration	July 31, 2014
Voting	July 31, 2014
Results Reporting	August 14, 2014
Integration of all IVS Modules	August 14, 2014

c) Providing a documented process and timeline for addressing deficiencies identified in UAT;

d) Fixing any deficiencies and receiving approval from the City before the IVS is moved from the QA Environment to the Staging Environment, and from the Staging Environment(s) to the Production Environment. See SCHEDULE "F" for details on the UAT acceptance procedure;

e) Providing on-site training to City staff, if necessary, which, at a minimum, includes:

i. Developing and providing training and education materials on the use of the IVS;
ii. Developing and executing the "Election Official" training plan provided in response to Requirements;
iii. Developing and executing the "System Administrator" training plan provided in response to Requirements; and,
iv. Providing all training manuals, system manuals, testing scripts and results for the City's review, and once approved, for the City's use.

6) Providing a Risk Management Plan, including mitigation strategy, to ensure a viable, robust IVS for the critical election timeline;

7) Providing on-site and remote support during integration and implementation of the IVS in the Production Environment which, at a minimum, includes technical support for City staff and a Technical Contact Centre as detailed in SCHEDULE "J".

8) Accessibility User Acceptance Testing of the IVS for WCAG 2.0 Level AA conformance, as detailed in the Requirements. During Accessibility UAT of the IVS, the Vendor will:

   a) Provide basic training to the City's Accessibility Subject Matter Expert and team in charge of overseeing the accessibility compliance;

   b) Provide details of the accessibility QA activities executed by the Vendor and the results obtained; and

   c) Perform necessary customization of the software with respect to feedback received during Accessibility testing;

9) Providing a fully functional Demonstration Service, prior to the end of Phase 4 (Implementation), which mirrors the Production Service and demonstrates the full functionality and accessibility of the IVS (Internet and IVR registration and voting and the CEVL);

10) Participating in the City's July 28 and October 6, 2014 Mock Election Results reporting Tests. In preparation for the Results Test(s), the Vendor will, at a minimum:

   a) Configure the results test event using content and expected results outcomes provided by the City;

   b) Monitor the IVS during the results reporting tests;

   c) Execute the mixing and tallying process to obtain IVS election results, for integration with TEIS, after the close of polls;

d) Provide the IVS's tabulated results according to the City's and Election Systems & Software's (the City's Vendor of Record for Vote Tabulation equipment and software) interface requirements;

e) Provide agreed-upon statistics of the Results reporting Test(s);

f) Following the test(s), ensure all data is cleared from the test environment(s); and

g) Perform necessary customization of the software with respect to feedback during the test(s).

11) Provide documented details of the QA testing activities executed; and

12) Provide a Staging Environment IVS to the Independent External Auditor, engaged by the City, for full pre-election audit. During the pre-election audit, the Vendor will assist the City as required with the audit scope definition.

6.4.2 Phase 4: City Responsibilities

In Phase 4 – IVS Configuration, Implementation and User Acceptance Test, the City will:

1) Establish the City Testing Team that will be involved in the acceptance activities;

2) Engage the services of a qualified Independent External Auditor with experience providing auditing and testing services, and other security-related services such as Privacy Impact Assessments, Threat Risk Assessments, Vulnerability Assessments and Penetration Test of the Internet Voting Solution. On the city's behalf, the Auditor will review the proposed IVS, system, policies, process, procedures, operations and environments for the information systems and data storage.

3) Receive skill and knowledge transfer for all aspects of the integration of the IVS with the City's existing infrastructure;

4) Review the Demonstration Service WCAG 2.0 Level AA compliancy and if it functions to the agreed-upon specifications and meeting all Requirements from Phase 2 Deliverables;

5) Review the Production Environment WCAG 2.0 Level AA compliancy and if it functions to the agreed-upon specifications and meets all Requirements from Phase 2 Deliverables;

6) Review that the final UAT covers all the functionality required; and

7) Confirm that there are no open issues, and provide sign-off on the Notice of Final Acceptance of the IVS.

6.4.3 Phase 4: Vendor Deliverables

The minimum Deliverables for Phase 4 – IVS Configuration, Implementation and User Acceptance Test are:

1) QA and Staging Environments;

2) Production Environment;

3) Initial Data Migration completion;

4) Initial Content Migration completion;

5) Complete IVS Testing;

6) Risk Management Plan;

7) Documented process and timeline for addressing deficiencies identified in the UAT;

8) Fixing any identified deficiencies until no defects are identified, or until otherwise directed by the City;

9) A “Back-out” or “Restore” Plan;

10) A Technical Support Call Centre;

11) A fully functional Demonstration Service;

12) A fully functional Public Engagement Service;

13) A fully functional Staging Environment for auditing; and

14) Documentation (hard and soft copies), including but not limited to:

    a) A user manual;
    b) A quick reference information sheet (for outreach purposes);
    c) A System Administrator manual;
    d) A detailed Operation and Maintenance procedure;
    e) System and technical specifications for all customizations, interfaces, processes, data models and information flows;
    f) System configuration specifications, procedures and functions;
    g) Hardware and software setup (including performance tips, backup and recovery; security routines); and

h) Source code and supporting documentation for any customized components.

6.5 Phase 5 – Demonstration and Final Acceptance

Phase 5 - Final Acceptance will commence upon the successful implementation and operation of the Internet Voting Service in the Production Environment. Upon the completion of the Final Acceptance period, and delivery of documentation objects described within all phases of Section 6 the City shall issue a Notice of Final Acceptance.

6.5.1 Phase 5: Vendor Responsibilities

In Phase 5 – Demonstration and Final Acceptance, the Vendor will, at a minimum:

1) Acquire sign-off from the City on the Notice of Final Acceptance of the IVS in time for the Go/No-Go Live dates;

2) Provide the City with all hardware, software and components that will be required on Election Night for the mixing and tallying of votes in an isolated environment (including a duplicate, redundant system for contingency). This must be provided on an air-gap unit in a ready-state;

3) Continue running and supporting the Public Engagement and Demonstration Services until the mutually-agreed upon date and time at which the Services will be shut down;

4) Shut down the Public Engagement and Demonstration Services at the mutually agreed-upon date and time with the City;

6.5.2 Phase 5: City Responsibilities

In Phase 5 – Demonstration and Final Acceptance, the City will:

1) Confirm that the Demonstration Service is WCAG 2.0 Level AA compliant and works to the agreed-upon specifications and meeting all Technical, Functional and Non-Functional Requirements from Phase 2 Deliverables;

2) Confirm that the Production Environment is WCAG 2.0 Level AA compliant, works to the agreed-upon specification and meets all Technical, Functional and Non-Functional Requirements from Phase 2 Deliverables;

3) Confirm that the final UAT covers all the functionality required; and

4) Confirm that there are no open issues, provide sign-off on the Notice of Final Acceptance of the IVS;

5) Determine a date and time for the shut-down of the Demonstration Service, with the Vendor; and

6) Utilize the Demonstration Service for accessibility testing;

7) Utilize the Public Engagement Service for communication, education and outreach purposes.

6.5.3 Phase 5: Vendor Deliverables

The minimum Deliverables for Phase 5 – Final Acceptance are:

1) An IVS that is free from deficiencies and which works to the agreed-upon specifications and meeting all Requirements from Phase 2 deliverables;

2) All hardware and software required on Election Night, in a ready state;

3) Confirm shut down of the Public Engagement and Demonstration Services.

6.6 Phase 6 – Go Live – Registration and Voting

The main objective of this phase is to deploy the solution in the Production Environment and for the Vendor to provide support throughout the Registration and Voting period.

6.6.1 Phase 6: Vendor Responsibilities

In Phase 6 – Go Live –Registration and Voting, the Vendor will, at a minimum:

1) Ensure all Phase 6 activities, which include all tasks pertaining to the launching of the IVS across all levels, are complete. This also includes monitoring the deployment to ensure the rollout is secure, efficient and effective;

2) Deploy the trusted environment into the Production environment, full functionality of the IVS, including but not limited to the processing of voter registrations and delivering PINs via the Voter Contact Centre, beginning September 8, 2014, which can process and send registration information securely and directly to voters in their preferred method (e.g. mail, email, SMS or via a telephone call to the voter);

3) Provide a single point of contact on-site and available during normal Business Hours during the full Registration and Voting periods;

4) Provide the City with support during the Availability Management times outlined in SCHEDULE "J";

5) Validate the isolated mixing and tallying server hardware, software and components (including a duplicate, redundant system for contingency);

6) Validate that the digital ballot box is empty, providing a “zero-tally report”;

7) At a minimum, digitally sign all code and configuration files and election related information, in coordination with the Independent External Auditor;

8) Deploy the monitoring plan and application, providing the City with access to view the monitoring application;

9) Provide daily status reports on the usage and performance of the IVS, as pre-defined by the City;

10) Assist the Independent External Auditor as needed; and

11) Apply mitigation activities identified by the Auditor or the City.

6.6.2 Phase 6: City Responsibilities

In Phase 6 – Go Live Registration and Voting, the City will:

1) Review, approve or decline voter registrations using the IVS; and

2) Review the daily performance reports and system usage statistics status reports from the Vendor.

6.6.3 Phase 6: Vendor Deliverables

The minimum required Deliverables for **Phase 6 – Go Live –Registration and Voting** are:

1) A single point of contact on-site at the specified City site and available during normal Hours defined in SCHEDULE “J” during the full Registration and Voting periods;

2) Deploy the Staging and Production Environments;

3) A Zero-Tally report;

4) A technical support call centre and Voter Contact Centre, as outlined in SCHEDULE "J";

5) Daily end user support reports for all incidents, inquiries and work requests;

6) Data and custom reporting services, including consultation, scoping, project management, formatting, testing and implementation of data uploads or extractions, as well as custom reports, as required;

7) Full documentation such as support requests, service tickets etc.;

8) Monitor the IVS performance using the monitoring application and provide daily performance reports and system usage statistics;

9) Perform mixing and tallying of the IVS votes and provide the City with the encrypted results after the close of polls on Election Day (8:00 PM EST, October 27, 2014);

10) Communications, Documentation and impact assessments related to system maintenance periods, planned down-times, and product upgrades as required; and

11) System administration.

6.6.4 Phase 7 – Project Closure

The objective of this phase is to formally close the Internet and Telephone Voting Project for the 2014 Municipal Election. All IVS configuration data, software or hardware related to the production of results, and any data collected in the provisioning of the IVS, including collected data, activity logs and records must be stored in a secure, encrypted format, and destroyed or returned to the City, after 120 days period, as required by *MEA* section 88, with proof of record destruction, in an agreed-upon format.

6.6.5 Phase 7: Vendor Responsibilities

In Phase 7 – Project Closure, the Vendor will, at a minimum:

1) Provide the Independent External Auditor with full access to the Production environment, following the declaration of final results, and assist the Auditor when required in the post-election audit process;

2) Prepare a Lessons Learned document about the project, which should include the following, at a minimum:

    a) Key Challenges;

b) Actions Taken to Overcome Challenges;
c) What worked well;
d) What did not work well or what would we do differently next time; and
e) A list of recommendations;

3) Store all IVS configuration data, software or hardware related to the production of results, collected data, activity logs and records must be stored in a secure, encrypted format, for 120 days following the declaration of final results as required by Section 88(1) of the *MEA*, and, after the 120-day period, when directed by the City, destroy and/or return all data to the City, with proof of record destruction, in an agreed-upon format.

    a) If a recount is required, the Vendor will, at the direction of the City:

        i. Validate the immutable logs, checking that ballots logged match the ones in the database;
        ii. Perform additional mixing/and tallying processes;
        iii. Provide recount results to the City;
        iv. Securely store and encrypt all above-mentioned election results and configuration data until directed by the City; and
        v. Repeat this process as directed by the City, until all challenges for a recount are resolved;

4) Prepare Certificates of Destruction (COD) for all media which carries City data; and

5) Participate in Project Closure meeting with the City's Project Team.

6.6.6 Phase 7: City Responsibilities

In Phase 7 – Project Closure, the City will:

1) Coordinate the post-election audit by the Independent External Auditor;

2) Communicate the formal audit results to the public and media;

3) Store results generating hardware and software in a secure facility;

4) Participate in the Project Closure meeting;

5) Advise the Vendor if a recount is required;

6) Direct the Vendor to destroy or return all data to the City, no earlier than 120 days following the declaration of final results;

7) Review and validate all Certificates of Destruction (COD);

6.6.7 Phase 7: Vendor Deliverables

The minimum required Deliverables for **Phase 7 – Project Closure** are:

1) Store all IVS data and Election data in a secure, encrypted format;

2) Upon direction from the City, destroy or return all data to the City, no earlier than 120 days following the declaration of final results;

3) Certificates of Destruction (COD) for all media which carry City data;

4) Recount analysis report, if applicable; and

5) Documented Lessons learned from the project;

7.0 Documentation Requirements

The following statements represent Mandatory Documentation Requirements that will only come into effect for the Vendor.

1) The Vendor must provide all documentation as outlined in the Deliverables of each phase of the Project. Vocabulary should be reasonably consistent throughout the manuals;

2) All documentation must be provided by the Vendor in both printed and electronic format. The format of any electronic documentation must be supported by the IVS and the City's authoring tools. Such documentation must be current, complete and accurate;

3) Documentation provided by the Vendor should include all application/system configuration specifications, procedures and functions in reasonable detail, including screen and report layouts.

8.0 Requirements

The Vendor should provide an IVS that addresses the Requirements in accordance with Vendor's response to such requirements in SCHEDULE "H" and "I".

9.0 Maintenance and Support

1) The Vendor should provide an IVS that addresses the Service Support Terms in SCHEDULE "N".

2) Upon execution of the Agreement, the Vendor will enter into a Service Level Agreement (SLA) with the City to support the mutually agreed-upon terms and conditions of the Vendor's support and maintenance of the IVS during the implementation and production of the IVS, as detailed in SCHEDULE "N" of this Agreement.

3) In each case, so as to minimize interruption to the City's ongoing business processes, with time being of the essence, and to be done at the Vendor's sole expense, the Vendor must represent and warrant that any restoration, repair or replacement made will not corrupt any data of the City or introduce any viruses into any of the City's systems.

4) The Vendor must provide the City with the maintenance and support (Levels 1, 2 and 3 Support) and regular management reports needed for the smooth functioning of the IVS during the implementation and entire Go Live and Project Closure phases of the IVS as shown in the following chart:

Level	Level Description
Level 1 Support	“Level 1 Support” means the support that is provided by the Vendor to address issues relating to the use of the IVS. The issue is captured in an issue tracking repository in order to properly manage from intake to resolution. An evaluation process is executed to determine the nature and severity of the issue. The issue will be resolved by Level 1 Support or escalated to Level 2 Support. Level 1 Support is required to be staffed during Business Hours.
Level 2 Support	“Level 2 Support” means the support that is provided by the Vendor to address issues that are not resolvable by Level 1 and cause reduced function of the IVS and business units. Level 2 Support is required to be staffed to support business operations beyond Level 1 when necessary for completion of the issue. Issues that cannot be resolved by Level 2 Support will be escalated to Level 3 Support. Level 2 Support is required to be staffed during Business Hours.
Level 3 Support	“Level 3 Support” means the support that is provided by the Vendor to address catastrophic conditions related to the IVS. These issues could be related, but not limited to, the application, underlying data engine or operating system errors. Issues of this nature require immediate expert attention from the Vendor. Due to the nature of the issue and its impact on business function and operation, Level 3 support is required 24 hours per day, 7 days per week throughout the Internet Voting Project for the 2014 Municipal Election.

5) The Vendor must document, notify and fix any deficiencies identified in the Production Environment and provide notification as needed. The following table describes how deficiencies of various severity levels will be addressed:

Deficiency Severity	Severity Description	Impact
Major	Privacy breach or discovery of a security vulnerability that could result in a privacy breach.	• Remove Production system access immediately. • Inform the City's designated business contacts by email and phone within 15 minutes of discovery of the breach. • Identify the root cause. • Propose possible mitigation solutions that will not jeopardize the integrity, security and privacy of the IVS, and the time required to implement. • The Vendor will inform the City on resolution and test fix. • Document the root cause and fix within 12 hours of resolution. • Provide a media relations spokesperson to support the City in addressing any media inquiries.
Major	Disastrous, severe or significant consequences for the IVS with no immediate workaround. Current implementation risks data integrity or limits client access to the IVS or its contents.	• Remove Production system access immediately. • Inform the City's designated business contacts by email and phone within 30 minutes of the discovery of the deficiency. • The Vendor will provide a point of contact to initiate a service request that will have an escalation process to address the severity. • Identify the root cause. • Propose possible mitigation solutions that will not jeopardize the integrity, security and privacy of the IVS. • The Vendor will inform the City on resolution and tested fix. • Document the root cause and fix within 12 hours of resolution. • Provide a media relations spokesperson to support the City in addressing any media inquiries.

Deficiency Severity	Severity Description	Impact
Minor	Small or negligible consequences for the IVS. Simple workarounds typically exist.	• Inform the City's designated business contacts by email and phone immediately upon discovery of the deficiency. • The Vendor will provide a point of contact to initiate a service request that will have an escalation process to address the severity. • The Vendor will respond to the City contact within two (2) business days. • Identify and document the root cause. • Propose possible mitigation solutions. • Obtain sign-off from the City on resolution and tested fix. • Document fix.
Cosmetic	Trivial defects that cause no negative consequences for the IVS. Typically related to appearance as opposed to function.	• Inform the City's designated business contacts by email and phone upon discovery of the deficiency. • The Vendor will provide a point of contact to initiate a service request that will have an Escalation Process to address the severity. • The Vendor will respond to the City contact within three (3) Business Days. • Identify and document the root cause. • Propose possible mitigation solutions. • Obtain sign-off from the City on resolution and tested fix. • Implement change in next release unless otherwise agreed. • Document fix.

ATTACHMENT 1

TO THE STATEMENT OF WORK FOR RFP 3405-13-3197

PAYMENT SCHEDULE

Payment Authorization

1) The Vendor's Project Manager will deliver a SCHEDULE C-1, Deliverable Acceptance Request Form, when the Deliverables for that Payment Milestone have been completed. The City will have a maximum of five (5) Business Days to verify that the Payment Milestone acceptance criteria have been met and to provide a Notice of Acceptance or rejection of the Deliverable Request Form to the Vendor.

2) If the City rejects the Payment Milestone, then the Vendor will take corrective actions before resubmitting a new Deliverable Acceptance Request Form to the City and again seeking acceptance of the completion of a Payment Milestone within a new five (5) Business Day period.

3) The required verification reviews and acceptances will be coordinated by the City Project Manager. Upon the issuance of a SCHEDULE C – Notice of Acceptance of Deliverable Form, the Vendor is entitled to issue the invoice for same.

4) When submitting an invoice, the relevant purchase order or blanket contract number, City Project Manager's name and location, along with the approved Deliverables/milestones being billed and any separate document evidencing approval by the City of such Deliverables will be attached to such invoice.

5) Payment of such invoices will be net sixty (60) days from receipt of the invoice.

6) Payment shall be made in accordance with the payment schedule set out below:

Note: A Notice of Acceptance is required prior to the issuance of an invoice. The parties cannot proceed to the next phase of Implementation until the Notice of Acceptance has been received for the preceding phase.

Table 1: Payment Schedule for the Project s. 10 applied s. 11 applied

ITEM NO	PAYMENT MILESTONES (DELIVERABLES)	PAYMENT
1.	Phase 1 – Project Initiation (0%) – Begins April 1, 2014	
(a)	Phase 1 – Complete by April 14, 2014	[redacted]
2.	Phase 2 – Configuration and Integration Requirements Validation (0%) – April 15, 2014	
(a)	Validated configuration and integration requirements document	[redacted]
(b)	Final Project Plan complete – April 30, 2014	
3.	Phase 3 – Customize, Integrate and Test IVS (20%) – Begins by May 1, 2014	
(a)	Technical design, integration components and functionality documentations	[redacted]
(b)	Customized interface ready for testing – Complete by May 20, 2014	
4.	Phase 4 – IVS Configuration, Implementation and Test (20%) – Begins by May 21, 2014	
(a)	Customization of the IVS complete	[redacted]
(b)	Data Migration complete	
(c)	User Acceptance Test complete and passed	
(d)	Go/No-go decision (if Go) – Complete by August 11, 2014	
5.	Phase 5 – Final Acceptance (20%) – Begins by August 12, 2014	
(a)	Phase 5 – complete on or before August 15, 2014	[redacted]
6.	Phase 6 – Go Live – Registration and Voting (30%) – Begins by August 16, 2014	
(a)	Phase 6 – Complete by October 28, 2014	[redacted]
7.	Phase 7 – Project Closure (10%) – Begins October 29, 2014	
(a)	Phase 7 – Complete by February 25, 2015	[redacted]
	TOTAL	[redacted]

ATTACHMENT 2

TO THE STATEMENT OF WORK FOR RFP 3405-13-3066

TRAINING SCHEDULE

s. 11 applied s. 10 applied

Line	Training Course	Duration (days)	Number of Students	Cost per Student	Extended Cost
1	"Election Official" Training	4	30	[redacted]	[redacted]
2	System Administrator Training	1	5	[redacted]	[redacted]
3	Technical Training	1	10	[redacted]	[redacted]
4	Additional Costs				[redacted]
5	One hundred (100) hours of post-training support (Specify Hourly Rate): [redacted]				[redacted]
6				**Total:**	[redacted]

Module	Content	Tailored for	Length (Days)	No. of Students	Location
Scytl Voter Registration	Course 1: Voter Registration System Introduction	Election Officials	0.5	30	COT
Scytl Voter Registration – Back Office	Course 2: Voter Registration System Management	Election Officials	1	30	COT
Scytl Online Voting	Course 3: Internet Voting System Introduction	Election Officials	0.5	30	COT
Scytl Online Voting – Back Office	Course 4: Internet Voting System Management	Election Officials	1	5	COT
Scytl Back Office	Course 5: Advanced Internet Voting System Security Concepts	COT Technical Staff	1	10	COT
DataFix Municipal Voter View	Course 6: Voters' List Management Introduction	Election Officials	0.5	30	COT
DataFix Municipal Voter View	Course 7: Voters' List Management System Management	Election Officials	0.5	30	COT

SCHEDULE "B"
LIST OF BASE SOFTWARE AND BASE SOFTWARE PRICING

This section contains Itemized pricing for additional modules available from Scytl Canada, Inc. The quoted prices will remain valid for the duration of this contract.

Table 1: Scytl Products and Services s. 10 applied s. 11 applied

Line Item	Item	Unit	Unit Cost
Internet Voting Service			
1	Service for Full Implementation	1	[redacted]
2	Scytl Online Voting (Single Use License)	1	[redacted]
3	Scytl Voter Registration (Single Use License)	1	[redacted]
4	Scytl Voter List Management (Single Use License)	1	[redacted]
5	Software licenses for Full Implementation	1	[redacted]
7	Voter Notification Letter Step 1 (Single)	1	[redacted]
8	Voter Notification Letters Step 1 (Batch)	1	[redacted]
9	Voter Notification Letter Step 2 (Single)	1	[redacted]
10	Voter Notification Letters Step 2 (Batch)	1	[redacted]
11	Voter Contact Centre (Over 37,500 minutes)	1	[redacted]
12	Voter Contact Centre (Up to 37,500 minutes)	1	[redacted]
13	Voter Contact Centre (37,500 minutes)	1	[redacted]
Additional Products and Services			
15	Social Media Monitoring	1	[redacted]
16	SMS Voter Notifications Delivery	1	[redacted]
17	Braille Letters	1	[redacted]
18	DataFix Voters' List Management Solution	1	[redacted]
19	Telephone Voting	1	$18,694.63

Table 2: Scytl Products and Services s. 10 applied s. 11 applied

	Category	Unit Cost
Internet Voting Service		
1	Service for Full Implementation	[redacted]
2	Software licenses for Full Implementation	[redacted]
3	Software Support and Maintenance	[redacted]
4	Training	[redacted]
	[redacted]	[redacted]
	Subtotal	[redacted]
Other Costs		
1	Customization Support and Maintenance	
	- Technical Support	[redacted]
2	Voter Notification Letters (Step 1)	[redacted]
3	Voter Notification Letters (Step 2)	[redacted]
4	Voter Contact Centre (7,500 voters; 37,500 minutes)	[redacted]
	Subtotal	[redacted]
Additional Products and Services		
1	Telephone Voting	[redacted]
2	Social Media Monitoring	[redacted]
3	SMS Voter Notifications Delivery	[redacted]
4	Braille Letters	[redacted]
5	DataFix Voter List Management Solution	[redacted]
	Subtotal	[redacted]
	Total (exclusive of taxes)	[redacted]

SCHEDULE "C"

SCHEDULE OF FORMS

SCHEDULE C-1 - Deliverable Acceptance Request Form
SCHEDULE C-2 - Deliverable Acceptance Approval Form
SCHEDULE C-3 - Progress Payment Milestone Request Form
SCHEDULE C-4 - Progress Payment Milestone Approval Form
SCHEDULE C-5 - Final Notice of Acceptance Request Form
SCHEDULE C-6 - Final Notice of Acceptance Approval Form

TORONTO

C-1 - Deliverable Acceptance Request Form

Project Management Office

Project Name:	Internet Voting for the 2014 Municipal Election		
City Project Manager:	Jerry Liu	City Telephone:	416-392-0486
Vendor Project Manager:	Richard Catahan	Scytl Canada Telephone:	289-795-3252
Project Sponsor:		Planned Due Date:	
Phase ID & Name:		Submission Date:	
Deliverable:			

Deliverable Acceptance Request
Deliverable:
<<Description of the Deliverable as per Statement of Work >>
Acceptance Criteria:
<<Description of the Deliverable Acceptance Criteria>>

Means of Verification:
<<Description of the process taken for the completion of the Deliverable>>
Dependencies:
<<List Working Documents received as input to this Deliverable. List all Deliverables for which this Deliverable is a prerequisite.>>
Risk/Issues:
<<Description of the risks and justifications associated with any delays in City approval>>

Deliverable Acceptance Prepared By:			
Name	Project Role	Signature	Date

TORONTO

C-2 - Deliverable Acceptance Approval Form

Project Management Office

Project Name:	Internet Voting Service Implementation for the 2014 Municipal Election		
City Project Manager:	Jerry Liu	City Project Manager:	Jerry Liu
Vendor Project Manager:	Richard Catahan	Vendor Project Manager:	Richard Catahan
Project Sponsor:		Planned Due Date:	
Phase ID & Name:		Submission Date:	
Deliverable:			

Deliverable Reviewed
The above referenced Deliverable has been reviewed. Based on the defined acceptance criteria, the Deliverable is: Accepted ☐ Rejected ☐
Review Process:
<<Description of City review process>>
Detailed reasons , if rejected:
<<Description of deficiencies, errors>>

Deliverable Accepted / Rejected By:			
Name	Project Role	Signature	Date

Deliverable Approval Signatures:			
Name	Project Role	Signature	Date

TORONTO

C-3 - Progress Payment Milestone Request Form

Project Management Office

Project Name:	Internet Voting Service Implementation for the 2014 Municipal Election		
City Project Manager:	Jerry Liu	City Project Manager:	Jerry Liu
Vendor Project Manager:	Richard Catahan	Vendor Project Manager:	Richard Catahan
Project Sponsor:		Project Sponsor:	
Phase ID & Name:		Phase ID & Name:	
Milestone:			

Progress Payment Milestone Request
Milestones:
<<List Deliverable Milestones required to complete this Progress Payment Milestone as per Payment Schedule>>

Progress Payment Milestone Request Prepared By:			
Name	Project Role	Signature	Date

TORONTO

C-4 - Progress Payment Milestone Approval Form

Project Management Office

Project Name:	Internet Voting Service Implementation for the 2014 Municipal Election		
City Project Manager:	Jerry Liu	City Project Manager:	Jerry Liu
Vendor Project Manager:	Richard Catahan	Vendor Project Manager:	Richard Catahan
Project Sponsor:		Project Sponsor:	
Phase ID & Name:		Phase ID & Name:	
Milestone:			

Milestone Reviewed
The above referenced Milestones have been reviewed. Based on the defined acceptance criteria, the Milestone is: Accepted ☐ Rejected ☐
Review Process:
<<Description of City review process>>
Detailed reasons, if rejected:
<<Description of deficiencies, errors>>

Milestone Accepted / Rejected By:			
Name	Project Role	Signature	Date

Milestone Approval Signatures:			
Name	Project Role	Signature	Date

TORONTO

C-5 - Final Notice of Acceptance Request Form

Project Management Office

Project Name:	Internet Voting Service Implementation for the 2014 Municipal Election		
City Project Manager:	Jerry Liu	City Project Manager:	Jerry Liu
Vendor Project Manager:	Richard Catahan	Vendor Project Manager:	Richard Catahan
Project Sponsor:		Project Sponsor:	
Phase ID & Name:		Phase ID & Name:	

Final Notice of Acceptance Request Prepared By:			
Name	Project Role	Signature	Date

TORONTO

C-6 - Final Notice of Acceptance Approval Form

Project Management Office

Project Name:	Internet Voting Service Implementation for the 2014 Municipal Election		
City Project Manager:	Jerry Liu	City Project Manager:	Jerry Liu
Vendor Project Manager:	Richard Catahan	Vendor Project Manager:	Richard Catahan
Project Sponsor:		Project Sponsor:	
Phase ID & Name:		Phase ID & Name:	

Final Acceptance Reviewed
Your request for Final Acceptance has been reviewed. Based on the defined acceptance criteria, the Final Acceptance is: Accepted ☐ Rejected ☐
Review Process:
<<Description of City review process>>
Detailed reasons , if rejected:
<<Description of deficiencies, errors>>

Final Acceptance - Accepted / Rejected By:			
Name	Project Role	Signature	Date

Final Acceptance - Approval Signatures:			
Name	Project Role	Signature	Date

SCHEDULE "D"

CHANGE ORDER FORM

Change Request Identification			
Change Request Name	[enter brief name for this project change request]	**Change Request ID #**	[1]
Date Change Request Submitted	yyyy/mm/dd	**Priority** (**L**ow/**M**oderate/**H**igh/**C**ritical)	[L]
Date Last Updated	yyyy/mm/dd	**Impact** (**L**ow/**M**oderate/**H**igh)	[L]

Description & Rationale
Prepared by the person requesting the change. Brief description of the change. Why is this change needed (specific numbers if possible)? What will be the impact if the change is not implemented?

Assessment

Prepared by the project team. List the project areas/tasks that will be affected by the change, the resulting benefit, as well as the impact on the schedule and budget.

Areas Affected	Benefits	Schedule Impact	Budget Impact

Recommendations
Describe the options that have been considered. Explain pros and cons of various implementation strategies. Make a recommendation as to how this change could be implemented.

Acceptance & Sign-Off			
Identify the decision making body that will approve/reject this change.			
☐ **Approved as Requested**	☐ **Approved with Changes**	☐ Rejected	
Prepared By:			
	Name & Title	***Signature***	***Date***
Approved By:			
	Name & Title	***Signature***	***Date***
Approved By:			
	Name & Title	***Signature***	***Date***

Comments

SCHEDULE "E"

HOURLY RATES

s. 10 applied

Line	Description	Hourly Rate (8-40 hours)	Hourly Rate (41-120 hours)	Hourly Rate (121-240 hours)
1	Data Conversion Assistance	[redacted]	[redacted]	[redacted]
2	Custom (Solution) Development	[redacted]	[redacted]	[redacted]
3	Custom Report Writing	[redacted]	[redacted]	[redacted]
4	Database Administration Database administration Database Scripting	[redacted]	[redacted]	[redacted]

SCHEDULE "F"

TESTING: QUALITY ASSURANCE PLAN/QUALITY ASSURANCE DETAILS

Quality Assurance Details (QA)

(1) The Vendor will complete and present the Quality Assurance Plan/Quality Assurance Details (QA) to the City Project Manager, within two weeks of the commencement of Phase 4 – Internet Voting Service Configuration, Implementation and User Acceptance Test. Following the approval of the initial Quality Assurance Plan by the Internet Voting Service Core Team, the City Project Manager will have the authority to approve changes to the Quality Assurance Plan as the Project proceeds unless, in the City Project Manager's sole opinion, the approval of the Internet Voting Service Core Team is required.

(2) The Quality Assurance Plan /Quality Assurance Details (QA) are first developed as a Phase 4 Deliverable by the Vendor and will be updated throughout the Phase. The Quality Assurance Plan /Quality Assurance Details (QA) will provide all Project resources with a clear understanding of the activities and tasks that they are responsible for performing to ensure completion of the Project.

(3) A high level Quality Assurance Plan /Quality Assurance Details (QA) is provided below. Additional information will be provided within two weeks of the Effective Date.

(4) City uses HP Quality Centre to manage requirements, test cases, defect tracking and performance testing.

High Level Quality Assurance Details (QA)

Testing:

Testing of the Solution should take place on the QA and Staging Environment(s) before changes are promoted to the Production Environment.

Testing takes place at different phases of development:

(1) Unit testing is completed by each developer as they are developing their portion of the application.
(2) "First-run" testing is completed by the tester after the application is merged on the QA Environment.
(3) Regression testing is completed by the tester when fixes have been applied to the merged application.
(4) Integration testing is completed by the tester when all integrations are completed. This is the final test phase, where the IVS is fully tested including any integration points.

(5) Performance testing is completed to ensure that the IVS is capable of meeting the performance requirements stated within the RFP.

Test Plan:

1) The Vendor will prepare an overall Test Plan and schedule.

Test Cases:

2) The Vendor will complete a base set of test cases for review by the City. These test cases will ensure the proper functionality of the base IVS.
3) Vendor will work with City Personnel and an External Testing Vendor engaged by the City to develop additional test cases, which will test IVS specific functionality.

User Acceptance Testing (UAT)

During User Acceptance Testing, the Vendor shall:

a) Provide documented process and timeline for addressing deficiencies identified in UAT;

b) Fix any deficiencies and receiving approval from the City before the IVS is moved from the QA Environment to the Staging Environment and from the Staging Environment to the Production Environment.

c) Ensure that prior to implementation of the IVS with the City's infrastructure, the IVS is thoroughly tested in the UAT environment to ensure proper functionality and acceptable performance;

d) Provide test scenario, cases and scripts for review and approval by the City prior to performing IVS testing;

e) Test the IVS, with the participation of City technical staff, the External Testing Vendor, the external Accessibility testers and the Independent External Auditor, to ensure all of the Functional, Technical and Non-functional Requirements have been met and that the Solution is functioning properly;

f) Provide testing criteria for user acceptance testing (UAT) by the City, the Independent External Auditor and Accessibility testers;

g) Provide training to City staff, Independent External Auditor and the Accessibility testers on how to perform UAT;

h) Provide a minimum of two (2) weeks for the City to perform UAT; and

i) Fix any deficiencies and receiving approval from the City before the IVS is moved from the QA and Staging Environments to the Production

Environment. The following table describes how deficiencies of various severity levels will impact the UAT process:

Deficiency Severity	Severity Description	Impact on UAT
Major	Disastrous, severe or significant consequences for the Service with no immediate workaround. Testing functions cannot be fully completed.	UAT period for that module restarts from zero once the deficiency has been fixed.
Minor	Small or negligible consequences for the Service. Simple workarounds typically exist.	UAT period for that module halted mid-stream while deficiency is fixed. Upon fix, UAT period for that module will recommence.
Cosmetic	Trivial defects that cause no negative consequences for the Service. Typically related to appearance as opposed to function.	UAT period for that module halted mid-stream while deficiency is fixed. Upon fix, UAT period for that module will recommence.

i. If the Vendor is unable to correct any major or minor failure(s) within the UAT period(s), or if more than three (3) failures of the same type (excluding cosmetic) occur within the UAT period, the City may deem the Service to be a total failure and at its option may terminate the UAT period and terminate the Agreement.

ii. In such event, the Solution shall be returned to the Vendor and the Vendor shall forthwith repay to the City all payments it has received pursuant to the Agreement (plus interest commencing on the day of the termination at a rate of prime plus 2 percent per annum).

iii. Conversely, if the Vendor does correct any error(s) or failure(s) and if more than three (3) failures of the same type do not occur within the UAT period, or in the event that the City elects not to exercise its right of termination, then the Vendor shall be entitled to receive a notice of waiver of the termination rights from the City in respect of such UAT period testing and the Project will proceed to the next Project phase.

SCHEDULE "G"
TRAINING

Refers to Attachment 2 of SCHEDULE A-1.

SCHEDULE "H"
REQUIREMENTS

Req. No.	Requirement
1.1	The IVS must be accessible to Persons with Disabilities including voters, Independent External Auditors, Election Officials and City staff. In the case of websites and web content, all such content must conform to the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA as required by the AODA Information and Communication Standards. For more information about the City's accessibility requirements, see: http://www.toronto.ca/elections/accessibility For more information on the AODA Information and Communication Standards, see: http://www.mcss.gov.on.ca/en/mcss/programs/accessibility/info_comm/index.aspx
1.2	The Vendor must indicate their support for the City to conduct an Independent Review of the Operation of the IVS. The City intends to engage an External Technology Auditor to perform an independent review of the operation of the IVS before, during and after the conclusion of the election.
1.3	The IVS must be usable with common Assistive Technology software such as screen readers (e.g. JAWS, NVDA, Voice-Over), screen magnification software (e.g. ZoomText), voice dictation software (e.g. Dragon Naturally Speaking) and on-screen keyboards.
1.4	The IVS must be usable with common Assistive Technology hardware devices such as alternative keyboards, joysticks, touch screens, etc.
1.5	All course and training material associated with the Deliverables must meet accessibility requirements as outlined in the Ontario Human Rights Code. In the case of training websites and web content, all such content must conform to the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA. Note: Any instructional video material must include a soundtrack which explains any relevant visual details, captions, and an ASL version.

Req. No.	Requirement
1.6	Proponents, associates and subcontractors must be able to demonstrate an understanding of accessibility and accommodation requirements for Persons with Disabilities in the delivery of their Solution and services, including: (a) How people with various disabilities will access the Solution; (b) Web accessibility requirements and techniques; (c) Techniques for making videos accessible; and, (d) Techniques for making the Voter Contact Centre accessible.
1.7	The IVS must be web-enabled and support the geographically diverse voter, daylight savings and time zones when scheduling, logging and reporting on activity. The IVS must be able to accommodate 24/7 access during the Advance Vote Period.
1.8	The IVS must allow voters to log into the system prior to the start of the Advance Vote Period without permitting those voters to cast a ballot (for example, to test their PIN) until the Advance Vote Period begins.
1.9	The Solution must provide a demonstration website, which shall be made available at time of submission of the Proposal, with the following characteristics: (a) Sufficient data capacity for data for ten thousand (10,000) voters; (b) Pre-populated with fictitious voter data; (c) An election consisting of one ballot type (based on the Sample found in Appendix K of the RFP); (d) Three (3) offices (Mayor, Councillor, School Trustee), each with a minimum of ten (10) candidates; (e) One (1) referendum question with a Yes/No answer; (f) The URL to access the website; (g) Fifteen (15) IDs and passwords to access the website as a "voter;" and, (h) Fifteen (15) IDs and passwords to access the website as an "Election Official."
1.10	The IVS must support both Official Languages of Canada (English and French), including the display of French characters (i.e., accents).
1.11	The IVS must allow a voter to customize all text or audio content within the IVS, at any point, to either French or English, including in respect to how it will conform to the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA.
1.12	The IVS must not require any client-side software other than the Internet browser.

Req. No.	Requirement
1.13	The IVS must provide support personnel in a Voter Contact Centre hosted within Canada.
1.14	The IVS must have all production and redundant server hardware (including server hardware for technical support) located in Canada.
1.15	The IVS must ensure that all City voting data (including data stored in primary and back-up data centres) is stored in Canada and is protected and secured from any unauthorized access.
1.16	The Proponent must agree to not conduct data mining on the user data, unless it is necessary for services required by the City.
1.17	For the provisioning of the IVS, data must only be accessed from within Canada.
1.18	The Vendor, must agree that, upon confirmation from the City Clerk after the legislated records retention period of 120 days, all traces of electoral data captured within the IVS or in the Vendor's possession, including backups and summary data, will be returned to the City or destroyed.
1.19	To ensure the integrity of the Solution's data and voter privacy, the IVS must control access using a VPN or 2-Factor Authentication.
1.20	The Proponent must indicate their support for the City to conduct a Privacy Impact Assessment (PIA), Threat Risk Assessment (TRA) and Vulnerability Assessment (VA), of the Solution to identify privacy and security risks. The Proponent should identify any limitations to the support of this requirement and should specify the reasons for such limitation.
2.0	**FUNCTIONAL REQUIREMENTS**
	REGISTRATION & VOTING
2.1	The IVS must ensure the voter receives clear and accessible instructions on the registration and voting procedure.
2.2	Removed.
2.3	The IVS must allow a user to process through self-registration web site.
2.4	The IVS must give notification to a voter that user-supplied information will be stored on servers outside the City infrastructure.
2.5	The IVS must confirm a voter has read the declaration of qualification and agrees that they are eligible to use the IVS before allowing the voter to proceed.

Req. No.	Requirement
2.6	The IVS must manage a voter registration if a voter has already registered under the same name and the same address.
2.7	The IVS must manage a voter registration if a voter has registered under the same name and a different address.
2.8	The IVS must provide automatic notification for confirmations, registrations, changes, vote cast, and vote cancellations.
2.9	The IVS must securely communicate a voter's unique PIN in an accessible format of the voter's choice (i.e., postal mail, Braille, email, SMS or telephone).
2.10	The IVS must be able to re-assign a voter to a different Ward.
2.11	The IVS must be able to re-assign a voter to a different address within the same Ward.
2.12	The IVS online module must support registration or voting using multiple Operating System platforms.
2.13	The IVS must allow voters to phone the Voter Contact Centre to register to use the Service by communicating directly with an agent.
2.14	The IVS must support other languages.
2.15	The IVS must manage and provide a notification message to voters who log in to the system before the Internet Voting Period begins (for example, to test their PIN).
2.16	The IVS must display or read all candidate names for an office (Mayor, Councillor or Trustee) to ensure the voter views all candidate names for an office prior to making a selection and casting their ballot.
2.17	The IVS must prompt a voter to confirm their candidate selection prior to navigating to the next office. The solution must offer the voter an opportunity to start the voting process over.
2.18	The IVS must notify a voter of under-votes or over-votes (i.e. spoiled ballots) and allow the voter to either correct the ballot or to cast the ballot as marked, with only valid votes being counted.
2.19	The IVS must support a voter's ability to decline a ballot.
2.20	The IVS must allow a voter to submit a blank ballot.
2.21	The IVS must verify the authenticity of a ballot and ensure it is a valid ballot.

Req. No.	Requirement
2.22	The IVS must provide a confirmation (receipt number or other information) to a voter to indicate that their ballot has been cast successfully.
2.23	The IVS must ensure that a voter's ballot, once cast, is counted and that the vote(s) marked on the ballot are recorded for the correct candidate(s), and that such votes are verifiable.
2.24	The IVS must ensure that a voter's ballot, once cast, cannot be viewed, tampered, or altered in any way even if a public machine (e.g. Public Library computer) is used.
2.25	The IVS must ensure no data showing a link between a voter and their selection(s) is stored, ensuring the integrity and anonymity of the vote.
2.26	The IVS must protect the privacy, anonymity and integrity of a voter's ballot throughout the Internet Voting Process.
2.27	The IVS must ensure that a voter can only cast one ballot.
2.28	The Centralized Electronic Voters' List (CEVL) management system of the IVS must ensure a voter cannot cast more than one ballot (e.g. using the Internet or Telephone, and voting in-person at an Advance Vote location).
2.29	The IVS must be able to manage a situation where a voter has been marked as voted ("struck off") incorrectly.
2.30	Removed.
2.31	The IVS must notify a voter of a failed session, and that the vote has been rejected due to the presence of another vote cast using their credentials.
2.32	The IVS must only allow votes to be cast only during the Internet Voting period, as defined by City Council Bylaw.
2.33	Removed.

Req. No.	Requirement
	REPORTING
2.34	The IVS must provide several standard reports or a dashboard for viewing the following, at a minimum: (a) The full Voters' List; (b) The list of voters who have registered to use the IVS (including by Ward); (c) The number of votes processed; (d) A list of voters who have completed the voting process; (e) Voting traffic statistics; (f) Failed login attempts; (g) Voting session statistics, including timeouts and lost voter sessions; (h) Errors, system responsiveness; and, (i) Any other measures to indicate quality of service at all times.
2.35	The IVS must provide the City with reports (including audit reports) that can be filtered by numerous parameters, including Ward, date, and daily reports during the Advance Vote Period.
2.36	The IVS must be able to identify and report on any ballots that were spoiled (over-votes and under-votes).
2.37	The IVS must allow the export of report data to the following formats: PDF, CSV, TXT, MS Excel and Word.
2.38	The IVS must provide a built-in survey tool for collecting feedback from voters.
	SOLUTION SUPPORT
2.39	The Vendor must provide 24/7 support throughout the election process, including media and candidate education/demonstration(s) of technology, on-site support and telephone response(s).
2.40	The IVS must offer support (phone, online) to voters during the Internet and Telephone Registration and Voting processes in both Official Languages of Canada.
2.41	The IVS must provide a self-service feature to allow a voter to retrieve a lost password including methods for a voter who does not have access to email.
2.42	The IVS must provide the ability to use a voter's shared secret as a method of authenticating the voter's identity, in the event a voter needs to retrieve a lost PIN.

Req. No.	Requirement
2.43	Removed.
2.44	The IVS must provide online help, and online help in other languages. Refer to "How to Vote" at: www.toronto.ca/elections/voters
	VOTER CONTACT CENTRE
2.45	The Voter Contact Centre must address issues, including but not limited to: (a) Changing school support, to ensure the voter views the appropriate ballot; (b) Modifying a voter's address, if the voter has moved since the previous election; (c) Adding a voter to the voters' list; (d) Retrieving voter PINs and (e) Re-setting Voter passwords.
2.46	The Voter Contact Centre must integrate with the City's 311 Contact Centre to provide support in other languages.
2.47	The Voter Contact Centre must have the capability to respond to the call volumes and with respect to availability and response times detailed in SCHEDULE "J" of this Agreement.
2.48	The Voter Contact Centre must log incoming and outgoing communications and/or correspondence with voters.
2.49	The Voter Contact Centre must provide statistics on call volumes, types of calls received, etc.
2.50	Removed.
	VOTERS' LIST MANAGEMENT
2.51	Removed.
2.52	The CEVL must allow Election workers to access the voter's list electronically and in real-time, including different levels of user access at the same location and user access restricted by ward.
2.53	The CEVL must support the capability to produce files in a format (e.g., PDF, Microsoft Word) that can be used by a print and mail facility for PIN production and distribution.
2.54	The IVS must provide a validation process to ensure that all voter information has been deleted from the system providing the print and mail service.

Req. No.	Requirement
2.55	The IVS must ensure the voter is presented with the correct ballot based on their Ward and school support.
2.56	The IVS must support the capability to add a voter to the CEVL and issue the voter a valid PIN, in addition to the IVS's ability to: (a) Audit the process of generating PINs; and, (b) Ensure safeguards are present in the generation of PINs to ensure randomness and prevent scripted attacks.
2.57	The IVS must have the ability to meet any legislative requirements for adding or editing a voter record and creating any forms required.
2.58	The CEVL must provide export capabilities to provide the City with an updated voters' list upon request.
2.59	Removed.
2.60	The CEVL must provide the ability to provide Candidates with access to the list of voters who have voted using the IVS at the end of each day during the Advance Vote Period.
2.61	The IVS must be compatible with other input devices, including barcode scanners (for scanning the barcodes found on Voter Information Cards at the in-person Advance Vote).
2.62	The IVS must perform the balancing process ensuring the number of voters marked voted matches the number of votes cast plus declined and any blank ballots.
2.63	The IVS must be able to maintain Ward and Subdivision boundaries, including a street index, that allows for the splitting and merging of voting subdivisions.
	ACCESSIBILITY & USABILITY REQUIREMENTS
2.64	IVS must provide accessible experiences to voters with a variety of disabilities.
2.65	Removed.
2.66	The IVS must allow voters to change the language of the IVS when they access the application.

Req. No.	Requirement
2.67	The IVS must provide confirmation for actions which cannot be undone, including conformity to WCAG2 SC 3.3.4 Error Prevention (Legal, Financial, and Data). For more information on WCAG2 SC 3.3.4 Error Prevention, see: http://www.w3.org/TR/WCAG20/#minimize-error-reversible.
2.68	The IVS must provide an "Activity Indicator," notifying the voter on screen or over IVR that their action is being processed.
2.69	From a usability perspective it is important for the City to offer voters a consistent experience. The IVS must provide an expected response to a sequence of actions by the user, use identical terminology and abbreviations throughout, and any prompts, messages or directives from the IVS should always appear, or be announced within the IVR, in the same place.
2.70	The IVS online component must adhere to Responsive Web Design Principles.
2.72	The IVS online component must support screen resolutions of 800 x 600 or higher, without the need to scroll horizontally.
2.73	Removed.
2.74	The IVS online component must be compliant with HTML4 Browsers.
2.75	The IVS must help voters logically and intuitively navigate the order of links and forms, find content, determine where they are on the page or phone tree, and all IVS functionality must be accessible by a Voter using one (assistive) device.
2.76	Removed.
2.77	The IVS must be structured according to the logical information flow, so information is presented in the same order for users with assistive devices as for users without assistive devices.
2.78	Where it may serve to improve a form or a voter's understanding of the task, the online component of the IVS must use checkboxes, radio buttons and drop down lists whenever possible instead of open input fields.
2.79	Removed.
2.80	The IVS online component must support audio and video capabilities.
2.81	The IVS must use a method other than CAPTCHA of confirming that the user attempting to register or use the IVS is a human being.
3.0	**TECHNICAL REQUIREMENTS**

Req. No.	Requirement
	CONFIGURATION OPTIONS
3.1	The IVS must support the use of a customized domain name as specified by the City (e.g. “TorontoVotes2014.ca”). Please note: The City will be responsible for the registration of the customized domain name.
3.2	The IVS must support customization to the standard look and feel of other City web pages/sites.
3.3	The IVS must support the ability to customize the time allowed for a voting session prior to the system timing out.
3.4	The IVS must allow business administrators to implement Configuration changes without help from I&T or the Vendor.
3.5	The IVS must ensure that no information is stored on a voter's computer or any storage device, even on a temporary basis.
3.6	The IVS must be protected as part of the network architecture, including but not limited to perimeter and local firewalls, application gateways and firewalls, VPNs and network zones.
3.7	The IVS must use anti-virus software as part of the network architecture.
3.8	The IVS must integrate the Advance Vote Internet and Telephone Voting results with the Election Night voting results from the City's existing Election Night Management System (ENMS). The IVS must offer migration services which can amalgamate data from various sources, including but not limited to Oracle, SQL, Access, Excel worksheets into the IVS so records reside in one repository.
3.9	The IVS must support the import/export of the City's Voter's List. The City requires that all data transferred into and out of the IVS must be encrypted during transit. To facilitate this, the City utilizes Axway Secure Transport for FTPS (File Transfer Protocol Secure) services. The IVS must integrate with City file transfer services, including use of certificates issued by well known Certificate Authorities (CA), High Strength encryption and static IP addresses?
3.10	The IVS must ensure data security in the hosted environment.
	ARCHITECTURE
3.11	The IVS hosting environment must have load balancing support and redundancy.
3.12	Removed.

Req. No.	Requirement
3.13	The IVS must provide a Business Continuity (BC) and Disaster Recovery (DR) Plan.
3.14	The Vendor must provide a process for ensuring DR capabilities will meet the City's requirements detailed in SCHEDULE "J".
3.15	Removed.
3.16	Removed.
3.17	The Vendor must provide operational data backup and restore procedures in detail, including the frequency at which the backup and restore process is regularly tested and run, and the retention process.
3.18	The IVS must provide an advanced monitoring tool that will allow the City to monitor the IVS application availability.
3.19	The IVS must notify the City and voters of scheduled down-time.
3.20	Removed.
3.21	The IVS must allow the City to choose when upgrades are to be performed to allow proactive communication to manage voters and advise of down-time.
3.22	The IVS must provide an outline of the database maintenance provided with the Solution, including information on any required processes (Reindex, etc.) from external or third-party applications. If the Solution provides maintenance tools, outline the best practices in utilizing those tools in keeping the data within the Solution clean.
	PERFORMANCE REQUIREMENTS (SPEED, CAPACITY, AVAILABILITY)
3.23	The IVS must be load tested and the results be verified to ensure they meet the City's requirements detailed in SCHEDULE “J”
3.24	The IVS must accommodate the minimum number of concurrent voter sessions detailed in SCHEDULE “J”.
3.25	The IVS must be able to process and store data related to 1.6 million voters.

Req. No.	Requirement
	SECURITY
3.26	The IVS must detect and/or prevent each of the commonly cited classes of risk listed below: (a) Hacking – One or more outside hackers attempt to penetrate the election web servers, IVR system or supporting infrastructure; (b) Insider Tampering – One or more insiders with varying levels of privileges attempt to observe or change votes; (c) Viruses or Malware – A virus spreads or a worm propagates that is designed to change voter's votes on their PCs; (d) DoS - An attacker attempts to make voting impossible via the IVS for some or all users; and (e) Phishing – Voters are directed to a fake website where their PIN or identity is stolen and used.
3.27	The IVS must provide: (a) A robust and secure architecture to ensure a high level of availability during the voting period, with no single point of failure and no single storage locations in the system design; (b) A highly tamper-evident design; (c) Protection from attacks via the user's device (such as via the privileges given to a user, whether by the intended user, a remote observer or a virus); (d) Automatic measurement or assessment of the reliability of home computers; (e) In the case of Internet voting, that no information relating to a voting session shall remain on the computer once the session has been completed; (f) Elegant handling of voters who attempt to use unsupported browsers; (g) No indeterminate states and no silent failures; (h) Use of modern security techniques to ensure reliable and accurate operation, and a security-in-depth design is preferred; (i) Maintenance of voter privacy; (j) Protection from identity theft; and, (k) Protection against various DoS attacks and traffic analysis attacks whether via third-party filtering services or devices that may be installed in the data centre.

Req. No.	Requirement
3.28	The IVS must protect against electronic “eavesdropping” on an elector casting a vote, either: (a) By someone with authorized access to the IVS; or, (b) By someone else who is not physically present with the elector when they are voting using the IVS.
3.29	The IVS must use a secure mechanism for ensuring that each ballot is for a particular voter, and that no external, unauthorized, or “rogue” ballots or votes are cast.
3.30	The IVS must identify and advise Election Officials of any suspicious voting activity or unauthorized access to voting servers.
3.31	The IVS must enforce strong password criteria for voters' accounts, such as minimum password length, required pass phrase composition (e.g., required use of letters, numbers and symbols), and recently-used passwords.
3.32	The IVS must provide voter password protection with multiple security levels to limit access to the data.
3.33	The IVS must support a password-aging function for administrative users and a process for management of user passwords and PINs, including expiration, notifications to reset and, security questions.
3.34	The IVS must have a lockout function that disables an ID/password or PIN combination after a pre-determined number of failed login attempts. The IVS must have the ability to control access based on login attempts, specifically the amount of time a user or voter is locked out, the number of times a user or voter is locked out before the account is frozen, and the user role responsible for resetting a locked-out user or voter.
3.35	The IVS must store password and PIN values in an encrypted format.
3.36	The IVS must perform automatic timeout/sign-out of voters when they have been away from a session for specified a period of time. The session timeout function must be programmable and flexible.
3.37	The IVS must provide segregated Administrative and support staff IDs roles in the Administrative module.
3.38	The IVS must include an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).
3.39	Removed.

Req. No.	Requirement
3.40	The IVS must limit System-Level privileges to the Solution administrator through administrative ID/password credentials only, supporting role-based access.
3.41	The IVS must support fine-grain authorization for administrative users and voter accounts to underlying functionality, congruent with the principle of least privilege.
3.42	The IVS must encrypt data at rest.
3.43	The Vendor must provide a list of the cryptographic and security standards fulfilled by the Solution.
3.44	The Vendor must provide an authentication diagram showing the path of authentication from end user into the application. This diagram should include the different types of users including end users, administrators and infrastructure support personnel.
3.45	The Vendor must detail any outsourced or subcontracted functions and how the IVS will ensure the confidentiality, privacy, and security of City data are safe-guarded, including detail on processes for monitoring and enforcing compliance with any of the IVS service providers.
3.46	The IVS must list ALL locations where City data will be stored, processed or accessed.
3.47	Removed.
3.48	Removed.
3.49	Removed.
3.50	Removed.
3.51	Removed.
3.52	The IVS vendor must have an ongoing security awareness program (i.e. security training, company policy reminders, etc.) in place.
3.53	All Vendor employees involved in the IVS must sign an agreement verifying they have read and understand company polices standards and procedures.
3.54	The Vendor must have a vulnerability management program in place for the IVS-hosting environment, including documented Business Continuity (BC) and Disaster Recovery (DR) Plan for the patch management process.
	INFRASTRUCTURE

Req. No.	Requirement
3.55	The IVS must ensure that the time on all the hardware required by the Internet Voting IVS is synchronized to a central time using NTP (Network Time Protocol).
3.56	Removed.
3.57	Removed.
3.58	In the event of a system failure, the IVS must be capable of notifying City Technical Staff via Systems and Application monitoring and messaging (email) systems.
	RESULTS
3.59	The IVS must be able to regenerate the internet voting results in the event a recount is required.
3.60	Removed.
3.61	The IVS must ensure that the number of ballots cast equals the number of ballots counted, plus the number of spoiled ballots (over-votes and under-votes).
4.0	**NON-FUNCTIAL REQUIREMENTS**
	AUDIT REQUIREMENTS
4.1	The IVS must have auditing capabilities (e.g., capturing information whenever a content object is accessed) to help the organization reduce compliance risk.
4.2	Audit trails for a record must be maintained for as long as the record they refer to is maintained. The audit trail must follow any changes that have ever been made to the record to ensure that those changes have not compromised the integrity of the record.
4.3	Removed.
4.4	The IVS must pass relevant penetration tests, including DoS attack tests.
4.5	The IVS must monitor, record and secure all events/activities on the server used for storing the votes cast.
4.6	The Vendor must confirm that, upon direction from the City Clerk after the legislated record retention period of 120 days, unless a recount has been called, all electoral data captured within the IVS, or in the Vendor's possession, will be destroyed or returned to the City.

Req. No.	Requirement
4.7	The IVS must prevent the audit trail information from being edited or deleted by any user.
4.8	The IVS must monitor and control administrator access to data.
4.9	The IVS must ensure data related to the City Internet Voting Process is the property of the City. The City may request an electronic copy of the data at the end of the Election process. The format of this electronic copy can be in one of the following formats: database backup, XML, Excel or a database server backup.
4.10	Removed.
4.11	The IVS must ensure that certain information would be withheld from the general public and be provided only upon request after the election, including: (a) System logs: Created as the exhaustive record of all actions taken by the computer system and its users during the election (with the exception of capturing voter identity or voting intent); and, (b) System access: Any kind of technical access to production systems, including access by the Independent External Auditor, would be indirect and mediated by the City.
4.12	Removed.
4.13	Removed.
	INTEGRITY
4.14	Administrative and support staff IDs/roles must be segregated in the delivery of the Service or supporting the environment.
4.15	Removed.
4.16	The IVS must provide an end-to-end verification process that may create a receipt that would enable a voter to verify, post facto, that their vote has not been altered, without revealing which candidates they voted for.
4.17	Removed.

Req. No.	Requirement
	TRAINING
4.18	Removed.
4.19	Removed.
4.20	The IVS must provide on-site training for Elections Staff.
4.21	Removed.
4.22	The IVS must offer voter training including, but not limited to, manuals, audio and visual aids.
4.23	The IVS must offer self-paced training opportunities or the ability to play back training videos for users.
	VALUE ADDED SERVICES
	This section describes the additional services and products that the City will receive at no additional cost or fees. All proposed value added services are further described in Appendix F: Value added services of the Vendor's Proposal Submission.
A1:	Secure Online Credential Delivery: The Vendor must include, as a value added capability of the IVS, the provision of secure on-line credential delivery (or OTL – One-Time-Link).
A2:	The IVS, at a minimum, must hash all code using SHA-256 or other message digest algorithm, mutually agreed upon between the Vendor and the City, as well as signed by a mutually agreed upon public Certificate Authority (CA). The City's preference for a CA is Verisign.
A3:	Advanced monitoring tool: The Vendor must provision for access to an advanced monitoring/reporting tool that will allow the City to analyze, in real time, the status of the election, allowing users to customize their own reports with predefined automatic alerts.
A4:	Execution of critical actions in an isolated/physically dedicated environment: As detailed in Section 5.1.4.1 of the Vendors' RFP submission, the Vendor will execute all the critical actions in a physically dedicated environment that will be isolated from any other network. These critical operations will be executed in an environment that will not be shared by other Vendor clients.

Req. No.	Requirement
A5:	End-to-End Encryption: The IVS must have the capability of performing end-to-end encryption from any kind of device (such as computers, tablets and mobile devices) without having to install any external component/plug-in, by using the built-in JavaScript technology (available in every modern browser) to execute Vendor's cryptographic protocol.
A6:	Immutable logs: The IVS must store all important actions performed by the system, including Voters' and administration users' activities, in special, cryptographically chained logs, ensuring that no one can manipulate the stored entries.
A7:	Electoral Board: The Vendor must implement a special secret sharing scheme to split the private key in pieces which can be stored on smartcards protected by Toronto election officials.
	ADDITIONAL SERVICES
	This section describes the additional/optional services to be included by the Vendor in the stipulated Agreement's SOW.
A8:	Phone Voting: The Vendor is to provide a telephone voting system that enables any voter to cast their vote privately with a standard land line or mobile phone.
A9:	Social media monitoring: The Vendor is to provide a Social Media Monitoring tool to monitor and measure the climate around the City of Toronto's 2014 Municipal Elections by analyzing the information published in the social media. This tool automatically identifies information from social networks (e.g. Twitter) and other social media (e.g. blogs, online news sites, forums…) related to the election process, processes it in order to provide an aggregated view showing what is being said about the election, the candidates, the City, etc.
A10:	SMS voter notifications delivery: The Vendor is to provide, as an optional service, SMS messages as an alternative notification submission channel.
A11:	Braille letters: The Vendor is to offer the service to print the letters in Braille, if requested by any voters. The Vendor will implement grade 1 (or grade 2) Braille formats, Braille embossing and production, letter shop and mailing via Canada Post.
A12:	DataFix Voter List Management Solution: The Vendor will utilize DataFix's Municipal Voter View (MVV) list management system as the IVS CEVL solution. The MVV solution will be tightly integrated and tested with the Scytl voting platform.

Req. No.	Requirement
A13:	MVV Mobile: The Vendor will provide a mobile application that, used as contingency in the event that election workers at the voting place cannot access the live CEVL, will allow them to continue to process voters, and to strike electors off the Voters' List as having voted. MVV Mobile will log the location and time of each transaction, storing the data in the local database. Once connectivity is restored, the application will automatically synchronize the electors recorded in the mobile application with Municipal VoterView.
A14:	Candidate Access Portal: The Candidate Access Portal will offer candidates with a dedicated portal for controlled access to view Voters' List data that is applicable to their constituency. Candidates must be able to view real-time data for eligible electors via basic search capability. In addition to displaying elector information like name, property address, and mailing address, candidates must also be able to view voter strike-off status. The Portal must provide candidates with the ability to extract delimited text files containing the elector data that they are entitled to view. These extracts are must be suitable for importation into Excel and allow candidates to obtain current elector data without requiring the involvement of election staff.
A15:	Data Loads: The Vendor will complete a "merge" of the Supplementary List of Electors (SLE) when available, following the initial load of the Preliminary List of Electors (PLE) This merge routine must compare new data supplied by MPAC in the SLE to the original data in the PLE and the list of changes that have occurred in MVV. If an elector was updated in MVV and also appears as a change in the SLE, then the merge process must raise the issue as conflict to be resolved through an interface in MVV.

Req. No.	Requirement
A16:	Data Cleansing (Street Index): The Vendor must provide one of following three options: a) Municipal Voter View Functionality: MVV includes a data cleansing function that permits municipal users to review street name data that is received in the PLE. The tool allows users to make batch changes to incorrect street names, and once corrected users can mark the street name as accepted (in other words, correct). By filtering the list according to the accepted status, users can view street names that may require modification. The MVV must utilize an automatic "accepted" status flag based on the data provided by the City. (Street name corrections to non-accepted street names will be performed by City staff.) b) Property Address Verification as a Service The Vendor must provide a validation service using street index data from a variety of reliable sources to validate and correct street names and to apply ward/poll fixes. Street name matching and cleansing will occur upon receipt of the PLE. Once cleansed, the data will be loaded into MVV. c) MVV Application Enhancements: The MVV application must be enhanced specifically for the City, for cleansing street name data and verifying ward/poll assignments. This would be to implement additional MVV application changes to permit the City to perform the cleansing work on a semi-automated basis.
A17:	Daily Delta Process The Vendor must create an automated process that, on a nightly basis, will prepare a list of elector additions, changes, and deletions that occurred over the preceding 24 hour time period, The format of the resulting delta file and the delivery mechanism must be customized according to specific City requirements.

Req. No.	Requirement
A18:	Data Cleansing (Duplicate Electors) MVV must include integrated data cleansing functions that will be offered by default to the City. For example, mailing address additions or changes in MVV are processed through address accuracy software in real-time to identify potential issues. Where possible, corrections are provided that the user can optionally accept. MVV also includes batch data cleansing functions to identify duplicate electors and other data quality issues across the full voters' list. This functionality will be provided to the City, with some application customizations. For example, DataFix algorithms would identify more than 50,000 potential duplicate electors in the City of Toronto, which the current MVV user interface for reviewing and resolving duplicates is not built to handle.
A19:	Balancing of Electors at the CEVL user level: a) The MVV must provision for counts of recorded electors at the individual user level to produce extracts of recorded electors. These extracts can optionally include the username of the election worker who marked the voter as having voted; OR b) The MVV must offer a default report, "Recorded Electors by Poll Worker," that will allow the City to view balancing reports at the user-level.
	COST METRICS
A20:	Phone Voting (50,000 voters): (a) 15% usage (7,500 voters); estimated call duration of 10 minutes.
A21:	Social media monitoring: (a) Setup includes a queries analysis meeting, and the configuration of 50 queries and 10 dashboards. (b) Includes one (1) multi-user access to dashboards and reports. (c) Three (3) months of service (with a limit of 200,000 mentions tracked and processed per month).
A22:	SMS voter notifications delivery: (a) The price includes the setup fee. (b) Messages are sent from within Canada. (c) Maximum of 100,000 SMS messages are sent (50,000 SMS messages for Step one and 50,000 SMS messages for Step two).

Req. No.	Requirement
A23:	Braille letters: (a) The service will include a QA process by a certified Braille expert. (b) The letters are mailed in a 9" x 12" envelope and each document will have a fly sheet with address information. (c) Based on 1,000 letters (1 letter producing 2 output pages). Per usage cost over 1,000 letters: $6.99 per letter (d) Postage costs included.
A24:	MVV Mobile: (a) MVV Mobile service is estimated to be $25,000.
A25:	Candidate Access Portal: (a) Service is estimated to be $19,000.
A26:	The estimated fee for running the merge process (including expected customizations): $12,500.
A27:	Daily Delta: (a) Development, testing, and managing of the nightly delta process is estimated to be $7,500.00.
A28:	Data Cleansing (Street Index): • Options (a) and (b) - no additional fee. Functionality is included in MVV out of the box. • Option (c) - Further discussion with the City is necessary. A fee estimate cannot be provided at this time.
A29:	Balancing of Electors at the CEVL user level: No extra cost for the options offered in A19.

SCHEDULE "I"

IVR Telephone Voting Service Requirements

Req. No.	Requirement
T1.	The IVR Service must be able to be operated regardless of whether the voter has a speech impairment or is unable to talk.
T2.	The voter must be allowed to restart if the voting session is interrupted.
T3.	Following authentication, the voter must be issued the ballot for the appropriate ward and school support, based on their address. The voter must be informed of the ballot name (for example name of ward) before they may start voting.
T4.	The Service must not announce any identifying information about the voter (e.g. voter's name).
T5.	The voter must not be able to choose their own ballot. If they are provided with the incorrect ballot they must be instructed to contact the Voter Contact Centre.
T6.	The ballot presented to voter must be a true and fair representation of the paper ballot (e.g. The order of candidates must be the same as the order presented on the Internet Voting service and the paper ballot).
T7.	The Vendor must implement robust procedures to ensure that candidate names are pronounced correctly reflecting the pronunciation guidance provided by the candidate and/or the City.
T8.	Text to speech rules used by synthetic speech technology cannot replicate proper name pronunciation and must not be used other than for prototyping purposes.
T9.	Candidates' names must be spoken in first name/last name order so that telephone voters can efficiently identify a candidate by name, even when the names are not presented in this format on the paper ballot.
T10.	The system must not allow the voter to submit more than one vote for each office.
T11.	The voter's selection(s) must not be linked to the voter's identity.
T12.	Any information on how to vote offered in a voting location must also be offered via the telephone voting system, in addition to instructions specific to using the IVR system.
T13.	The Vendor must, during design, and prior to implementation, engage users with a range of disabilities to test the IVR and provide feedback.

Req. No.	Requirement
T14.	The IVR must use consistent terminology, as compared to Internet voting, including but not limited to: a) Personal Identification Number (PIN); b) Password and Shared Secret; c) Receipt ; and d) The order of steps for casting a vote.
T15.	PINs must be between four (4) and eight (8) digits in length.
T16.	Passwords must only contain numeric characters (digits) and must be 4 to 8 digits in length.
T17.	When issuing PINs for telephone voting, via email, SMS, on paper or in Braille, numbers of more than 4 digits must be chunked into groups of 3 or 4 digits to assist comprehension and memory retention.
T18.	Accessible receipts or PINs should be delivered in the voter's preferred accessible format, either by the system, phone, SMS, email, Braille, or via postal mail in a printed letter format.
T19.	PINs sent by email must be able to be copied and pasted in full in one step.
T20.	Receipts must be in numeric characters only.
T21.	Where two or more menu choices are presented to the voter, the choices must be in the form of a menu of options, assigned in sequential order (e.g. assigning the first option to key 1, the second to key 2, etc).
T22.	Where the voter is asked a 'yes' or 'no' question, the affirmative option must be indicated by the "1" key and the negative by the "2" key.
T23.	The pound ("#") key must be used to confirm or move forward to the next stage in the voting session but must not be used to submit a completed ballot. This is to avoid any risk of double entry of the # key resulting in the unintentional submission of the ballot.
T24.	The asterisk or star ("*") key must be used to enter the "Options Menu."
T25.	The zero ("0") key must be used to request context-sensitive help, providing the option to transfer the voter directly to a human operator at the Voter Contact Centre for assistance.

Req. No.	Requirement
T26.	Within a voting session, unless information re-entry is required for reasons of privacy, security, or verification, the user must not be required to enter any given piece of information more than once. Confirmation of voter entries must be repeated back to the voter (i.e. PIN entry, not voter-identifying information)
T27.	Voters who are having difficulty in navigating or comprehending the automated telephone voting service should be given the option to "zero out" and speak with a Voter Contact Agent in order to obtain technical support on the IVR service.
T28.	At any point in the voting process, prior to casting their ballot, the voter must be provided with the opportunity to cancel a ballot, and/or change preferences and information that they have entered during the call.
T29.	When a voter indicates that they wish to cancel or clear all preferences from their current ballot, the system must present the voter with the confirmation menu before acting on the instruction.
T30.	The IVR must not require speech input from the user.

SCHEDULE "J"

QUALITY LEVEL METRICS

The metrics and values documented below are for the purpose of the Vendor's reference to address the requirements related to the scalability and availability of the IVS.

1. Projected Volume

The IVS must provide adequate baseline response times to meet the City's business needs under the following conditions:

For Internet Voting and Telephone Voting:

- A maximum of 6,000 concurrent users accessing the IVS during the peak registration and voting periods;
- 20 internal City users for administration/configuration of the system;
- 450-500 election workers with the Internet Voting Period running concurrently with the on-site Advance Vote; and,
- A voters' list comprised of 1.6 million records.

For the Voter Contact Centre:

- The Vendor should provide a Voter Contact Centre service level based on total call volume over the course of the Internet Registration Period and Voting Period of 50,000 calls.
- For the purposes of the Voter Contact Centre, the anticipated mean call duration is five (5) minutes.
- The Voter Contact Centre should take into consideration a potential influx of calls during:
    - The beginning of Internet Voting Registration;
    - The initial mail-out of voter PINs;
    - The beginning of the Internet Voting Period; and,
    - The final day of the Internet Voting Period.

2. Scalability

Scalability is the ability of the IVS to continue to function well when it, or its context, is changed in size or volume in order to meet the City's needs:

- The system should scale up to five times (5x) the initial projected volume.
- The voting period will last a minimum of six (6) days

3. Quality Level Metrics: Response Time

The IVS must be able to return the results of voter's request within the target response times, regardless of the number of concurrent users, storage capacity, or number of records in the system.

Table 1.

System Response Time	Service Objectives/Targets
Maximum time to authenticate a voter	< 5 seconds
Maximum time to display the results of a voter action for navigation between pages	< 5 seconds
Average time to initiate a voting session	< 5 seconds
Maximum time to wait to determine if a ballot has been successfully cast	< 10 seconds

Table 2.

Voter Contact Centre Response Time	Service Objectives/Targets
Maximum time for a call to be placed into the queue	< 12 seconds
Maximum time for live agent to answer a call in queue	< 75 seconds
Maximum percentage of deflected inbound calls	< 2 %
Minimum First Call Resolution (FCR) rate	> 75%

4. Availability

Availability requirements include system recovery time objectives, system uptime, maintenance activities and fail-over requirements.

5. Recovery Time Objective (RTO) & Recovery Point Objective (RPO)

The RTO states the target for maximum time to recover from an outage incident related to any one of Solution's Modules, Server and Network Hardware, or Operating System Software that results in the IVS operating below the Capacity requirements, as described by this document and is stated below. These targets are not the recovery objectives for a disaster recovery situation.

Table 3.

Use Case	RTO	RPO
Public Engagement Period	< 8 hours	< 8 hours
Demonstration Period	< 4 hours	< 4 hours
Registration Period	< 1 hour	< 10 minutes
Voting Period	< 1 minute	< 1 minute
Post-voting period	< 3 hours	Close of Advance Vote

6. Availability Management

The solution must provide automated recovery from system failures with minimal manual intervention. The availability objectives are:

- Production – 24/7 with the following exceptions:
  - Change Window: Weekday(s) 2:00 AM EST – 5:00 AM EST(on request)
  - Overall Availability of uptime during:
    1) Registration period: 99.9%
    2) Peak voting hours: 99.99%, 4:00 PM EST – 10:00 PM EST
    3) Off-peak voting hours: 99.95%, 10:00 EST PM – 4:00 PM EST

- Production Voter Contact Centre Support:
  - Registration period: 99.9% availability, Monday to Sunday, 8:00 AM EST – 10:00 PM EST
  - Internet Voting period: 99.9% availability, Monday to Sunday, 24 hours

- Production Technical Support:
  - 99.9% availability, Monday to Sunday 9:00 AM EST – 10:00 PM EST
  - Help Desk available 24 hours a day, 7 days a week
  - During Voting Period, Tech Support available on-site, Tuesday October 14 to Sunday October 19 8:00 AM EST – 8:00 PM EST
  - Tech Support available on-call at all other times, with a response time of 5 minutes

- Staging Environment:
  - Help Desk – normal business hours
  - Technical Support available on-site, Monday to Friday, 7:00 AM EST – 6:00 PM EST
  - Tech Support available on-call at all other times

- Results Reporting:
  - Results produced after 8:00 PM on Monday, October 27, 2014
  - Technical Support available on-site, Monday October 27, 2014 7:00 PM EST – 10:00 PM EST

SCHEDULE "K"

KEY PROJECT MILESTONES AND DATES

Deliverable	Date (2014)
Phase 1 Begins	April 1
Phase 1 Complete	April 14
Phase 2 Begins	April 15
Phase 2 Complete	April 30
Phase 3 Begins	May 1
Public Engagement Service – Go Live	May 2
Phase 3 Complete	May 20
Phase 4 Begins	May 21
Registration module complete	June 30
Voting module complete	June 30
Results Reporting module complete	July 15
First Mock Results Reporting Integration Test	July 28
Registration module UAT Go/No-Go	July 31
Voting module UAT Go/No-Go	July 31
Demonstration Service - Go Live	August 11 (on or before)
Phase 4 Complete	August 11
Phase 5 Begins	August 12
Integration of all IVS Modules UAT Go/No-Go	August 14
Results Reporting UAT Go/No-Go	August 14
Phase 5 Complete	August 15
Phase 6 Begins	August 16
Demonstration Service Shut Down	August 21

Deliverable	Date (2014)
Registration - Go Live	September 8
Second Mock Results Reporting Integration Test	October 6
Internet Voting begins	October 14, 10:00 AM EST
Internet Voting ends	October 19, 8:00 PM EST
Registration ends	October 19
Results generation	October 27, 8:00 PM EST
Phase 6 Complete	October 28
Phase 7 Begins	October 29
Disposition of Records, upon direction of the City Clerk.	February 25, 2015 (earliest possible date)
Phase 7 Complete	February 25, 2015

SCHEDULE "L"
INTERNET VOTING SERVICE PROCESS DIAGRAMS

Figure 1.

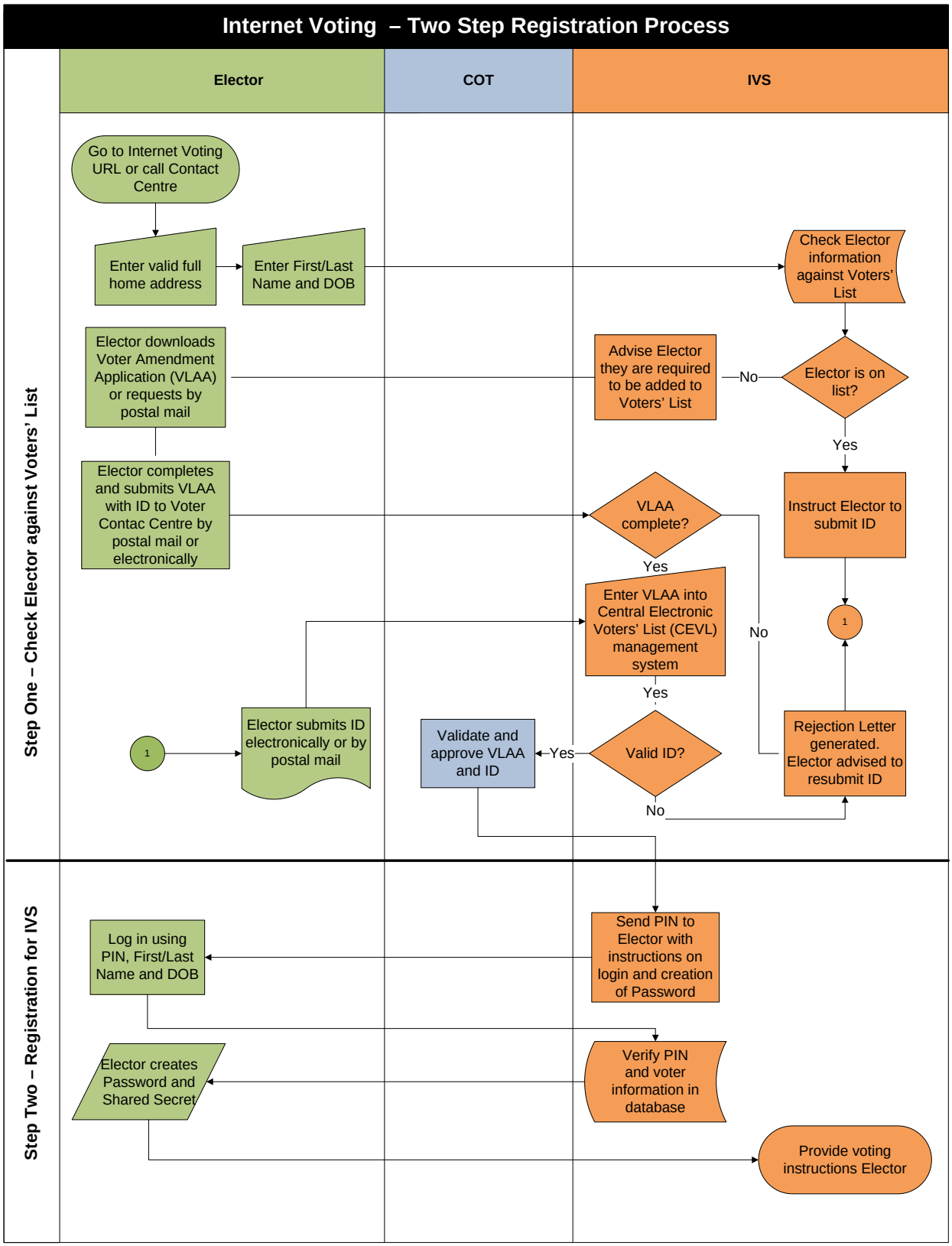


Figure 2.

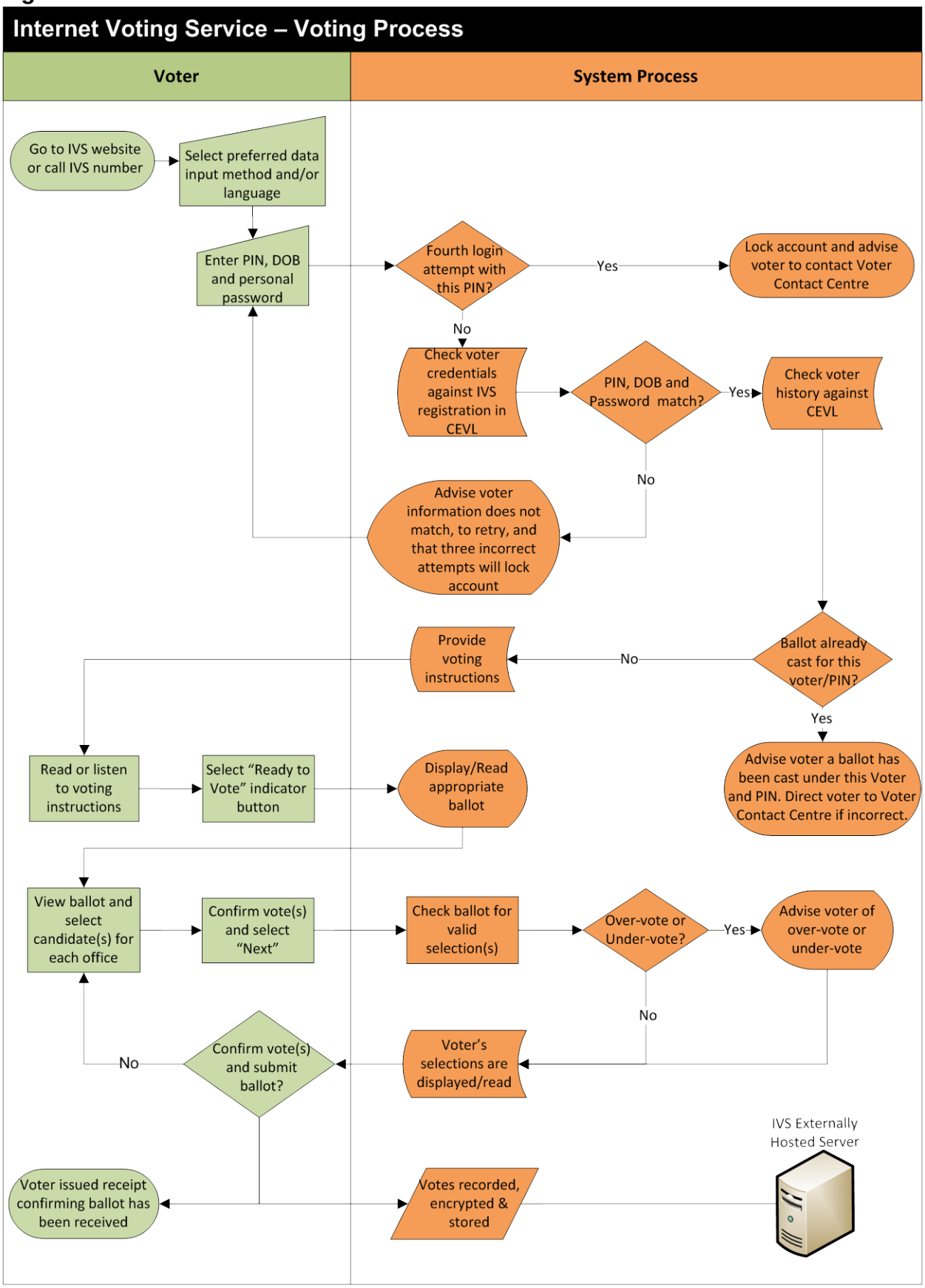
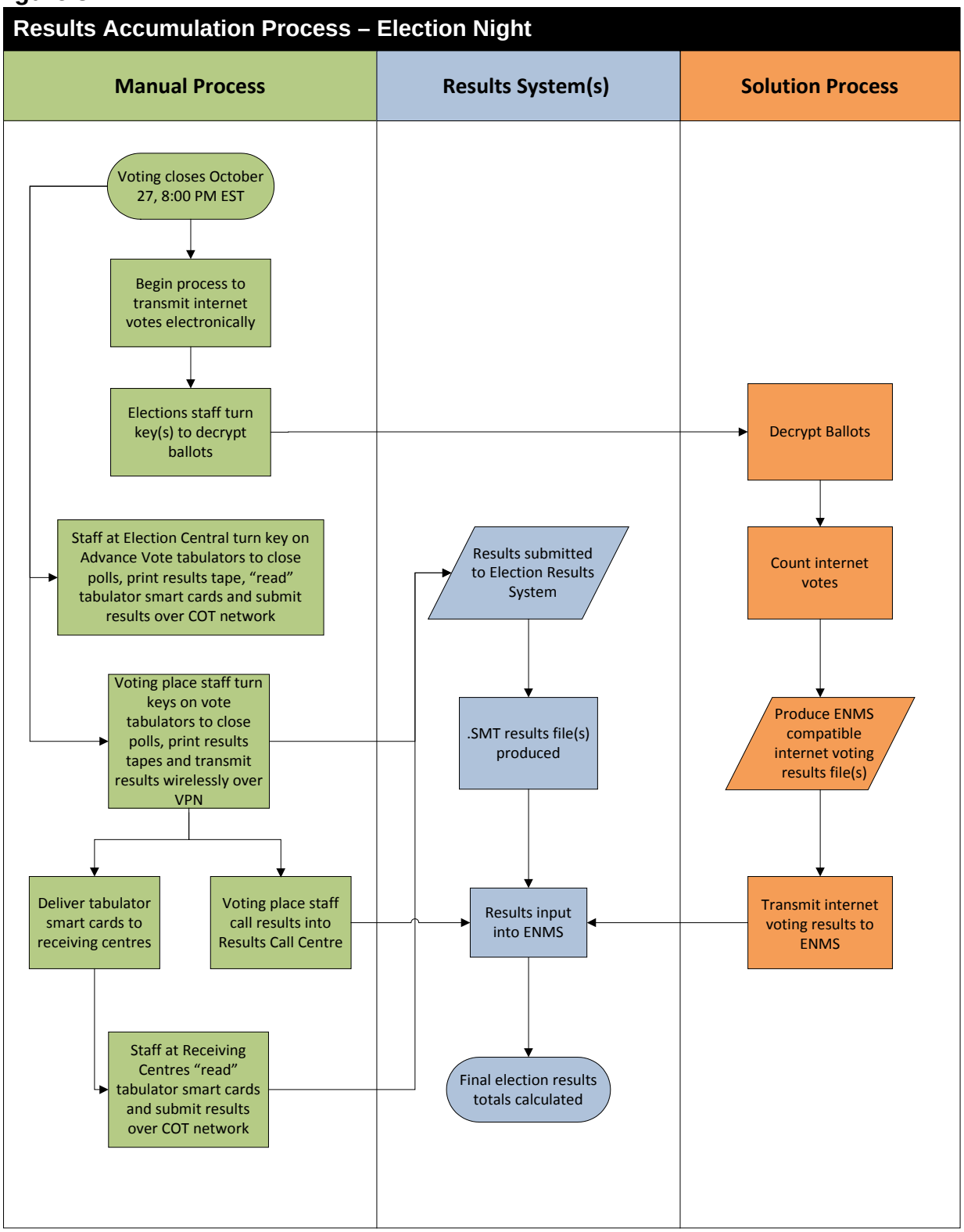

Internet Voting Service – Voting Process
Voter
System Process
Go to IVS website or call IVS number
Select preferred data input method and/or language
Enter PIN, DOB and personal password
Fourth login attempt with this PIN?
Yes
Lock account and advise voter to contact Voter Contact Centre
No
Check voter credentials against IVS registration in CEVL
PIN, DOB and Password match?
Yes
Check voter history against CEVL
No
Advise voter information does not match, to retry, and that three incorrect attempts will lock account
Ballot already cast for this voter/PIN?
No
Provide voting instructions
Yes
Advise voter a ballot has been cast under this Voter and PIN. Direct voter to Voter Contact Centre if incorrect.
Read or listen to voting instructions
Select "Ready to Vote" indicator button
Display/Read appropriate ballot
View ballot and select candidate(s) for each office
Confirm vote(s) and select "Next"
Check ballot for valid selection(s)
Over-vote or Under-vote?
Yes
Advise voter of over-vote or under-vote
No
Confirm vote(s) and submit ballot?
No
Voter's selections are displayed/read
IVS Externally Hosted Server
Voter issued receipt confirming ballot has been received
Votes recorded, encrypted & stored

Figure 3.


Results Accumulation Process – Election Night
Manual Process
Results System(s)
Solution Process
Voting closes October 27, 8:00 PM EST
Begin process to transmit internet votes electronically
Elections staff turn key(s) to decrypt ballots
Decrypt Ballots
Staff at Election Central turn key on Advance Vote tabulators to close polls, print results tape, "read" tabulator smart cards and submit results over COT network
Results submitted to Election Results System
Count internet votes
Voting place staff turn keys on vote tabulators to close polls, print results tapes and transmit results wirelessly over VPN
.SMT results file(s) produced
Produce ENMS compatible internet voting results file(s)
Deliver tabulator smart cards to receiving centres
Voting place staff call results into Results Call Centre
Results input into ENMS
Transmit internet voting results to ENMS
Staff at Receiving Centres "read" tabulator smart cards and submit results over COT network
Final election results totals calculated

SCHEDULE "M"
THE CITY'S EXISTING I&T INFRASTRUCTURE

This Schedule describes existing and planned Corporate I&T infrastructure and strategic products.

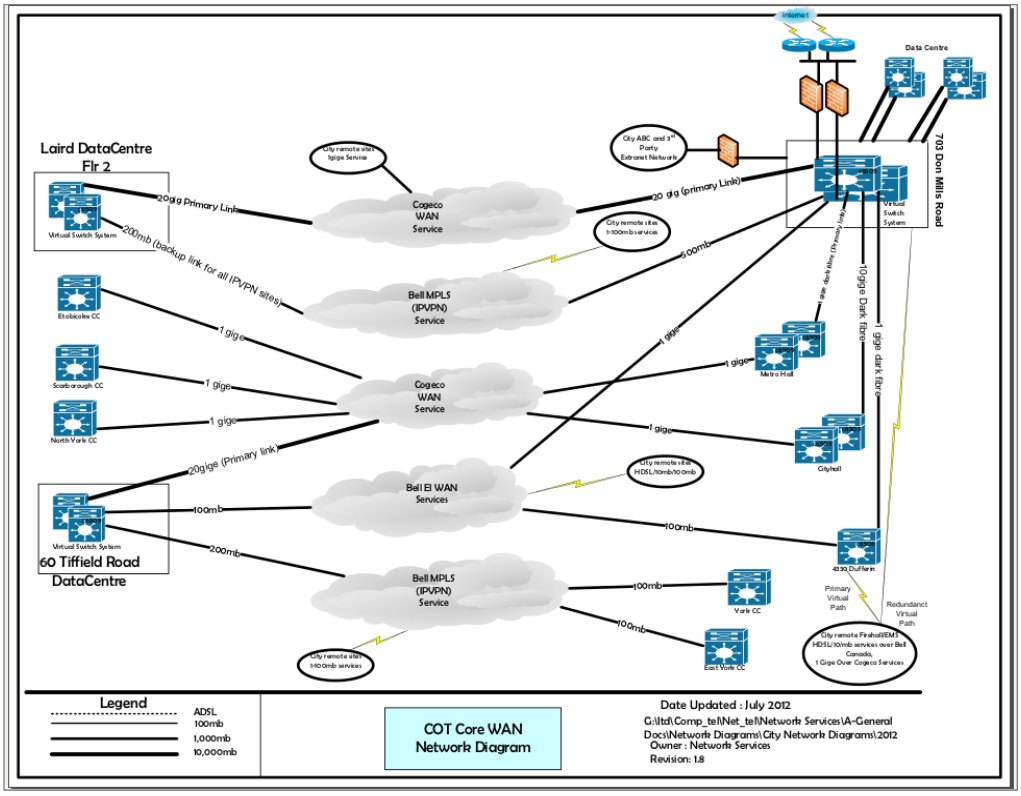
All new approaches and options provided and proposed should leverage the existing infrastructure in place as well as planned upgrades and migrations. In addition all Solutions should integrate with existing and planned management services.

Network Infrastructure
CityNet is a single communication utility providing network services for IP based systems. CityNet comprises over 600 network sites, with the core composed around 7 major Civic Centres, the three Corporate Data Centres and 4330 Dufferin (Fire/EMS office). The Data Centres are connected via a 20 Gbps fibre ring. The other major sites are connected via high speed 100 Mbps/1 Gbps/20 Gbps Fast Ethernet/Optical Ethernet Wide Area Network Service.

Remote sites are connected via HDSL or 10/100/1000 Mbps WAN fibre service. Most WAN connectivity terminates at the communications hubs at the Don Mills and Tiffield Road data centres.

Extranet connections are in place connecting the CityNet to various external organizations (The Province of Ontario, The TTC, Toronto Police, etc.).

Figure 1.



Internet access is provisioned by our Primary ISP via a dedicated 100 Mbps reserved connection. Current average (monthly) bandwidth utilization is about 90-100 Mbps. Business day usage averages over 90 Mbps. Additional outbound Internet service is handled by a secondary 150 Mbps ISP connection.

Standards based Internet services are also provisioned to support the City's Internet presence.

- SMTP mail gateways and Ant-Virus and Anti-Spam Scanning
- Domain Name Services (external).
- Domain Name Services (internal).
- Internal NTP Time Services.
- Bluecoat Proxy Caching System.
- Axway Secure Transport (SSH, FTPS based) File Transfer System.
- Accellion (HTTPS based) File Transfer System.

Internet Services are configured to separate Internal and External networks, with no provision on Internal clients for Internet DNS resolution or direct Internet connectivity. All client applications must be proxy aware to access Internet based services.

Security Services

First-level protection is provided by a stateful packet filtering firewalls. Security Configurations restrict traffic only to hosts in the DMZ (demilitarized zone) and the firewall. Other than SMTP, DNS, NTP, HTTP, all traffic is limited to outbound only.

Second level protection is provided by another stateful packet filtering firewall. All standard protocols (HTTP, HTTPS, SMTP, DNS, NTP and SSH) are supported along with custom proxies for non-standard protocols.

All internal access to servers in the protected networks are permitted only to authorized personnel by a secure encrypted tunnel via SSH (secure shell).

Endpoint Protection

The City uses Symantec Endpoint Protection (Version 11.6) on Windows Servers.

Strategic Products

RDBMS

The City's RDBMS platform for Business Critical and 24/7 applications is Oracle Enterprise and Standard Server editions (Version 11g Release 2) on a supported Unix based OS. The strategic high availability Solution for Oracle databases is Oracle Real Application Cluster (RAC). In total, the City has 200 Database instances deployed on 69 servers.

Microsoft SQL Server (2008 or above) is also supported for non-business-critical applications. There are approximately 20 Corporately managed SQL Server Databases.

All other RDBMS products are considered to be non-strategic platforms.

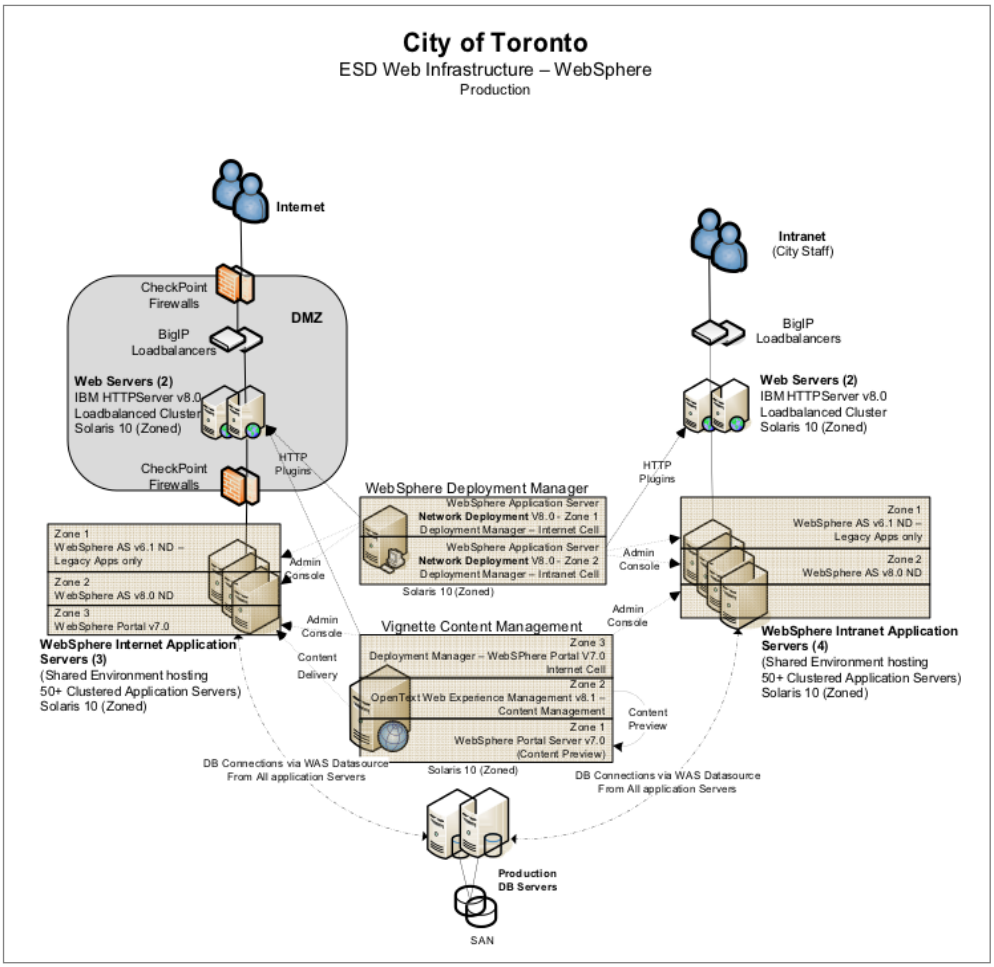
Web Application Environment

The City supports internally developed and commercially supported J2EE applications in two independent and segregated web application environments for internal Intranet and public Internet use respectively. The environments are based on IBM WebSphere Application Server Network Deployment (version 8.0) on Solaris 10 with applications deployed in 2-node clusters. Separate systems host IBM HTTP Server (version 8) instances on Solaris 10 configured with WebSphere plugins for forwarding of requests to application clusters.

WebSphere Portal (version 7), Open Text Web Experience Management (Vignette Content Management) version 8.1, Lotus Domino (version 8.5.2) and Google Search Appliance (version 6.108) are also deployed into these environments.

All primary Web based services are deployed minimally in 2-node configurations for High Availability and clustered via F5 BigIP Local Traffic Managers.

Figure 2.



Enterprise Application Integration Platform
The City uses Software AG WebMethods Broker (Version 8.2) and Integration Server (Version 8.2) as its common Enterprise Application Integration (EAI) platform. MyWebMethodsServer (Version 8.2) is used for administration and monitoring.

Telecom Platform
The City of Toronto is currently contracted with Bell Canada under a five-year Large Organization Centrex (LOC) contract which is designed to work in a large multi-location, multi-wire environment served from 3 Bell Canada Digital Multiplex Systems (DMS) 100 central switches, incorporating 27,250 + subscribers across 1,400+ locations.

SCHEDULE "N"
SERVICE LEVEL AGREEMENT (SLA) – HOSTED SERVICES

This Service Level Agreement is between the City of Toronto ("Client" or "City") and Scytl Canada ("Vendor" or "Scytl").

10.0 Principles

1) "Service Level Agreement" means a part of a service contract where the level of service is formally defined. The Agreement details minimum performance measures at or above which the Service delivered is considered acceptable and contains the specific Services provided, hours of availability, response times, and systems supported.

2) All parties to the Service Level Agreement (SLA) are mutually committed to fostering the spirit of partnership and adopting a joint problem-solving approach to resolving SLA issues. There will be open dialogue and information sharing. Changes impacting any part of this Agreement will be communicated and agreed to between the parties in advance of implementation.

11.0 Support Services

The Vendor must provide the City with the maintenance and support (Levels 1, 2 and 3 Support) and regular management reports needed for the smooth functioning of the IVS during the implementation and entire Go Live and Project Closure phases of the IVS. Support must be provided according to SCHEDULE "J". Outside of the times outlined in SCHEDULE "J", support must be provided as shown in the following chart:

Level	Description
Level 1 Support	Support is provided by the Vendor to address issues relating to the use of the IVS. Issues are logged and tracked to properly manage the issue from intake to resolution. An evaluation process is executed to determine the nature and severity of the issue. If not resolved at Level 1 Support the issue will be escalated to Level 2 Support. Level 1 Support is required to be staffed during Business Hours.
Level 2 Support	Support is provided by the Vendor to address issues that are not resolvable by Level 1 and cause reduced function of the IVS and business units. Level 2 Support is to be staffed, when necessary, to support business operations beyond Level 1 for completion of the issue. Issues not resolved by Level 2 Support will be escalated to Level 3 Support. Level 2 Support is required to be staffed during Business Hours.

Level 3 Support	Support is provided by the Vendor to address catastrophic conditions related to the IVS. These issues could be related, but not limited to, the application, underlying data engine or operating system errors. Issues of this nature require immediate expert attention from the Vendor. Due to the nature of the issue and its impact on business function and operation, Level 3 support is required 24 hours per day, 7 days per week throughout the Internet Voting Project for the 2014 Municipal Election.

11.1 Roles and Responsibilities

The following section identifies the specific roles and responsibilities associated with the two levels of technical support relating to the hosting and maintenance of the Internet Voting Service.

11.1.1 City of Toronto

In the event that the City experiences an Internet Voting Service-affecting situation caused by a problem with City system(s) or other non-Scytl-provided services, or if the City identifies any disruption or issues affecting the Internet Voting Service, the City will:

1) Inform the Scytl Technical Support Lead of the problem immediately;

2) Refer all diagnosed unresolved hosting or suspected software issues to the Scytl Technical Support Lead; and

3) Advise the Scytl Technical Support Lead, if the issue(s) caused by City system(s) or non-Scytl-provided services are resolved.

11.1.2 Scytl

In the event that Scytl experiences an Internet Voting Service-affecting situation, the Scytl Technical Support Lead will:

1) Act as the single point-of-contact with the Election Administrator;

2) For each issue that arises, the Scytl Technical Support Lead will:

   (a) Notify the Election Administrator immediately, or receive issue notifications from the Election Administrator, via email or a phone call;

   (b) Create Issue Ticket(s), and provide the ticket number to the Election Administrator;

(c) Answer the Election Administrator's questions or resolve the issue and notify Election Administrator of the issue resolution;

(d) Close the Issue Ticket;

3) Provide scheduled weekly end user support reports for all incidents, inquiries, and work requests;

4) Document, maintain and share support Documentation, such as support requests and, service tickets;

5) Provide weekly performance reports and statistics;

6) Provide any communications, Documentation and impact assessments related to system maintenance periods, planned down-times, and product upgrades as required;

7) Provide the City with access to:
   a) Case Management Tools to log and track cases via a 24/7 self-service portal;
   b) Online Support and Knowledge base self-service resources 24/7 through the website.

8) Assign a Client Success Manager who will be responsible for:
   a) Discussing (during normal business hours) ad hoc questions pertaining to the alignment of business requirements to configuration settings.

9) With prior approval from the City, schedule and communicate all maintenance at least 48 hours in advance to the Election Administrator; and

10) Communicate all unscheduled downtime to the Election Administrator immediately upon detection and follow up with a cause and resolution detail to update to the City's I&T Service Desk records.

11.2 Service Level Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

11.2.1 Service Scope

1) The following Services are covered by this Agreement:

   a) Manned telephone support, English and French
   b) Monitored email support, web form, txt, live chat, TTY and third party intercept operator;
   c) Regular system health checks

d) Technical support during business hours and outside of normal business hours following the quality level metrics and service availability outlined in SCHEDULE "J"

11.2.2 Service Availability

These IVS will be available during the following times. These times are subject to exceptions as detailed in SCHEDULE "J" of this Agreement:

1) The IVS Registration module will be available 24 hours per day, 7 days per week, from September 2, 10:00 AM to October 19, 2014, 7:00 PM, inclusive; and

2) The IVS Voting module will be available 24 hours per day from October 14, 10:00 AM to October 19, 2014, 8:00 PM, inclusive.

11.2.2.1 Voter Contact Centre:

1) The Voter Contact Centre service provider (AMA) is to deliver the support for the City of Toronto call centre Requirements, as detailed in SCHEDULE "J", consisting of 20 call center agents. In addition to the Voter Call Center, the service provider will include provisions for an overflow call center to handle any unforeseen or additional call volume that may occur.

2) The Vendor (Scytl) will provide 36 stations with overflow backup of 40 more stations. When 70% of capacity is reached (25 stations), additional lines are to be opened from backup staff (web based).

3) The support services to be provided by the Voter Contact Centre, Monday to Sunday 8:00 AM to 8:00 PM EST, include but are not limited to:

   a) Voter Registration.
   b) Assisting voters who need help to register online.
   c) Providing technical support to voters who cannot access the Solution or need to reset their PIN.
   d) Voters' List update services (changing school support, modifying voter's address, adding new voters, etc.).

4) Coverage parameters specific to the service(s) covered in this Agreement are as detailed in SCHEDULE "J"

11.2.3 Service Support & Software Availability

1) The Vendor must provide Technical Support and IVS automated recovery from system failures with minimal manual intervention 24 hours a day, 7 days a week, with exceptions as outlined in SCHEDULE "J" of this Agreement.

2) During Project implementation (before Go Live Registration begins on September 2, 2014), the Vendor will provide technical support of the IVS, from Monday to Friday, 8:00 AM – 8:00 PM EST. During the Go Live phase, s, the Vendor will provide 24/7 technical support as detailed in SCHEDULE "J" of this Agreement.

3) After Final Acceptance and from that point forward, Scytl will implement, maintain and comply with the issue notification and escalation procedures set out in this Schedule.

4) Issue resolution will be provided by qualified Scytl personnel to correct issues in the Applications and the Services by the provision, in the first instance, of bug-fixes, patches and workarounds and, by way of a permanent remedy for errors, the provision of all modifications necessary to the Software and the Services so that the Software and the performance of the Services conforms in all material respects to the Design Specifications detailed in the Agreement. Support Services will be available as described below twenty-four hours per day, seven days per week, including during holidays.

11.2.4 Scytl Service Support Package:

Support feature	Description
Live Phone Support	Scytl will provide 24/7 support during the IVS Registration and Voting periods, and throughout the election process by means of the Voter Contact Centre During Project Implementation (before the Registration Period begins September 2, 2014), standard support will be provided, from Monday to Friday, 8:00 AM to 8:00 PM EST.
On-site Support	Scytl will provide on-site support to the City during the IVS Registration and Voting period and Election Day, to rapidly address any issues that arise.
Named Lead Administrators	Up to five (5) individual Election Administrators who may contact Scytl Technical Support, including one "Super Lead Administrator."
Online Support and Knowledge Base	The Scytl IVS will provide voter self-service support resources available 24/7 through the web interface within the Scytl online "help guides" in the configured languages of the system (English and French at a minimum).
Service Levels	Standard, as set forth in section 11 of this Schedule.

11.3 Service Requests

11.3.1 General Queries

1) The Vendor shall endeavor to respond to all general queries about the Internet Voting Service within one (1) business day outside of designated dates.

11.3.2 Defect Resolution

1) In support of the Services outlined in this Agreement, Syctl will respond to service related incidents and/or requests submitted by the Customer within the following time frames:

   a) 0-1 hour (during business hours before Go Live) for issues classified as High priority.
   b) Within 2 hours for issues classified as Medium priority.
   c) Within 4 working days for issues classified as Low priority.

Severity Level	Meaning
High Priority	An emergency condition that has a critical impact on the Internet Voting Service and that makes the operation of any one or more critical functions of the Internet Voting Service impossible. High Priority issues include: • The IVS is not functioning correctly. **Time to Restore Objective:** Scytl will remedy High Priority problems within one (1) hour of the reported problems being confirmed where such problems are reported during normal Business Hours.
Medium Priority	A condition that makes continued operation of the Internet Voting Service, or a component thereof, difficult, but the issue is limited in scope and may be circumvented or avoided on a temporary basis. Voters are not affected. Medium Priority issues include: ▪ They IVS is unable to launch Administrative applications; ▪ The IVS is unable to record calls. **Time to Restore Objective:** Scytl Canada will remedy Medium Priority issues within two (2) hours of the problem being confirmed by Scytl.
Low Priority	A condition that can be avoided or circumvented and that does not have a material impact upon the operation of the Internet Voting Service. Voters are not affected. Low Priority issues include: ▪ Reinstallation or Installation of any Scytl software ▪ Failure to generate any daily administrative functionality **Time to Restore Objective:** Scytl will remedy all Low Priority issues within four (4) business days of the problem being confirmed by Syctl.

1) A "Defect" is a technical defect within the Internet Voting Service and/or those portions of software integration within the Vendor’s control. Defects fall into two

general categories: major (Severity 1 and Severity 2) and minor (Severity 3). The "Severity" of a Defect is determined by the City and the Vendor.

2) If the incident falls under the description of Severity 1/Severity 2, the City will provide input when reporting a defect but the Vendor will make the final distinction on the Severity level, subject to the following definitions and parameters: The Vendor must document, notify and fix any deficiencies identified in the Production Environment and provide notification as needed. The following table describes how deficiencies of various severity levels will be addressed:

1. Major Defects

- **Severity 1 (S1):** A Defect that results in at least one of the following. Severity 1 does not include downtime for maintenance:
  - the Scytl URL produces no results, or
  - The City's authorized users cannot log in to Scytl's application after repeated attempts.

- **Severity 2 (S2):** A Defect that results in any of the following:
  - no issues are being recorded or delivered;
  - no queue will process any transactions;
  - no report within the application produces any data or the data has not been refreshed in fewer than twenty-four (24) hours; or
  - dashboard will not function.

2. Minor Defects

- **Severity 3 (S3):** A Defect in one or more application features.
- **Cosmetic Defects:** Trivial defects that cause no negative consequences for the IVS. Typically related to appearance as opposed to function.

Deficiency Severity	Description	Required Actions by Vendor
Major (S1)	Privacy breach or discovery of a security vulnerability that could result in a privacy breach.	1) Remove Production system access immediately. 2) Inform the City's designated business contacts by email and phone within **15 minutes** of discovery of the breach. 3) Identify the root cause. 4) Propose possible mitigation solutions that will not jeopardize the integrity, security and privacy of the IVS, and the time required to implement. 5) Inform the City on resolution and test fix. 6) Document the root cause and fix within **12 hours** of resolution. 7) Provide a media relations spokesperson to support the City in addressing any media inquiries.
Major (S2)	Disastrous, severe or significant consequences for the IVS with no immediate workaround. Current implementation risks data integrity or limits client access to the IVS or its contents.	1) Remove Production system access immediately. 2) Inform the City's designated business contacts by email and phone within **30 minutes** of the discovery of the deficiency. 3) Provide a point of contact to initiate a service request that will have an escalation process to address the severity. 4) Identify the root cause. 5) Propose possible mitigation solutions that will not jeopardize the integrity, security and privacy of the IVS. 6) Inform the City on resolution and tested fix. 7) Document the root cause and fix within **12 hours** of resolution. 8) Provide a media relations spokesperson to support the City in addressing any media inquiries.

Deficiency Severity	Description	Required Actions by Vendor
Minor (S3)	Small or negligible consequences for the IVS. Simple workarounds typically exist.	1) Inform the City's designated business contacts by email and phone immediately upon discovery of the deficiency. 2) Provide a point of contact to initiate a service request that will have an escalation process to address the severity. 3) Respond to the City contact within two (2) business days. 4) Identify and document the root cause. 5) Propose possible mitigation solutions. 6) Obtain sign-off from the City on resolution and tested fix. 7) Document fix.
Cosmetic	Trivial defects that cause no negative consequences for the IVS. Typically related to appearance as opposed to function.	1) Inform the City's designated business contacts by email and phone upon discovery of the deficiency. 2) Provide a point of contact to initiate a service request that will have an Escalation Process to address the severity. 3) Respond to the City contact within three (3) Business Days. 4) Identify and document the root cause. 5) Propose possible mitigation solutions. 6) Obtain sign-off from the City on resolution and tested fix. 7) Implement change in next release unless otherwise agreed. 8) Document fix.

11.4 Issue Tracking and Reporting Process

1) During the processing of an issue, it may be necessary for a Scytl Support Lead to perform additional investigations.

2) An issue is considered closed when the Election Administrator is satisfied with the solution and agrees that the issue can be closed. The Scytl Support Lead will summarize the case, explain the solution and respond to any further questions from the Election Administrator.

3) If the City does not respond to a case in status ‘Client Action Required’ or ‘Client to Review Resolution’ within 5 days then the case will be closed. If the Administrator needs to reopen the case at a later date they may call the Scytl Support Lead for assistance.

4) If an issue cannot be resolved at any level, or will take a longer time than set timelines to solve, the Scytl Support Lead will explain the reason for the delay and update the Administrator as progress is made or weekly, whichever comes first.

5) The Election Administrator will receive feedback using the following methods or technologies:

- Via a phone call
- Via email

11.4.1 Escalation Contacts

Escalation Level	Scytl	City Of Toronto
Level 1	Product Specialist	Election Administrator
Level 2	Global Product Specialist Manager	Election Administrator
Level 3	Global Product Specialist Director	Election Administrator

(1) The Election Administrator will call the Scytl Support Lead for all and will be issued a case number for the issue at which point the issue has been officially recorded and accepted by Scytl Product Support.

(2) The single point of contact for issue fulfillment is the Scytl Support Lead.

11.5 Back up and Maintenance

1) As part of the Scytl hosting service, Scytl will back up the City of Toronto database. The principal objective of the backup, maintenance, and monitoring processes is to ensure maximum uptime and limited data loss due to any unforeseen emergencies.

2) Scytl will perform daily backups of the full database and hourly transactional backups to separate hot disks. Two days of hot backups are stored on a local SAN disk for immediate recovery. Scytl will perform full backups and daily differential backups of our data onto tape. Daily backups are stored for one week, weekly backups for five weeks, and monthly backups for the duration of the IVS project.

11.5.1 Server Uptime

1) The Scytl production server is to be up available 24/7 with exceptions as outlined in SCHEDULE "J". Scytl will monitor application availability and safeguard against software applications hanging or loss of connectivity to the database. In accordance with the Service Level Agreement, Scytl will notify the Election Administrator and specified people in the table of any server/application downtime. In case of a failure, Scytl will resolve the issue in accordance with the Service Level Agreement. The following individuals are notified immediately upon any failure:

Contact	Notification Mechanism	Phone
John Meraglia	Email: jmeragli@toronto.ca	416-395-1303
Jerry Liu	Email jliu@toronto.ca	416-392-0486

11.5.2 System Maintenance Schedules

1) Maintenance windows are planned outages for changes or routine maintenance. Advance notice is to be given to the City of any planned outages. Scheduling is to be done during the night hours over the weekends, so as to minimize any disruption to the Service.

2) When Scytl requires a maintenance window to modify the Internet Voting Service environment, , outside of the change windows outlined in SCHEDULE "J", the City's Election administrator is to be notified at least 48 hours in advance.

3) Maintenance updates may include:

- Code fix and planned updates to servers;
- Fully tested Security patches;
- Memory upgrade(s);

- Hard Disk drive replacement or upgrade;
- Addition of new servers;
- Changes to IP addresses;
- Re-wiring or cabling;
- Log archiving and deletion of logs; and
- Fully tested Scytl patches.

The list is not exhaustive and does not include all possible maintenance window circumstances.

11.5.3 Additional Maintenance and Support Responsibilities

1) The Vendor will provide maintenance and support, repairs, releases/updates (minor and major), patches, fixes, workarounds as further detailed in this for the duration of this Master Agreement. The City of Toronto reserves the right to waive and decline any new releases/updates offered by the Vendor for the duration of the Term and the Vendor shall continue to provide the support services as per this Schedule. Furthermore, the Vendor will provide upgrades for the Products they provide during the pre-production/development period, as well as during the Warranty Period at no additional cost to the City.

2) Any increases in the price of the IVS and support not fixed in the Master Agreement will not exceed the annual cost of living rate set by Revenue Canada.

11.6 SLA Review Meeting

1) SLA review meetings between the City of Toronto and Scytl will occur prior to the start of the implementation and IVS Registration period, and IVS Voting Periods. These meetings will include representation from Scytl and the City of Toronto. The purpose of the review meetings will be to review service performance, issues, achievements/shortfalls, service problems, trends and requirements to identify service improvement strategies and/or modify this SLA as required.

2) The information gathered at the review meetings will be used to measure success in meeting service objectives and to determine improvements, enhancements or development of new services and to ensure that the managers responsible for the services are apprised of potential problem areas. These review meetings will be scheduled and coordinated by the City Election Administrator.

3) The SLA will be reviewed following the effective date. Changes are recorded in the revision history of this Agreement, providing they are mutually endorsed by the two parties and managed through the Change Management process.

12.0 Issue and Dispute resolution

1) Issue and Dispute resolution will be subject to the processes defined in the overall agreement.

13.0 Security and Privacy

13.1 Introduction

1) This section describes the City information management requirements and expectations as they relate to the Vendor's delivery of service.

2) This document defines the following requirements, procedures and identifies interface/contact points between the City and the Vendor:

    1. Security/Privacy Contacts
    2. Security/Privacy Incident Management Procedures
    3. Operational Security/Privacy requirements

3) This section will ensure the Vendor’s Employees, Contracted Employees and Employees of the Sub-Contract arrangement with the Vendor clearly understand the City's requirements and operational processes to follow in the handling of the data of the City.

13.2 Security/Privacy Contacts

1) A Security/Privacy contact(s) will be appointed by both Scytl and the City. The Security/Privacy contact(s) is responsible for:

    - Liaising between the City and Scytl on security, privacy or other compliance matters;
    - Situational management of data breaches, information management and all other risk management issues as it pertains to the data collected, used or retained on behalf of the City;
    - Cooperatively investigating all security breaches within the bounds of the Internet Voting Service provided;
    - Assurance that all privacy/security breaches are reported, controlled and mitigated within the bounds of the Internet Voting Service provided to the City; and
    - Ensuring that privacy requirements under the *Municipal Freedom of Information and Protection of Privacy Act* are observed by Scytl in the handing of any data pertaining to their function as an agent/consultant of the City of Toronto.

2) The contacts are listed in Appendix A of this Schedule.

13.3 Security/Privacy Incident Management Procedures

13.3.1 Overview

1) This section summarizes the Security Incident Management process. It defines the process, identifies its scope, objectives and describes the activities leading to identifying, communicating and resolving the Security Incident related to the Internet Voting Service and City data.

13.3.2 Scope and Definitions

1) The Security Incident Management process outlines the actions and communications required to address IT security incidents and data breaches through the involvement of the City and Scytl's teams. It is an ongoing process concerned with minimizing the impact of IT security problems affecting the confidentiality, availability and services of the Internet Voting Service.

2) A security incident can originate within or outside the Internet Voting Service Environment, can involve external sites, and can range in severity. IT security incidents potentially involve system penetrations, unauthorized access or disclosure, destruction of data, fraud, crime or other serious matters.

13.3.3 Scytl's responsibilities:

1) Scytl shall notify City of Toronto of any High-Security Incidents and privacy breaches. See Appendix G of this Schedule for the Privacy Breach Protocol.

13.3.4 Security Incident Definition

1) A Security Incident is any adverse event whereby a material aspect of information security is compromised: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples of Security Incident Definitions can be found in Appendix C of this Schedule.

13.3.4.1 Definition of Security Incident Severity

1) Each security incident is categorized into one of three Incident Severity Levels, as defined below.

Severity Level	Meaning
HIGH	An adverse event, or detected vulnerability posing significant risk, such as: • Critical IT systems, services, including privacy breach of the most sensitive information - unauthorised or fraudulent access/use, destruction, disclosure, disruption, interruption, repudiation, loss, or theft; Loss of Tape / Media; • Reputation – total loss or grievous harm; and requiring immediate or urgent response
MEDIUM	An adverse event, or detected vulnerability posing moderate risk, such as: • IT systems, services, or sensitive information - unauthorised or fraudulent access/use, destruction, disclosure, disruption, interruption, repudiation, loss, or theft; and/or • Reputation – partial loss or harm; and requiring routine response
LOW	An adverse event, threat, or detected/suspected vulnerability: • Posing negligible risk; and requiring limited or no response (e.g. only awareness and periodic statistical reporting)

2) High-level Examples of HIGH, MEDIUM, and LOW Severity Security Incidents are listed in Appendix C of this Schedule. The list is not exhaustive and does not include all possible incidents. Incidents not on this list should be rated according to the Severity Level definitions given above.

13.3.4.2 Security Incident: Notification time

1) The elapsed time between the incidence of a security issue once confirmed (i.e. As soon as the Vendor is aware that such security incident has taken place) and the Vendor's provision of appropriate notifications to the City should be:

- High Severity*: Immediately
- Medium Severity: Within 2 hours

** All privacy and data breaches are considered high severity*.

13.4 Access to City Data

1) This section will detail the requirements on the collection, sharing, or disclosure of information between the City and the Vendor. The safeguards and controls upon the same are detailed in order to confirm compliance with both the applicable legislation and best practices.

13.4.1 Role based access model

1) Access to information will be limited by the role of the end user as granted by the administration of program. Program administrators will be responsible for the application, including issuance, alteration and removal of roles and access based upon need.

2) Application user roles and their access capabilities/restrictions are defined in Appendix D of this Schedule.

13.4.2 Application access process

(1) Program Administrator shall follow the Application Access Administration Process in Appendix D of this Schedule to grant, change, and revoke user access to the application.

13.4.3 Access control and authentication

1) Access to application and data are restricted to authorized users only. Access will be authorized only after successful authentication with identification and password.

2) Appendix E of this Schedule lists the minimum requirements for access control and authentication.

13.4.4 Other Operational Security Requirements

1) It is expected that The Vendor will manage the environment to meet Scytl's current SSAE16 control framework security requirements as listed in Appendix F of this Schedule.

2) The Check List includes the following sections:

- Physical Security
- Destruction of time expired, faulty or failed media
- Secure system and network configurations
- Control of access to the systems and networks
- Adequate logging and monitoring of events in the service
- Adequate documentation

- Appropriate management of personnel
- Appropriate procedures for dealing with malicious software
- Notification and management of changes
- Management of test data

13.4.5 Privacy Requirements

1) The Vendor, as an agent of the City of Toronto as defined by the *Municipal Freedom of Information and Protection of Privacy Act* (the Act) must comply with the following:

   (a) Appointment of the Security/Privacy Contact as per Section 3, who will make themselves available for an information session with the City of Toronto's Corporate Information and Management Services Unit for instruction on the requirements of the Vendor under that Act

   (b) All collections, uses and disclosures of information shared with, collected for or used by the Vendor on behalf of the City of Toronto must comply with the collection, use and disclosure provisions of the Act

   (c) Refer to Appendix H of this Schedule for additional Privacy Protection Requirements

   (d) Upon detection and confirmation of a privacy breach relating to City of Toronto data the following steps must be undertaken within 1 business day;

      - Notification of the City's Security/Privacy Contact as appointed under Section 1 and the CIMS contact
      - Suspension of the practices leading to the breach, including locking down any technologies that have been compromised
      - Retrieval of the data if possible
      - In the case of theft or peripheral devices, contacting the police and filing a police report
      - Identifying the individuals whose information has been breached
      - Any other actions deemed as reasonable under the City of Toronto Privacy Breach Protocol (Appendix G of this Schedule).

2) Any requests for City of Toronto data must be communicated to the City prior to any disclosure

APPENDIX A: Security/Privacy Contacts

1) **City of Toronto**

Eddie Ng,
Security & Risk Management Specialist,
Strategic Planning & Architecture,
Information & Technology Division,
416 -392-4493

2) **Scytl**

Jesus Choliz
Director of Security and Compliance
jesus.choliz@scytl.com

APPENDIX B: Security Incident Definition – Examples

The definition of a security incident may vary depending on many factors. The following categories and examples are applicable:

- *Compromise of integrity*, such as when a virus infects a program or the discovery of a serious system vulnerability;

- *Data privacy*, such as when data on any media is compromised like loss of data, unauthorized distribution, access to sensitive data, theft or other breach of City data;

- *Denial of service*, such as when an attacker has disabled a system or a network worm has saturated network bandwidth;

- *Misuse*, such as when an intruder (or insider) makes unauthorized use of an account or City of Toronto data within Scytl systems;

- *Damage*, such as when a virus destroys data; and

- *Intrusions*, such as when an intruder penetrates system security

APPENDIX C: Examples of IT Security Incidents

Severity Level	Examples
HIGH	a) **Malicious Code Attacks/Alerts – anti-virus software is ineffective (i.e., cannot detect/clean)** • Alert received about new malicious code posing a HIGH risk • Infection of network server, gateway, firewalls, or critical business systems • Destruction or corruption of confidential or critical production data or applications • Infection at two or more business locations or network domains within the last hour b) **Hacking Attack** – Actual or suspected penetration, compromise, or unauthorised privileged access – network, server, gateway, firewall, critical business system, sensitive/confidential information c) **Unauthorised Access** – Actual or suspected misuse of privileged access to systems or sensitive information by an authorized user d) **Denial of Service** – Actual or suspected systematic attack shutting down or interfering with IT services/processes e) **Vulnerability Alert/Report** – Uncorrected vulnerability is detected or suspected on systems that exposes to HIGH severity attacks f) **Criminal Acts** – Actual or suspected fraud, espionage, or other unlawful acts involving IT systems and/or sensitive information g) **Law Enforcement or Regulatory Investigation** – External investigation involving actual or suspected misuse of IT systems and/or sensitive information h) **Firewall Problems** – Any high severity problems impacting normal firewall operation. i) **Secondary / removable Storage media** (e.g. Tape, removable disk, CD's or Optical) Problem - Actual or suspected lost or theft of such media
MEDIUM	a) **Malicious Code Attacks/Alerts – anti-virus software is ineffective (i.e., cannot detect/clean)** • Alert received about new malicious code posing a MODERATE risk • Infection of server or workstations not connected to the network • Destruction or corruption of non-essential data or

Severity Level	Examples
	applications • Infection contained to one business location or network domain b) **Hacking Attack** - Repeated/determined penetration attempts by a single attacker that are unsuccessful c) **Unauthorised Access -** Actual or suspected misuse by an authorized user of general access to systems d) **Denial of Service** – Actual or suspected isolated (i.e. non-systematic) attack interfering with IT services/processes e) **Vulnerability Alert/Report** – Uncorrected vulnerability is detected or suspected on systems that exposes system to MEDIUM severity attacks
LOW	a) **Malicious Code Attacks/Alerts** • anti-virus software is effective • Alert received about new malicious code posing LOW risk • Inbound infected file or E-Mail blocked by the firewall or gateway • Infection that is readily detected and cleaned by the anti-virus software b) **Hacking Attack** • General/routine low-level network scans/reconnaissance of the network perimeter • Isolated penetration attempts by a single attacker that are unsuccessful c) **Unauthorised Access** – Unsuccessful attempt by an authorized user to misuse general access to systems or sensitive information d) **Denial of Service** • Unsuccessful attempted attack • SPAM blocked by the firewall or gateway e) **Vulnerability Alert/Report** – Alert received about a vulnerability that: • is known to have been corrected on the systems; or • is not relevant to City of Toronto (i.e. related to IT systems not used by City of Toronto).

APPENDIX D: Application User Roles

1) **Hosting Administrators** – Hosting Administrators are specific to Application and database servers managed by Scytl.

2) **Election Administrators** - Are City of Toronto resources that have full access and control to the City of Toronto Organizational structure within Election Services Division

APPENDIX E: Minimum Requirement for Access Control and Authentication to Back Office (System Administration)

Listed below are some industry standards and best practices for user ID and password management:

- No indication of ID and password requirements on screen
- Password length of at least 8 characters
- No echoing or storage of passwords in clear text
- System forced password expiry
- Reuse of passwords prohibited for at least 10 changes
- Re-authentication after communications or system failure
- User IDs and passwords disabled after a period of disuse

The above should be considered as the minimum requirement for access control and authentication. Adopting additional measures to strengthen the practice will be strongly encouraged.

APPENDIX F: Operational Security Requirement Check List

1. Physical Security Requirement

1) Maintain the physical security of the operating environment

2) Put in place appropriate procedures to ensure that the responsibilities for the maintenance of a secure operating environment are properly allocated and discharged

3) Ensure that adequate procedures are in place for the physical protection of the service equipment. This must as a minimum cover:
   - Intruders
   - Fire
   - Water
   - Environmental (such as: storms)
   - Physical damage (accident)
   - Physical damage (deliberate)

4) Implement physical and environmental controls to protect the service commensurate with the level of risk. The following minimum standards are to be implemented in any accommodation of the service equipment:
   - Equipment to be housed in unoccupied areas
   - Equipment area to be physically secured with controlled access
   - hand held fire extinguishers easily accessible
   - Automatic fire suppression equipment in place
   - Appropriate fire detection equipment installed
   - Smoke detection equipment installed
   - Water detection equipment as appropriate
   - Appropriate power supply cleanliness and contingency
   - Appropriate environmental controls
   - Appropriate regular cleaning regime
   - Cables properly managed
   - Cables properly labelled
   - Telephone with emergency numbers prominently displayed
   - Contingency Plan initiation sequence prominently displayed
   - Location of backup media prominently displayed close to associated equipment

2. Destruction of time expired, faulty or failed media

1) The Vendor must ensure that its staff understand the sensitivity associated with all media within the service and put in place appropriate procedures for its secure destruction in case of a fault, failure or life expiry

3. Secure system and network configurations

1) The Vendor must ensure that all systems that make up the service are configured in accordance with a recognized standard for operating system security

4. Control of access to the systems and networks to limit the incidences

1) The Vendor must have control in place to limit, as a minimum, the following incidences:

- Unauthorized access to organization systems
- Interference with network components
- Performance degradation across the network
- Interference with network traffic

5. Logging and monitoring of events

1) The Vendor must consider having a process in place to, as a minimum, monitor and log the following:

- Legitimate access
- Authentication exceptions
- Authority exceptions
- Privilege changes
- Data object owner changes
- Export of information
- Out of hours access

6. Adequate documentation

1) To enable proper delivery of the service, the provider must maintain, as the minimum, the following documentation:

- Scytl Technology Overview

7. Appropriate management of personnel

1) The Vendor must have procedure in place to manage the following personnel issues relating to information risk management:

- dismissal
- resignation
- termination
- transfer

2) The Vendor must ensure staff and subcontractor have an understanding of information risk management threats and concerns relating to the outsourced arrangement and of relevant information risk management policies

3) The Vendor's Staff assigned to the outsourced arrangement must be made aware of the City's requirements, expectations related to the security and privacy of the data

4) The Vendor's Staff assigned to the outsourced arrangement must receive training and regular updates on relevant information risk management policies and procedures

8. Appropriate procedures for dealing with malicious software

1) The Vendor must put in place appropriate checking and elimination procedures to ensure that the service is not affected by viruses during development, maintenance and operation

9. Notification and management of changes

1) The Vendor must have procedure to notify the City of any changes that may affect the environment of the outsourcing arrangement

2) The Vendor must have process for managing changes to the outsourcing arrangement

3) The Vendor must have process for testing changes

4) The Vendor must successfully test all changes before implementation

10. Management of test data

1) The Vendor must demonstrate that its testing regime is able to adequately manage test data

2) The Vendor shall not use City production data for testing purposes.

3) If the use of production information is essential to the successful implementation of the service, the Vendor must have process to seek City's approval and implement adequate procedures to manage the data appropriately. Not withstand to the approval from the City, the Vendor must manage the data in compliant with the regulatory / legislative requirements.

APPENDIX G: Privacy Breach Protocol

City of Toronto Third Party Privacy Breach Protocol

Background

1) It is a legal requirement under Section 1(b) of *MFIPPA* that the personal information collected and used by the institution is safeguarded against inappropriate and/or negligent disclosure.

2) Personal information is recorded information about an identifiable individual.

3) Examples of personal information may include: a person's name along with a photograph, phone number, driver's license, address, payroll number, or social insurance number.

4) The City of Toronto Privacy Breach Protocol outlines the process to be followed in the event of a privacy breach.

Privacy Breach

1) A privacy breach is any instance where an institution, intentionally or unintentionally, unlawfully discloses of personal information or records containing personal information. Examples can include the loss or theft of a lap top computer, mailing sensitive information to the wrong address, or disclosing personal information over the telephone without the appropriate consent in place.

2) Privacy breaches undermine public trust in the City and can result in significant harm to the institution and the public.

3) Responding to a privacy breach immediately and aggressively is the highest priority for City staff.

Six Steps

When a privacy breach happens, the following protocol shall serve as guidance in all applicable privacy breach instances:

- Confirm
- Contain
- Contact
- Investigate
- Document
- Mitigate

Step 1: Confirm

Upon discovering that a privacy breach has occurred, the following steps will need to be taken by divisional staff as soon as possible.

☐ 1. Confirm the occurrence of a privacy breach communicate the same to the Appointed Security/Privacy Contact (S/P C)

☐ 2. Determine if personal information or personal health information was disclosed.

☐ 3. Determine if the breach is an on-going concern or if the breach was a single occurrence.

☐ 4. The S/P C will be responsible for:

- All documentation of the particulars of the incident
- Contacting appropriate stakeholders
- Coordinating the reporting of specifics relating to the incident by unit/division staff
- Providing division policies and case files relating to the incident
- Being the point of contact for any mitigation strategies developed in response to the circumstances of the breach
- Suspending any processes deemed to be responsible for the breach if on-going

The purpose of the confirmation step is to begin to assign responsibilities so that the rest of the breach protocol may be followed in timely and complete manner.

Step 2: Contain

The S/PC must immediately:

☐ 5. Secure any evidence or documentation relating to the specific circumstances of the breach

☐ 6. If possible, the Vendor Security/Privacy Contact should immediately move to retrieve any documentation that has been disclosed inappropriately with all actions documented.

☐ 7. Suspend any process that caused the privacy breach if this behaviour is on going. This may include the following:

- Changing passwords/codes
- Shutting down computers affected
- Suspending mailings
- Immediately meeting with staff to provide instruction

In cases where the occurrence is a single unrepeated error (a stolen device or single mailing) – all policies relating to the occurrence will need to be reviewed in cases where the breach is as a result of an on-going practice, operations involved in the privacy breach will be suspended until it is resolved.

Step 3: Contact:

The vendor will need to contact appropriate staff as soon as possible upon confirmation of a breach and not to exceed 24 hours after detection and confirmation, to inform them of the breach.

☐ 8. Contact the City Security/Privacy Contact

☐ 9. Contact the Corporate Information Management Services

☐ 10. Appropriate SP and City Management

The stakeholders should meet or arrange a teleconference at the soonest opportunity to discuss response strategy and mitigation. Additionally this Privacy Breach Response Team (PBRT) will need to determine if secondary contacts should be implemented prior to proceeding with the investigation. In case of theft of equipment, break in or other criminal action including misuse or theft by an employee:

☐ 11. Contact Police and file a report

Secondary contacts may include:

☐ 12. Legal Services Division

☐ 13. Communications Division

☐ 14. District or Unit Management

☐ 15. Other Stakeholders

The PBRT and any additional staff will need to be notified of all particulars relating to the incident and the DC will need to have a detailed record of the occurrence and the steps taken to that point arranged chronologically using the attached briefing note template.

In most cases the breach will need to be reported to the Information and Privacy Commissioner (IPC) of Ontario. The CIMS office will be the **only** point of contact for this notification. Under no circumstances should the Security/ Privacy Contact or any other member of the division or SP contact the IPC.

Step 4: Investigate:

The PBRT should be informed of all polices/procedures or staff actions that precipitated the privacy breach. These should be used to develop the mitigation of the breach to be undertaken by the area. Breaches that are reported to the IPC will require a detailed submission including the above information. Assigning these responsibilities is integral to successfully mitigating the breach and preventing recurrence of the circumstances responsible for it.

The Corporate Information Management Services liaison will be responsible for assisting the DC in investigating the breach.

☐ 16. Interview staff and collect statements

☐ 17. Collect all policies, procedures and guidelines involved in the circumstances that led to the breach.

☐ 18. Disclose any previous breaches

☐ 19. Review staff training and responsibilities involved in the breach.

☐ 20. Review/ Examine any audit functions or evidence that can provide detail regarding the breach.

Step 5: Document:

☐ 21. Using the attached briefing note the City and the Vendor S/PC will collaboratively collect and arrange all information pertaining to the privacy breach. This information will include:

- The date, time, place and material involved in the breach
- A chronology of steps including notice
- Staff identified by position in the body of the briefing note with an appendix listing the names and positions mentioned in the note itself
- The scope of the breach—the number of individual records involved
- The nature and sensitivity of the information disclosed
- Any policies or procedures responsible for the breach
- Any attempts at mitigation undertaken to-date

Attach any additional documentation as an appendix to the Privacy Breach Briefing Note.

Step 6: Mitigation

Upon completion of the investigation and documentation, the PBRT should meet to discuss mitigation strategies.

☐ 22. Identify foreseeable harms that are likely to result from the breach.

☐ 23. List the individuals whose privacy has been breached along with contact information.

☐ 24. Prepare notification of the individuals via mail or other method.

☐ 25. Discuss potential follow-up strategies implemented post notification. (Examples may include a temporary information number to answer further questions, a press release, FAQ, or guidelines and resources for individuals worried about identity theft.)

☐ 26. Determine the final disposition of the breached material.

☐ 27. Review policies and implement staff training.

☐ 28. Prepare any notification or breach submission to the Information and Privacy Commissioner.

In cases where the IPC has been notified of the breach, all mitigation strategies will need to be detailed in the official submission. This submission will be completed by the Corporate Information Management Services and circulated to the stakeholders for review prior to submission.

Privacy breaches are a very serious matter. The City of Toronto privacy breach protocol will minimize and mitigate the potential harms resulting from them.

Prepared by: John Searle (jsearle@toronto.ca) 416-397-5215
Corporate Information Management Services
March 1, 2011

Privacy Breach Briefing Note

Date of Privacy Breach:

Date Reported to CAP/ PBRT:

CAP Representative's Name:

Division and Section Name:

Division Contact's Name:
Position Title:
Address:
Telephone Number:
Email address:

Summary of privacy breach (who, what, when, where, why and how):

Was a third-party involved (e.g. an organization providing services under contract with the City)?

Summary of Issue and Action Taken:

Investigation details:

Containment Efforts (what efforts (if any) were made to control the breach):

Consultation with Corporate Information Management Services (CAP) Representative

Future Action/Follow Up:
Staff Members Directly Involved:

- Scytl Incident management team creates and maintains a log file (date, time, and source) to identify every piece of information related to the event.

- Scytl should contain or mitigate the damage to assets and date.

APPENDIX H: ADDITIONAL PRIVACY PROTECTION REQUIREMENTS

1.0 Definitions

In this Appendix:

1) "access" means disclosure by the provision of access;

2) "Act" means the Municipal Freedom of Information and Protection of Privacy Act (Ontario, Canada), as amended from time to time;

3) "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

4) "personal information" means recorded information about an identifiable individual, other than contact information, collected or created by the Vendor as a result of the Agreement or any previous agreement between the City of Toronto and the Vendor dealing with the same subject matter as the Agreement but excluding any such information that, if this Appendix did not apply to it, would not be under the “control of a public body” within the meaning of the Act.

2.0 Purpose

The purpose of this Appendix is to:

1) Enable the City to comply with its statutory obligations under the Act with respect to personal information; and
2) Ensure that, as a service provider, the Vendor is aware of and complies with its statutory obligations under the Act with respect to personal information.

3.0 Collection of personal information

1) Unless the Agreement otherwise specifies or the City otherwise directs in writing, the Vendor may only collect or create personal information that is necessary for the performance of the Vendor’s obligations, or the exercise of the Vendor’s rights, under the Agreement.
2) Unless the Agreement otherwise specifies or the City otherwise directs in writing, the Vendor must collect personal information directly from the individual the information is about. Under this Agreement, the Vendor will not be collecting personal information from individuals.

4.0 Accuracy of personal information

1) The City must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Vendor or the City to make a decision that directly affects the individual the information is about.

5.0 Requests for access to personal information

1) If the Vendor receives a request for access to personal information from a person other than the City of Toronto's representatives Aaron Pun, James Lam or Michelle Poirier, the Vendor must promptly advise the person to make the request to the Manager of Corporate Learning and Leadership Development, Aaron Pun or the City of Toronto's Corporate Information Management Services.

6.0 Correction of personal information

1) Within 5 business days of receiving a written direction from the City to correct or annotate any personal information, the Vendor must annotate or correct the information in accordance with the direction.

2) When issuing a written direction to correct personal information under section 36(2), the City must advise the Vendor of the date the correction request to which the direction relates was received by the City in order that the Vendor may comply with section 25(2) of the Act.

3) Within 5 business days of correcting or annotating any personal information under section 36(2), the Vendor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the City, the Vendor disclosed the information being corrected or annotated.

4) If the Vendor receives a request for correction of personal information from a person other than the City, the Vendor must promptly advise the person to make the request to the City and, if the City has advised the Vendor of the name or title and contact information of an official to whom such requests are to be made, the Vendor must also promptly provide that official's name or title and contact information to the person making the request.

7.0 Protection of personal information

1) The Vendor must guard against such risks as unauthorized access, collection, use, disclosure or disposal of personal information, including any personal information expressly identified in the Agreement. Upon request, the Vendor must provide to the City of Toronto's Manager of Risk Management and Information Security, evidence from a reputable security expert (or SSAE16 report) documented proof of system integrity and security.

8.0 Storage and access to personal information

1) Unless the City of Toronto otherwise directs in writing, the Vendor must not store personal information outside of Canada or permit access to personal information from outside Canada, except to Scytl staff in the United States for the purpose of providing support.

9.0 Retention of personal information

1) Unless the Agreement otherwise specifies, the Vendor must retain personal information until directed by the City of Toronto in writing to dispose of it or deliver it as specified in the direction.

10.0 Use of personal information

1) Unless the City otherwise directs in writing, the Vendor may only use personal information if that use is for the performance of the Vendor's obligations, or to exercise the Vendor's rights, under the Agreement.

11.0 Disclosure of personal information

1) Unless the City otherwise directs in writing, the Vendor may only disclose personal information inside Canada to any person other than the City if the disclosure is for the performance of the Vendor's obligations, or the exercise of the Vendor's rights, under the Agreement.

2) Unless the Agreement otherwise specifies or the City otherwise directs in writing, the Vendor must not disclose personal information outside Canada.

12.0 Notice of foreign demands for disclosure

The Vendor is obligated to provide prompt notification to the City, if in relation to personal information in its custody or under its control the Vendor:

1) receives a foreign demand for disclosure;

2) receives a request to disclose, produce or provide access that the Vendor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or

3) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

13.0 Notice of unauthorized disclosure

In the event of a privacy breach, the Vendor must notify the City within 24 (twenty-four) hours of discovery with confirmation and the Vendor will take immediate action upon receiving a decision from the City's Corporate Information Management Services or the Information and Privacy Commissioner of Ontario regarding an unlawful disclosure of personal information in its custody or under its control.

14.0 Inspection of personal information

In addition to any other rights of inspection the City may have under the Agreement or under statute, if a privacy breach occurs, the City may, at a time and in a manner to be reasonably agreed (on reasonable notice to the Vendor), enter on the Vendor's premises to inspect any personal information in the possession of the Vendor or any of the Vendor's information management policies or practices relevant to its management of personal information or its compliance with this Appendix and the Vendor must permit, and provide reasonable assistance to, any such inspection. In the cases of "18-Notice of unauthorized disclosure", the Vendor will make available all information relating to the breach, per Section 18. The City reserves the right to send City personnel to the Vendor's site to perform a review, with all costs incurred borne by the Vendor.

15.0 Compliance with the Act and directions

The Vendor must in relation to personal information comply with:

1) The requirements of the Act applicable to the Vendor as a service provider, including any applicable order of the Information and Privacy Commissioner / Ontario under the Act; and

2) Any direction given by the City pursuant to this Appendix.

The Vendor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

16.0 Notice of non-compliance

If for any reason the Vendor knows that it does not comply, or anticipates that it will be unable to comply, with a provision in this Appendix in any respect having a detrimental impact on the security of the City's data, the Vendor must promptly notify the City of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

17.0 Termination of Agreement

In addition to any other rights of termination which the City may have under the Agreement or otherwise at law, the City may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Vendor, terminate the Agreement by giving written notice of such termination to the Vendor, upon any failure of the Vendor to comply with this Appendix in a material respect.

18.0 Interpretation

1) Any reference to the “Vendor” in this Appendix includes any subcontractor or agent retained by the Vendor to perform obligations under the Agreement and the Vendor must ensure that any such subcontractors and agents comply with this Appendix.

2) The obligations of the Vendor in this Appendix will survive the termination of the Agreement.

3) If a provision of the Agreement (including any direction given by the City under this Appendix) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

4) The Vendor must comply with the provisions of this Appendix despite any conflicting provision of this Agreement

5) Nothing in this Appendix requires the Vendor to contravene the law of any jurisdiction outside Canada.

SCHEDULE "O"
ESCROW PROVISIONS

(1) At the time of signing the Agreement, or at a time agreed between the parties, Licensor shall deposit an enabled source code version of the Software with all necessary passwords, software keys, or authorization strings (the “Source Code”) with the escrow holder (the “Escrow Holder’). Licensor shall update the Source Code with all new releases and updates and with any bug fixes or workarounds provided to Licensee. The annual escrow fees shall be borne entirely by Licensee. The escrow agreement for the Source Code deposit shall name Licensee as beneficiary and at a minimum shall provide for the release of the Source Code to Licensee upon the occurrence of any of the following release conditions (“Release Conditions”):

a) Any dissolution or liquidation proceeding is commenced by or against Licensor, and if such case or proceeding is not commenced by Licensor, it is not dismissed within sixty (60) days from the filing thereof; or

b) Licensor becomes insolvent or admits its inability to or fails to pay its debts generally as they become due; if any proceedings are commenced or taken for the dissolution, liquidation or winding up of Licensor; or if a trustee, custodian or other person with similar powers is appointed in respect of Licensor or in respect of all or a substantial portion of its property or assets; or if Licensor ceases to carry on all or substantially all of its business; or if any proceedings involving Licensor involving its bankruptcy or insolvency are taken under any legislation dealing with insolvency are taken under any legislation dealing with creditor’s rights; or Licensor makes any assignment or proposal in bankruptcy or any other assignment or proposal for the benefit of creditors, or

c) Licensor is in breach of its obligations:
   i) To provide support in accordance with this Agreement, or
   ii) To provide the Software to Licensee without infringing a third-party’s intellectual property rights,

   Licensor shall have a thirty (30) day cure period to rectify any of the foregoing Release Conditions after the receipt of a written notice from Licensee. Where there is a dispute regarding the existence or occurrence of a triggering event for a Release Condition, the Software shall be immediately released to Licensee, and the parties shall resolve any dispute as to the existence of the conditions required to release the escrow material in accordance with the dispute resolution provisions of the Agreement.

(2) Upon the release of the Source Code to Licensee, Licensee shall only use the Source Code in accordance with this Agreement and shall only use the Source Code internally or with Users for the purpose of providing maintenance, and support for, or to add functionality to the Software. Subject to the terms and conditions of this Agreement, Licensee’s contractors shall have the same limited

rights to use the Source Code as are granted to Licensee under this Section, provided that no more than three unrelated contractors will be utilizing the Source Code simultaneously. All contractors shall comply with the terms and conditions of this Agreement when working with or assessing the Source Code.

(3) Licensor represents, warrants and covenants that the Source Code, and all new releases, updates, bug fixes and workarounds deposited into escrow shall include all documentation and materials necessary for a competent programmer to compile, verify, maintain, and support the Source Code, and all without undue effort, and that no Licensor proprietary software is required to maintain and support the Source Code.

(4) Licensor shall, upon notice from Licensee, carry out such tasks in order to verify that the escrowed materials are complete and functional and shall provide written proof of such verification to Licensee.