

## 1.0 Scope of Work and Associated Deliverables

- 1.1 The Successful Bidder shall provide Project Management, design and coordination of all Work on the systems within this contract, and maintain all required communications between various City of Toronto divisions and third party service providers.
- 1.2 The Successful Bidder shall be the single point of contact and shall be responsible for all coordination of Work that pertains to the Systems, along with all required coordination and communications between Personnel and the City.
- 1.3 The Successful Bidder shall be in good standing with all manufacturers referenced in this RFQ (including but not limited to American Dynamics, Dedicated Micros, Milestones and Axis) and must have and maintain all up to date certifications.

## 2.0 Literature

Bidders, where applicable, should submit complete literature on all products being included in their quotation including, but not limited to, standard manufacturer's warranty, model numbers, part numbers and other relevant documentation as part of their Quotation.

## 3.0 Bidder Qualifications

- 3.1 Bidders must be authorized sellers or resellers for the Products listed section 33.0 Manufactures List and must hold title to any equipment that will be installed or removed. If requested by the City, Bidders must submit written verification of current and valid authorization, satisfactory to the City, prior to Award. Failure to submit written verification of authorization, satisfactory to the City within a time frame specified by the City will result in the Quotation being declared Non-Compliant.
- 3.2 Prior to award, if requested by the City, the Bidder must submit written verification that their technicians are certified and authorized to undertake the installation and delivery services described in this RFQ. Failure to submit written verification of certification/authorization satisfactory to the City within a timeframe specified by the City will result in the Quotation being declared Non-Compliant.

Bidders must provide within five (5) business days of such a request, a copy of each person's resume and certifications for proof of meeting the requirements listed in each Mandatory Criteria. Failure to provide this information within the timeframe specified, will result in non-compliance and the Bidder's Quotation will not be considered further.

- 3.3 All Certificates must be valid at the time of submission and throughout the duration of this contract.

### 3.4 Mandatory Criteria 1:

- Bidders must maintain personal with the minimum years' experience Personnel as indicated that meet the mandatory criteria in Table 1 below:

**Table 1**

Item Number	Years of Experience	Certification and or Training on the following systems
<b>CCTV</b>		
1.1	3	Milestone Certified Design Engineer
1.2	3	Milestone Certified Integration Technician
1.3	3	BriefCam
	3	Victor and VideoEdge Advance Installer
<b>DSC</b>		
1.4	3	Power Series 1864 System
1.5	3	DSC Power Neo Alarm Panels
<b>ACS</b>		
1.6	3	Visonic – PowerMaster 10/30
1.7	3	Key Tracer
1.8	3	Software House - CCURE 9000 Level 2

- During the Term of the Contract, the Successful Bidder may substitute Personnel due to staff changes with Personnel of equal or greater qualifications and experience. Any change of Personnel shall be approved by the City prior to the substitution taking place.

#### 3.4.0 All systems components and installation shall conform to the following standards and codes where appropriate:

- Manufacturing: ISO 9003
- Design: MIL 275E
- Communications: IEEE RS232C and RS485
- EMI emissions: FCC part 15
- Electrostatic immunity: IEC 801.2 level 4
- AC transients UL 964
- National Building Code
- Ontario Fire Code
- Electrical Standards Authority
- Process Control System Implementation Manual
- NFPA 730 & 731
- ULC 319/S304
- UL 1981 Central Station Automation System
- UL 681 Installation and Classification of Burglar and Hold up Alarm Systems
- UL1635 Digital Alarm Communicator System Units

## 4.0 Security Clearance Requirements

- 4.1 A Clearance Letter from Toronto Police Service is a formal document produced on secure paper indicating that the subject of the inquiry has no criminal convictions in the National Repository of Criminal Records, which is maintained by the RCMP. The Successful Bidder shall provide within fifteen (15) business days after contract award to the Project Manager, a Police "Clearance Letter", obtained within the past three (3) months for each person (including Subcontractors), that may be expected and/or will be performing Work under this contract.
- 4.2 The Successful Bidder's employees (including Subcontractors) that may be expected and/or will be performing Work under this contract shall not pose a foreseeable security concern or hazard to the City as it relates to the protection of its assets.
- 4.3 Unless authorized in writing by the Project Manager, only Personnel that provided a Clearance Letter to the Project Manager shall be permitted to Work under this contract.
- 4.4 The Successful Bidder shall provide an original recent (obtained within the past 3 months) Clearance Letter only. No copies will be accepted.
- 4.5 The cost for each of the Clearance Letters shall be the complete responsibility of the Successful Bidder.
- 4.6 Refer to the Supplementary Forms and Policies section

## 5.0 Specifications

### 5.1 Meeting

- 5.1.0 A kick-off meeting will be scheduled by the Project Manager with the Successful Bidder upon award to review the roles and responsibilities of the City and the Successful Bidder.
- 5.1.1 The Successful Bidder and their qualified Personnel (including Subcontractors) assigned to this contract shall attend the kick-off meeting if requested by the Project Manager.
- 5.1.2 The Successful Bidder's Project Coordinator (or designate) shall be responsible to coordinate, plan and schedule as many subsequent meetings as necessary throughout the Term of the contract to ensure effective project stakeholder communication.
- 5.1.3 All meetings shall be held within the City of Toronto. The Successful Bidder is responsible for all costs for consultation and project/subsequent meetings.

- 5.1.4 The City reserves the right to request subsequent meetings on-demand or on short notice and may change or cancel meetings at the discretion of the Project Manager and at no cost to the City.

## 5.2 Resource Commitments

- 5.2.0 The Successful Bidder is the Design/Builder on Record and must continue to meet all of the requirements of Systems certifications and qualifications with respect to training and staffing competency, at the sole expense of the Successful Bidder, throughout the Term of the Contract, for all of the systems and components installed and in use at the facilities.
- 5.2.1 The Successful Bidder must continue to meet all of the mandatory conditions of the Warranty throughout the Term of the contract and Warranty periods.
- 5.2.2 The Successful Bidder must be able to provide the necessary materials, tools, machinery and supplies to carry out all approved Work. These resources must be available at the sole responsibility of the Successful Bidder on a dedicated basis throughout the term of the contract, to coordinate and carry out all approved Work with due care, skill and efficiency. The City may request removal and replacement within five (5) calendar days of any Contract Leads at any time throughout the duration of the contract.
- 5.2.3 The Successful Bidder must guarantee to the City that their Services and performance, including those of the Subcontractor, shall be provided in a professional, good, workmanlike manner and comply with, but not be limited to the City's City-Wide Security Policy, Workplace Violence Policy and the City of Toronto's Security Video Surveillance Policy. Those deemed not complying, at the discretion of the City, will be removed from the site and all future projects for the duration of this contract. The Successful Bidder will be provided three (3) notices of non-compliance and then be in breach of this contract, which may include contract termination as per the City of Toronto policy and guidelines.
- 5.2.4 Only Personnel listed and registered with the City will be permitted to access and Work on City of Toronto sites.

## 5.3 Cleaning

- 5.3.0 The Successful Bidder must maintain the worksite, grounds, and building free from accumulations of waste material and rubbish, and provide on-site containers for collection of waste materials and rubbish as required. On site storage areas must be coordinated through and arranged by the City. Cleaning and disposal operations must comply with local ordinances and anti-pollution laws.

- 5.3.1 The Successful Bidder must clean dust and water residue from core drilling, cutting and patching of masonry, and drywall to satisfaction of the City. Furnishings, floors and finishes must be protected prior to the commencement of Work.
- 5.3.2 Promptly as Work proceeds, and upon completion, the Successful Bidder and each of its Subcontractors shall clean up and remove from the premises all rubbish, dirt, dust, debris and surplus materials resulting from the Work.
- 5.3.3 The Successful Bidder must at all times be considerate of site security and ensure all worksites are maintained accordingly.

#### 5.4 Cosmetics, Protection, and Finishes

- 5.4.0 The same tamper proof screws and fasteners shall be used on all equipment, enclosures, cabinets and materials in public areas. Corporate Security shall be provided two sets of tools (at no charge) which are required to service security equipment that have tamper proof screws and fasteners.
- 5.4.1 Finishes and graphics for all equipment in public areas shall be submitted to, and approved by the City.
- 5.4.2 The Successful Bidder shall be responsible for all cutting, core drilling, and patching required for the installation of this Work. Where alterations occur or new and existing Work is required, the Successful Bidder shall join, cut, remove, patch, repair, or finish the adjacent surfaces as required to meet same or better quality at no extra costs to the City.
- 5.4.3 Any Work likely to alter or detract from the original appearance must not commence without the City's written consent. Changes or alterations, completed without the City's consent, may be subject to restoration by the Successful Bidder. Any additional repairs required, due to unapproved Work, may be billed to the Successful Bidder for payment.
- 5.4.4 The Successful Bidder shall protect existing furnishings by providing and maintaining adequate temporary protective coverings.
- 5.4.5 The Successful Bidder shall provide and maintain adequate fire safety in accordance with applicable fire code and Regulations.
- 5.4.6 The Successful Bidder shall be responsible for any damage to existing structure or contents arising from a lack of adequate protection.
- 5.4.7 All Work shall be performed by a qualified and skilled trade's people as defined by the Occupational Health and Safety Act, Regulation 213/91 and all finishing shall be of the highest

quality. Construction and finishing techniques must preserve the original appearance of the affected areas.

- 5.4.8 Unless authorized in writing by the City, the Successful Bidder shall not post/affix any stickers, labels, signs, logos, or any kind of promotional or advertising material on any equipment or instruments, nor at any City of Toronto site. This includes decals warning of systems in use or Services provided.
- 5.4.9 All materials, accessories, special equipment, services, personnel, test equipment and tools required for installation of the equipment shall be provided by the Successful Bidder.

## 5.5 Codes, Permits, Fees and Inspection

- 5.5.0 All system components shall be installed according to manufacturer's instructions and in a professional manner. Workmanship and care must encompass all aspects of the task being performed so the full intent of the project may be realized.
- 5.5.1 All Work shall be performed in compliance with all applicable Regulations, Building Codes and Local By-laws.
- 5.5.2 The Successful Bidder shall be responsible for all work and material including, but not limited to surveying, scanning, soil sampling, stamped engineered drawings, cutting, core drilling, patching, trenching, excavating, temporary storage of material, laying of conduits and backfilling for the installation of assigned Work.
- 5.5.3 The Successful Bidder shall arrange for inspection of all Work by the authorities having jurisdiction over the Work. The Successful Bidder shall comply with the requirements of the authorities, federal, provincial and municipal Codes, and all other authorities having jurisdiction. These Codes and Regulations constitute an integral part of these specifications. In case of conflict, the applicable Code takes precedence over the RFQ document.
- 5.5.4 All Work shall be executed to the approval of the City. When the Work is reported to be complete, an inspection shall be made by the City, and all deficiencies found shall be corrected by the Successful Bidder within 30 calendar days of reporting the deficiency, and before the final payment is made.
- 5.5.5 The City may appoint and pay for an independent consultant to inspect the Work or to carry out specific tests as the Work progresses. The Successful Bidder shall notify the City and the consultant at least three calendar days prior to starting the Work, and shall provide any assistance that the consultant may require to carry out his/her inspections or tests at no additional cost to the City.

- 5.5.6 The consultant, if any, shall act on behalf of the City to ensure that the performance of the Work is carried out according to the specification, drawings and acceptable standard practice. The Successful Bidder shall co-operate with the consultant and shall comply with his/her directions in making good all deficiencies and defects, and in ensuring the proper execution of the Work.
- 5.5.7 The verification or acceptance of the Work by the consultant or the City does not relieve the Successful Bidder of his/her responsibility to comply with the specifications. Any Work subsequently discovered, which does not comply with the specifications shall be rectified by the Successful Bidder at no cost to the City.

## 5.6 Daily Check In/Out

- 5.6.0 Before Work commences, the Successful Bidder shall have already incorporated all site and facility constraints as it relates to on site access time and Work performance limitations.
- 5.6.1 Before commencing Work and prior to completion of any Work, the Successful Bidder's Personnel must check-in and out daily with the City of Toronto Security Control Centre at 416-397-0000, and if available with on-site Security.
- 5.6.2 Upon check-in and check-out, the Successful Bidder's Personnel shall clearly explain what effects their Work will have on current security systems or VSS that are being monitored, and they shall identify any anticipated alarm signals, as well as any system functional limitations.

## 5.7 Disruptions to City Operations

- 5.7.0 Careful consideration must be given at all times to the function of the facility and the persons contained. The Successful Bidder must make all attempts to cause as little disruption in service as possible when providing installation services. Work that may cause any type of major disruption to building operations and/or building occupants must first be cleared by the City, and may have to be completed after hours.
- 5.7.1 The Successful Bidder shall co-ordinate all Work with the City's representative to ensure minimum disruption of service.
- 5.7.2 Work shall be executed to minimize the impact or the disruption of the existing operational systems and City of Toronto facility operations. At any time during the performance of the Work, if the existing, operational systems are affected beyond the expectation approved through the Implementation Plan or there is an imminent danger to be affected beyond the approved expectation, the Successful Bidder shall stop Work and minimize the impact on the operational systems. The Successful Bidder shall immediately inform a City of Toronto Corporate Security representative. The Successful Bidder shall perform all Work to implement a temporary solution to enable 100% functionality for operational systems. The Successful Bidder is to

proceed with permanent Work only after a solution is approved by City of Toronto Corporate Security.

## 5.8 Impact on City of Toronto Operations

- 5.8.0 Operational restrictions may affect the scheduling of Work and may require some activities to be scheduled at night, during weekends, or during periods when facilities are not in service.
- 5.8.1 The Successful Bidder shall perform the Work in a manner to prevent disruption of normal City of Toronto operations. Any task that may cause disruption of operations shall be approved in advance by City of Toronto Corporate Security.

## 5.9 Inspection of Work

- 5.9.0 City of Toronto Corporate Security reserves the right to inspect any and all Work and reserves the right to be present during the performance of any Work under this Contract.
- 5.9.1 City of Toronto Corporate Security will perform periodical and statistical inspections of the Work. The Successful Bidder shall provide and facilitate access to Work for inspection.
- 5.9.2 The Successful Bidder shall correct within a maximum of one week (7 calendar days) any Work deemed not satisfactory by the City of Toronto.
- 5.9.3 In the event that the Successful Bidder does not correct the Work within the time frame specified, the City reserves the right to have the Work completed by another qualified firm at the Successful Bidders expense.

## 5.10 Occupancy Before Completion

The City may use portions of the Work although the same may not be entirely complete without claim of any kind by the Successful Bidder so doing, nor shall any such use relieve the Successful bidder from his/her obligation under this contract until the termination of the guarantee/Warranty period.

## 5.11 Monitoring/Programming

Many of the inspected devices require confirmation of device annunciation on the monitoring screen. Personnel must arrange/coordinate with the Corporate Security Lead to change a given device's armed, controlled or online status. Personnel must ensure the previous state is restored upon completion of the inspection testing.

## 5.12 Equipment, Placement, Relocation, Removal, or Expansion

- 5.12.0 Some existing hardware may require removal or relocation for installation of new devices. In each instance, the Successful Bidder must advise Corporate Security, and the Successful Bidder must receive written approval prior to the removal or relocation. All costs associated with the removal or relocation are the sole responsibility of the Successful Bidder.
- 5.12.1 All placements of security devices are subject to approval by Corporate Security before final acceptance is granted.
- 5.12.2 All equipment and devices, removed by the Successful Bidder for replacement or placement of a new security device, shall remain the property of the City and shall be submitted to the City upon device removal.

## 5.13 Design and Installation

- 5.13.0 The Successful Bidder is responsible to provide a fully functional system meeting the City's standards as required by this RFQ.
- 5.13.1 The Successful Bidder shall be the design builder required to supply and/or install fully functional integrated, Security System for the City of Toronto. The Successful Bidder shall be solely responsible for its design errors or omissions. Including, but not limited to situations where all the necessary materials to deliver a fully functional integrated CCTV and AV system have been missed. This clause shall not apply where the City requests a change to the original design request. The Successful Bidder shall be solely responsible for detailed design, project management, coordination, equipment procurement, installation, component wiring, terminations, connections, labelling, programming, integration, testing, commissioning and as-built drawings of all Systems.
- 5.13.2 The Successful Bidder shall supply and/or install all required Systems electronic equipment, hardware, software, licenses and connections, to allow for City required functionality under this RFQ.
- 5.13.3 The systems shall consist of field, infrastructure, and monitoring devices integrated to the access control and intercom systems necessary to provide a fully automated system to control authorized traffic in and out of controlled areas of City facilities.
- 5.13.4 The system shall be designed on a distributed processing architecture employing remote DGPs (Data Gathering Points) and operator workstations connected through TCP/IP and/or serial communication protocols, where applicable.

- 5.13.5 As part of this RFQ the Successful Bidder shall connect all devices to centrally located patch Panels and/or equipment located in communication rooms and /or DGP as detailed in the specification drawings and standards.
- 5.13.6 Connectivity from the IP equipment shall be based on Ethernet IP based protocols over a City supplied network, which shall connect and be programmed to servers and remote client workstations.
- 5.13.7 The Successful Bidder shall provide all programming data required to achieve the specified functionality (this includes situations where existing technology is being replaced with new technology). Such programming shall include (but is not limited to) programming of all alarms, events, triggers, timers, objects transmitting and receiving signals and interfaces as well as programming of signal receiving centre equipment to provide 100% full functionality.
- 5.13.8 Any required expansion boards/nodes and ancillary equipment needed for a full operation of the system are the responsibility of the Successful Bidder.
- 5.13.9 The Successful Bidder shall provide power supplies with battery back-up to meet NFPA 731 standards for all Systems. Failure to meet the standard will result in the Successful Bidder providing all supplies necessary at no additional cost to the City.
- 5.13.10 The Successful Bidder shall be required to populate all items such as parts and equipment from supply and install projects into a City supplied Microsoft Office database file. Upon review and approval by the City, these database files will be imported into the City central physical asset and material management database.
- 5.13.11 The Successful Bidder is responsible for all final wiring and terminations of all Systems.
- 5.13.12 The Successful Bidder shall be responsible for ensuring all structured cabling and electrical including back boxes, cabling, conduit, troughs and raceways meet equipment electrical and wiring requirements throughout all phases of the project.
- 5.13.13 The Successful Bidder shall inspect conduit, cabling, back boxes, junction boxes associated with the Systems during installation and shall notify the City Project Manager of any issues found.
- 5.13.14 The Successful Bidder shall maintain integration to existing security systems to the maximum level supported by the systems manufacturers.
- 5.13.15 Test and commission according to the 32.0 Compliance with Standards.
- 5.13.16 The Successful Bidder shall review the current site conditions and existing system configurations.

- 5.13.17 The Successful Bidder shall provide at all times sufficient competent labour, materials, and equipment to properly carry on its Work and ensure completion of each part in accordance with the Work schedule and within the contractual time period.
- 5.13.18 All installation materials, accessories and special equipment, Services, Personnel, test equipment and tools required for installation of the equipment shall be provided by the Successful Bidder.
- 5.13.19 Equipment shall be installed as per the manufacturer's recommendations, programmed and integrated to City Standards and the City Project Manager.
- 5.13.20 The Successful Bidder shall secure and be responsible for the safe keeping and protection of the system equipment until the system is fully accepted by the City of Toronto after the commissioning process.
- 5.13.21 The Successful Bidder shall coordinate all network provisioning with City of Toronto IT Services.
- 5.13.22 The Successful Bidder shall start to warrant the Systems, warranty start date, when all deliverables such as as-builts of the project have been accepted by the City and deficiencies corrected.
- 5.13.23 The Successful Bidder shall maintain the System in compliance with manufacturer's specified Preventative Maintenance schedule during the project installation period.
- 5.13.24 The Successful Bidder is responsible for all System decommissioning and removal of equipment in this RFQ, at no additional cost to the City. Including all cable removal as per ESA requirements.
- 5.13.25 The Successful Bidder shall be responsible to investigate, design and integrate to new and existing Systems.
- 5.13.26 It is the responsibility of Successful Bidder to design and finalize the System wiring diagrams, drawings, documentation and schedules in order to meet site specific conditions and provide a fully functional system.
- 5.13.27 Integration and Analytic programming for items not listed in the contract are to be shown as separate line items in quote indicating the type of integration and/or analytic to be achieved and used for the remainder of the contract term.

## 7.0 Supply and Installation Project Submission Requirements

- 7.1 The Successful Bidder shall (at no additional charge) submit to the Project Manager one (1) set of electronic copies of the following: project quotation, detailed project schedule, shop drawings, as-builts, warranty, and any other related supporting documents as detailed in this RFQ.
- 7.2 All electronic documents submitted to COT must be named by purchase order, site name, document type, date, and Service Request Portal Number.
- 7.3 As directed by Toronto City Council in 2005 under the City's Waste Diversion Plan, where feasible and appropriate, all hardcopy prints will be double sided. Therefore the Successful Bidder will be required to comply with this plan as it relates to all hardcopy print contract documents.

## 8.0 Detailed Project Schedule

- 8.1 Detailed Project Schedules are to be free from error and submitted.
- 8.2 The detailed project schedule shall include, but not be limited to the following information:
  - Commencement date for each major activity;
  - The duration of each activity;
  - The proposed sequence of activities;
  - Dependencies between internal activities and milestone;
  - Dependencies between external activities and milestone; and,
- 8.3 The schedule shall be progressively updated as the project progresses, which enables the Project Manager to readily identify activities by location and resources.
- 8.4 The schedule information shall be sufficiently detailed to enable integration of all interface activities by the Project Manager.
- 8.5 The schedule shall be presented in daily segments and shall include the following at a minimum:
  - Site surveys (as required);
  - Service Request Portal Number;
  - Submission and approval of Shop drawings;
  - Shipping confirmation date;
  - Material delivery and installation;
  - Conduit and wire pulls completed;
  - Progress photographs (only of concealed work);
  - Panels and power supplies installed and programmed;
  - Field equipment terminated, mounted and tested;
  - Security testing complete;
  - Acceptance testing complete;
  - As-built documents;

- Equipment integration and dry-run;
- Monitoring period (minimum one week);
- Commissioning and hand-over.

8.6 The schedule shall be clearly identified with the following:

- Site name, if applicable and address;
- CRO number;
- Start date of the project with time;
- Project Coordinator name with detailed contact information; and,
- Subcontractor name; and
- Project completion date.

8.7 Distribute copies of any revised schedule to:

- Project Manager; and,
- Security Project Lead
- Other Stakeholders as indicated by the Project Manager.

8.8 The Successful Bidder shall be responsible for any delay in the progress of the Work, and it being understood that no such delay shall be an "Excusable Delay" for the purposes of extending the time for performance for the Work or entitling the Successful Bidder to additional compensation. The Successful Bidder shall take all necessary steps to avoid delay in the final completion of the Work without additional cost to the City of Toronto. The City shall not be responsible for any expense or liability resulting from any such delay.

## 9.0 Shop Drawings

9.1 Shop drawings prepared are to be free from error and submitted in electronic format. Shop drawings are to include all items quoted with no substitutions without the prior consent of the City Project Manager. All documents produced shall be the property of the City of Toronto and the Successful Bidder shall have no rights over the entire documentation package or any parts of the documentation package.

9.2 Shop Drawings shall include:

- Date and revision number;
- Project title and number;
- Service Request Portal Number;
- Contract Drawing / Specification Reference;
- Name and address of:
  - Subcontractor;

- Supplier, Manufacturer; and,
- Wiring diagrams for each location (including distances);
- Details of types of wire and conduit type and sizes;
- Particular model number of hardware;
- Dedicated circuit in electrical panel to be used (for new installations);
- Progress photographs (only of areas with concealed work);
- Panels and power supplies (location to be installed);
- Field equipment (location of mounting);
- All device programming names;
- Contractor's stamp, signed by Contractor's authorized representative certifying approval of submissions, verification of field measurements and compliance with Contract Documents.

9.3 The Project Manager may change any drawing to remove, add or relocate any device. The Successful Bidder shall make any changes in the shop drawings, which the Project Manager may require consistent with the Contract Documents and resubmit unless otherwise directed by the Project Manager. The Successful Bidder shall notify the Project Manager in writing of any revisions other than those requested by the Project Manager and are subject to approval by the City Project Manager.

## 10.0 Project Commencement

10.1 Prior to the commencement of installation the successful bidder will submit the following:

10.1.0 The Security Contractor shall submit to the Corporate Security Lead the required Active and Passive network equipment specifications for all locations in scope

10.1.1 The specifications and active network equipment shall be in compliance with the City Networking standard and based on Cisco active networking equipment.

10.1.2 The Security Contractor shall submit a network communication and bandwidth flow chart for the proposed system this shall include communication steps between the various VSS components operating in normal and failover modes and their respective estimated network bandwidth requirements

10.2 Near project closeout and before project site acceptance testing the security contractor shall submit the following draft documentation in electronic form to the COT Project Manager:

- Draft test results of device and components installed
- Draft test result of cable inspection, testing and verification
- Draft schedule of all installed and/or configured devices listing as a minimum the following (Network configuration, Switch & port connectivity, location, Name/labeling, Serial Number, Warranty Start & Expiry date, Device Username/Passwords, Device IP and MAC Address, Function, etc....) in editable MS Excel format

## 11.0 As-Built Documentation

- 11.1 Upon successful completion and acceptance of each security project, the Successful Bidder shall submit one (1) electronic set of record documentation and drawings to City of Toronto Corporate Security within ten (10) calendar days from the date of acceptance.
- 11.2 As-built shall include drawings and shall be in the FORM of black line set, record drawings on AutoCAD 2005, as well as a .pdf version, and are to be provided on a clean CD-ROM, DVD, or via e-mail.
- 11.3 Drawings shall include:
- Shop drawing submittals;
  - Wiring diagrams for each location (include distances);
  - Details of types of wire and conduit (include type and size);
  - Particular model number of hardware (to match Summary of Security Devices Table to be provided by COT);
  - Approval of drawing submittals;
  - Beneficial occupancy date;
  - Project Completion date;
  - Equipment manufactures;
  - Factory Acceptance Tests;
  - Installation procedure;
  - O&M manuals; and,
  - Manufacturer's specification sheet.
- 11.4 Architectural: site plans, building plans, and floor plans showing all locations for every security device both new as well as any effected existing device.
- 11.5 All security devices depicted in the drawings must be individually labelled according to the programming on the security system to ensure tagging consistency.
- 11.6 All security device symbols depicted must be in conformance to the Security Industry Association Architectural Graphic Standards for Security System Layout SIA/IAPSC AG-01-1995.12(R2000.03).
- 11.7 A Summary of Security Devices Table, as installed in Excel format. The table shall include the following for each security device: Security Device CAD Symbol, Make, Model, Serial number, IP Address, MAC address, Device Type/Function, Install Date, Installing Company, network configuration, Switch & port connectivity, VLAN, location, Name/labeling, Serial Number, Warranty Start & Expiry date and a photograph of each installed device. A template will be provided by the COT.
- 11.8 Wiring diagrams and/or schedules for each system defining the interconnection of all inputs and outputs for all equipment/security devices/electrical connections including description of location and/or name of each device.

- 11.9 Construction Typical for all security applications.
  - 11.9.0 As-built shall include all information required in the prefabrication submittals revised to reflect "as installed" conditions.
  - 11.9.1 As-built shall also include one (1) sets of complete and current operation and Maintenance manuals for all devices and equipment.
  - 11.9.2 The Successful Bidder is solely responsible to include engineered stamped drawings when required by the City.
  - 11.9.3 As-builts may not have any written notes on them all entries must be electronic.

## 12.0 Installation Standards and Requirements

- 12.1 All direction for scope of work must be provided by the COT Project Manager. Any work completed without approval of the COT Project Manager may have to be altered at the COT request and without additional cost to the COT.
- 12.2 The Successful Bidder must deliver the specified Products and/or Services as per their Quotation without substitution or deviation.
- 12.3 The Successful Bidder shall be solely responsible for detailed design, project management, coordination, equipment procurement, installation, component wiring, terminations, connections, labelling, programming, integration, testing, commissioning and issuing of required documentation of City systems.
- 12.4 The Successful Bidder shall restore all property temporarily removed, damaged, or destroyed during the supply, delivery, and installation, of Products to the satisfaction of the City and at no cost to the City. The Successful Bidder, before final payment, shall remove all surplus materials and any debris of every nature resulting from its operation and put the site(s) in a neat, orderly condition; thoroughly clean. If the Successful Bidder fails to clean up at the completion of the supply, delivery, and installation of the Products, then the City may do so and charge the Successful Bidder for the costs thereof, or deduct said costs from any monies still owing to the Successful Bidder.
- 12.5 The Successful Bidder shall furnish all labour, materials, services, special equipment, supplies, tools, equipment, testing equipment, apparatus, trade tools, transportation, facilities and incidentals required and perform all operations necessary to accomplish the complete installation of the Product(s).
- 12.6 The Successful Bidder is responsible for all final wiring, integration and terminations of all systems.
- 12.7 Testing and commissioning is to be performance according to City and NFPA standards. Specific documentation to achieve this will be developed with the successful bidder and final template approved by City of Toronto (COT).

- 12.8 Unless authorised by the Project Manager, the Successful Bidder must flush mount all devices. Back boxes / junction boxes, all devices, equipment and components installed must be equipped with tamper resistant screws/fasteners.
- 12.9 Any back boxes / junction boxes must be installed on secure side (if applicable).
- 12.10 The Successful Bidder must ensure the electronic door operators are integrated with the access control system, and only activate when a valid card is presented. If not included during the quotation process, all associated costs will be at the Successful Bidders expense.
- 12.11 The Successful Bidder will ensure programming for any CCure systems is completed to Standard and report to maintenance mode Journal for a minimum of one week after successful site testing and deficiency correction. After one week, should no deficiencies exist, the Successful Bidder will remove the system from Journal and fully activate at the request of the City Corporate Security Lead.
- 12.12 All card readers must be ordered and programmed to City Standard/format and as directed by the City Corporate Security Lead.
- 12.13 All exit buttons are to be green in colour and embossed with the label "EXIT", no other type will be accepted even if quoted. Any errors will result in replacement by the Successful Bidder at no additional cost to the City.
- 12.14 All intercoms are to have a red button with red led status indicator that is used to communicate, no other type will be accepted even if quoted. Any errors will result in replacement by the Successful Bidder at no additional cost to the City.
- 12.15 Each facility covered under this contract shall be handed over to the City by the Successful Bidder as a turnkey operation.
- 12.16 Any power supplies, or other parts that are required shall be supplied by the Successful Bidder and shall be included in the quoted price. Power supplies must operate all connected hardware in all conditions.
- 12.17 The Successful Bidder shall be responsible for provisions of power, if it should not be present at a location. Dedicated power circuits shall be installed for each new device that will be installed as part of this project.
- 12.18 Any required expansion boards, ancillary equipment, needed for a full operation of the system are the responsibility of the Successful Bidder and must be included in the quote. Should they not be included but be required to operate the system then it will be the successful bidders responsibility to provide without cost to the City.
- 12.19 All device conditions and alarms shall be individually enunciated on the relevant system, as required for each specific project scope.

- 12.20 The Successful Bidder shall be responsible for the installation of all the equipment, units, and sub-systems, at all sites in order to meet all requirements specified in this document, as per all applicable standards, and as per manufacturer's intent.
- 12.21 All installation materials, accessories and special equipment, Services, Personnel, test equipment and tools required for installation of the equipment shall be provided by the Successful Bidder.
- 12.22 The Successful Bidder shall be responsible for all required trenching, civil work, and any associated costs.
- 12.23 The Successful Bidder shall provide all programming data required to achieve the specified functionality for each effected system (this includes situations where existing technology is being replaced with new technology). Such programming shall include (but is not limited to) programming of all alarms, events, triggers, timers, objects transmitting and receiving signals, networking, bandwidth settings, frame rates, images per second, permissions, integration between systems, and interfaces as well as programming of signal receiving centre equipment to provide 100% full functionality.
- 12.24 It is required that disruptions be minimized keeping the existing intrusion detection systems or video surveillance systems operational during the process of upgrading to the new systems until all devices from the new system are functional and ready to be used by the end user. Consideration for the critical nature of all facilities operations and occupants is crucial to the success of the project.
- 12.25 Any new materials used by the Successful Bidder to commission the existing devices to the new system shall be covered by the warranty under this contract.
- 12.26 All existing devices that will be re-used by the Successful Bidder shall be commissioned to the new systems as defined by the COT.
- 12.27 All existing devices that will be replaced with new devices under the scope of work of any specific project shall be removed by the Successful Bidder. The removal of existing equipment or parts which will not be used with the new installations shall be completed by the Successful Bidder. Parts in working order are to be returned to address noted below. Other parts to be disposed by bidder.

**Scarborough Civic Centre,  
Lower Level, Security Storage Room  
150 Borough Drive  
Toronto, Ontario, Canada  
M1P 4N6**

Working parts under 5 years old to be return are as follows:

- Electric Strike
- DVRs, NVRs
- Servers
- Security Network Switches
- Cameras
- Camera Mounts
- Encoders

- UPS
  - Request to Exit Buttons
  - Intercoms
  - Wall mounted duress buttons
  - Sirens
  - Communication Boards/Panels
  - Long Range Motion Sensors
  - Maglocks
- 12.28 Where this section applies, the Successful Bidder must provide the City a minimum of 24-hours' notice of delivery of old functioning electronic security hardware, electro-mechanical security hardware, and mechanical hardware. All other equipment not required to be delivered to the City shall be disposed of at the Bidder's expense.
- 12.29 All costs and expenses associated with returning old equipment shall be the responsibility of the Successful Bidder.
- 12.30 The Successful Bidder shall reuse existing conduit runs whenever feasible and run new cabling in the existing conduit runs. Where existing conduit is used the new and existing cables must not experience any negative performance indications. Any deficiencies found after installation must be corrected by the successful bidder at no cost to the COT.
- 12.31 The Successful Bidder shall be responsible for patching up holes left by existing equipment and making good all repairs where new equipment is being installed in the same place.
- 12.32 All installed equipment shall be fully functional and shall be capable to be monitored at each individual site as well as the Corporate Security Control Centre located at 703 Don Mills Road.
- 12.33 Devices such as communication boards or input/output boards shall not be installed on door of panels. Additional panels shall be installed by the Successful Bidder to accommodate the installation of such devices.
- 12.34 Upon completion of the installation of the equipment at each location, the Successful Bidder shall provide to the Project Manager the serial numbers and model numbers of all newly installed equipment, these are to be included in the Summary of Security Devices Table referenced in section "As-Built Documentation 11.7".
- 12.35 The Successful Bidder shall install plywood backboards for mounting of all infrastructure equipment which require such backing to be able to be safely mounted to a wall such as electronic key cabinets, panels, and power supplies, etc.
- 12.36 Connect equipment to the closest approved available panel/switch/computer with available inputs and outputs.
- 12.37 Any new and existing cables for all devices which are exposed on the surface of a wall or ceiling or any other accessible surface shall be placed in conduit or wire moulding by the Successful Bidder as directed

by the COT. This conduit/moulding shall be sized to allow for additional 25% increase in cable and include a cable pull string for future use. Type of conduit/moulding to be confirmed on specific project site meetings with COT. Plenum rated cable must be used in any spaces requiring plenum rated cabling as per building and/or electrical code. All cabling, conduit, and installation methods utilized must meet COT IT Cabling Standards, manufacturer recommendations, and both the Electrical and Building Codes.

- 12.38 All infrastructure equipment including power supplies, transformers, communication devices, controllers, recording devices, etc. must be installed in secure cabinets. The Successful Bidder shall provide and install such cabinets and mount all of the equipment inside the cabinets. All costs for such cabinets shall be included in the quoted price.
- 12.39 Video Surveillance installation and camera field of view shall be in compliance with applicable local privacy laws, the City video surveillance privacy policy and shall be approved by the Corporate Security Lead.
- 12.40 All IP enabled devices such as IP Cameras, Encoders, iStar's, NVR's, card readers, controllers, etc. shall be tagged with an appropriate device name in coordination with the Corporate Security Lead.
- 12.41 Typical naming conventions are as follows however final naming convention shall be coordinated with and approved by the Corporate Security Lead prior to the commencement of any device setup or installation:
- Site Address-NVR/Controller Number/Name
  - NVR's shall be numbered sequentially as added
  - Device numbers shall match port number on attached switch or controller
  - Ex: 1008YNG-NVR9-CAM3
- 12.42 All IP Cameras and Encoded Cameras shall be programmed on the VSS to display a short form naming. This Naming shall be coordinated with and approved by the Corporate Security Lead prior to configuring the VSS.
- Typical Camera/device short FORM name on Milestone system would be:  
1008YNG-F3-NW STAIR-3
- 12.43 The Security Contractor shall carry the cost of all required access hatches where required and shall patch and paint to match existing paint; all locations for access hatches shall be pre-approved by the Corporate Security Lead in writing before working on these access hatches.

## 13.0 VSS Design Criteria

- 13.1 The VMS architecture shall permit centralized administration and management for the IP VSS and its distributed components across the City's local and wide area corporate networks. This administration

shall be redundant providing seamless failover capabilities and continuous operation in the event of failure of one of the main IP VMS services.

- 13.2 The VMS shall allow for continuous system management and operation through resilient server clusters on the City provided domain, between 55 John Street and 703 Don Mills. This resiliency shall span the Management, SQL Database and Event servers providing continued operation at the primary and/or the secondary site depending on failure cause and location of components, infrastructure and/or related services.
- 13.3 The VMS shall allow for administering and managing the complete VSS system from any workstation having the Milestone XProtect® management client application installed and connected to the Corporate Security Lead's Corporate Network.
- 13.4 The VMS shall keep all (Audit, Event, and Rule and System logs) for duration of 60 days. Any storage or other specifications required from the Corporate Security Lead provided equipment shall be included and provided by the security contractor to the Corporate Security Lead as part of the server Specifications required.
- 13.5 The following will be supplied by the City of Toronto:
  - Microsoft SQL Software and Licenses
  - Physical Servers required for Milestone VMS Management Services including Microsoft Windows Server 2008/2012 Licenses:
    - Management Server
    - Event Server
    - SQL Server
    - Mobile Server
  - Client (user) Workstations
  - VSS Core Network Switches (Cisco Switches)
  - VSS Access Layer Switches (Cisco Switches)
  - SAN Network Switches (Cisco Switches)
  - Ethernet Cat6A Patch Panels
  - Fiber Patch Panels in VSS Racks
  - Fiber connectivity between existing telecom rooms, entrance facilities and equipment rooms.
- 13.6 The Security Contractor shall specify the required Cisco switch models, and configuration required for the VSS, and the SAN to operate fully (including interface modules, IOS software, ports, Supervisor Engine, Backplane BW, POE Power/port, QOS Groups & Types, etc....). It is the responsibility of the Security Contractor to ensure specified network infrastructure is adequate for the complete system operation in normal and failover modes. The Security Contractor is responsible to coordinate and provide all detailed server specifications required for the system full operation to the Corporate Security Lead IT departments. Should the switch be determined to not be functionally appropriate by the COT, it shall be replaced by the successful bidder with an appropriate device at no additional cost to the COT.

- 13.6.0 Provide all VSS components and accessories required for achieving the full required functionality including but not limited to IP cameras, power supplies (Where Applicable), transmission media converters and extenders, modules, Video Encoders, mounts, enclosures, cables, plenum rated back boxes/enclosures/kits and IR Illuminators etc....
- 13.6.1 The only acceptable video compression (digital encoding) method shall be non-proprietary H.264 encoding (Baseline and/or Main Profile)
- 13.6.2 The VMS shall transmit and communicate over Corporate Security Lead IP network LAN/WAN, Fibre cables, Ethernet cables, Coaxial cables and Elevator installed coaxial cable infrastructure.
- 13.6.3 The Security Contractor shall warranty and ensure network bandwidth transmission performance, display, compression and network latency, PC client workstation, NVR's, SAN's and VMS server performance is designed and engineered to be sufficient, functional and in accordance with Milestone Systems VMS equipment and VSS hardware manufacturer.
- 13.6.4 The Security Contractor shall be sensitive to network bandwidth requirements and communicate all requirements to the Corporate Security Lead. It will be the sole responsibility of the Security Contractor to design and engineer all network transmission paths under the performance conditions of this specification and the requested deliverables.
- 13.6.5 All VSS Servers and workstations will have corporate antivirus agents installed by the Corporate Security Lead's IT Team prior to the installation. The additional travel time incurred by the successful bidder for deliveries to required sites for programming shall be at no charge to the COT.

## 14.0 Video Recording

All video must be stored for 37 days. The local NVR disks must be capable of recording for the full thirty seven (37) days, at full system capacity.

### 14.1 Network Video Recorders

Minimum requirements include:

- 14.1.0 RAID1 OS Volume array (2 x 240GB SSD)
- 14.1.1 RAID controller with minimum 512MB Battery backed cache
- 14.1.2 Enterprise Remote management capabilities, with virtual media and console access capabilities c/w out-of-band interface
- 14.1.3 RAID 1 Volume array for recording live video (15K RPM or better).

- 14.1.4 RAID 5 Volume array for archived video (7.2K RPM or better).
- 14.1.5 At least one global hot spare
- 14.1.6 All hard drives shall be Enterprise / Data centre grade
- 14.1.7 All DISK I/O's should run at no more than 80% of the maximum System capacity under normal operating conditions including Antivirus software, Encrypting Video and other required system services. 20% overhead shall remain free.
- 14.1.8 NVR's shall be equipped with Enterprise server network cards
- 14.1.9 Each NVR shall be equipped with two network ports for live viewing and two separate ports for recording video. All camera recording streams shall be on a separate VLAN.
- 14.1.10 Each NVR shall have a redundant and resilient connection to the SAN (where applicable) through a dedicated network
- 14.1.11 NVR Hardware shall be off-the shelf HP or DELL Servers
- 14.1.12 The NVR solution and design shall be certified and approved by Milestone Systems to meet the performance requirements of the VMS solution.
- 14.1.13 All Recorders to be configured and connected to COT centralized Milestone management system

## 14.2 Class A Recorder

Recording 16 or less local IP Video or Camera streams each streaming H.264 compressed video at a resolution of 1920x1080p, frame rate of 15fps, stream bandwidth of 2400Kbps/Stream, with 100% estimated scene motion, and continuously recording for 24hrs for a total of thirty seven [37] days retention period without any altering or compression to original recorded streams (i.e.: reducing P frames, or other compression techniques)

Allow for thirty-seven [37] days continuous recording on the local NVR RAID5 Storage Array with hot spare disk.

The following is an example of the required NVR. Equivalents, or others, approved by Milestone to be presented to City Of Toronto for an approval.

Primary/Redundant NVR Specifications	
Requirements	
Processor/Chipset	1 x Intel Xeon E5-2620 v3 2.4GHz or COT approved equivalent
Operating System	Microsoft Windows Server 2012 x64 Standard
Monitor	Refer to TR Typical for KVM requirements
System Memory	Minimum 32GB 1600MHZ DDR3 Memory
Hard Drives/OS	2 x 240GB Solid State SATA drives, 6Gbps 2.5in Hot-plug Drive, 3.5in (Raid 1)
Hard Drives/Live video	2 x 600GB 15K RPM SAS 2.5in Hot-plug Hard Drive, 3.5in (Raid 1)
Hard Drives/Archive	5 x 8TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive (Raid 5 + Hot spare)
RAID Controller	Enterprise Class Raid Controller with minimum 1GB Cache, supporting required disks and RAID levels with battery backup and write-back cache support.
Graphics	On board
Network	Broadcom 5720 QP 1Gb Network Daughter Card
I/O Ports	USB 2.0 or USB 3.0
Chassis Type	Rack mount, c/w pull out rails (tool-less mounting with square holes) Chassis with up to 12, 3".5" Hard drives + 2, 2.5" Flex Bay Hard Drives
Expansion Slots	Minimum 3x PCIe (2x16 Bandwidth, x8 Bandwidth)
Security	Chassis Intrusion Switch Setup/BIOS Password; lockable bezel
Remote Management	Enterprise remote virtual media and console access capabilities c/w out-of-band interface (Ex: iDRAC7 Enterprise or COT approved equivalent)
Power	Dual, Hot-plug, Redundant Power Supply (1+1), 750W
Support	4-Hour 7x24 On-Site Service with Emergency Dispatch, 3 Year

### 14.3 Class B Recorder

Recording 32 or less local IP Video or Camera streams each streaming H.264 compressed video at a resolution of 1920x1080p, frame rate of 15fps, stream bandwidth of 2400Kbps/Stream, with 100% estimated scene motion, and continuously recording for 24hrs for a total of thirty seven [37] days retention period without any altering or compression to original recorded streams (i.e.: reducing P frames, or other compression techniques)

Allow for thirty-seven [37] days continuous recording on the local NVR RAID5 Storage Array with hot spare disk.

The following is an example of the required NVR. Equivalents, or others, approved by Milestone to be presented to City Of Toronto for an approval.

Primary/Redundant NVR Specifications	
<b>Requirements</b>	
Processor/Chipset	1 x Intel Xeon E5-2620 v3 2.4GHz (or COT approved equivalent)
Operating System	Microsoft Windows Server 2012 x64 Standard
Monitor	Refer to TR Typical for KVM requirements
System Memory	Minimum 32GB 1600MHZ DDR3 Memory
Hard Drives/OS	2 x 240GB Solid State SATA drives, 6Gbps 2.5in Hot-plug Drive, 3.5in (Raid 1)
Hard Drives/Live video	2 x 900GB 15K RPM SAS 2.5in Hot-plug Hard Drive, 3.5in (Raid 1)
Hard Drives/Archive	8 x 8TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive (Raid 5 + Hot spare)
RAID Controller	Enterprise Class Raid Controller with minimum 1GB Cache, supporting required disks and RAID levels with battery backup and write-back cache support.
Graphics	On board
Network	Broadcom 5720 QP 1Gb Network Daughter Card
I/O Ports	USB 2.0 or USB 3.0
Chassis Type	Rack mount, c/w pull out rails (tool-less mounting with square holes) Chassis with up to 12, 3".5" Hard drives + 2, 2.5" Flex Bay Hard Drives
Expansion Slots	Minimum 3x PCIe (2x16 Bandwidth, x8 Bandwidth)
Security	Chassis Intrusion Switch Setup/BIOS Password; lockable bezel
Remote Management	Enterprise remote virtual media and console access capabilities c/w out-of-band interface (Ex: IDRAC7 Enterprise or COT approved equivalent)
Power	Dual, Hot-plug, Redundant Power Supply (1+1), 750W
Support	4-Hour 7x24 On-Site Service with Emergency Dispatch, 3 Year

#### 14.4 Class C Recorder

Recording 64-128 local IP Video or Camera streams each streaming H.264 compressed video at a resolution of 1920x1080p, frame rate of 15fps, stream bandwidth of 2400Kbps/Stream, with 100% estimated scene motion, and continuously recording for 24hrs for a total of thirty seven [37] days retention period without any altering or compression to original recorded streams (i.e.: reducing P frames, or other compression techniques)

Allow for thirty-seven [37] days continuous recording on the local NVR RAID5 Storage Array with hot spare disk.

The following is an example of the required NVR. Equivalents, or others, approved by Milestone to be presented to City Of Toronto for an approval.

Primary/Redundant NVR Specifications	
Requirements	
Processor/Chipset	2 x Intel Xeon E5-2660 v4 2.0GHz (or COT approved equivalent)
Operating System	Microsoft Windows Server 2012 x64 Standard
Monitor	Refer to TR Typical for KVM requirements
System Memory	Minimum 64GB 1600MHZ DDR3 Memory
Hard Drives/OS	2 x 250GB Solid State SATA drives, 6Gbps 2.5in Hot-plug Drive, 3.5in (Raid 1)
Hard Drives/Live video	2 x 900GB 15K RPM SAS 2.5in Hot-plug Hard Drive, 3.5in (Raid 1)
Hard Drives/Archive	10 x 10TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive (Raid 5 + Hot spare)
RAID Controller	Enterprise Class Raid Controller with minimum 1GB Cache, supporting required disks and RAID levels with battery backup and write-back cache support.
Graphics	On board
Network	2 x Broadcom 5720 QP 1Gb Network Daughter Card
I/O Ports	USB 2.0 or USB 3.0
Chassis Type	Rack mount, c/w pull out rails (tool-less mounting with square holes) Chassis with up to 12, 3".5" Hard drives + 2, 2.5" Flex Bay Hard Drives
Expansion Slots	Minimum 3x PCIe (2x16 Bandwidth, x8 Bandwidth)
Security	Chassis Intrusion Switch Setup/BIOS Password; lockable bezel
Remote Management	Enterprise remote virtual media and console access capabilities c/w out-of-band interface (Ex: iDRAC7 Enterprise or COT approved equivalent)
Power	Dual, Hot-plug, Redundant Power Supply (1+1), 750W
Support	4-Hour 7x24 On-Site Service with Emergency Dispatch, 3 Year

## 15.0 VSS Storage Area Network (SAN)

### 15.1 The SAN shall have the following minimum requirements:

- Equipped with redundant and hot-swappable power supplies and cooling Fans
- Support hot-swappable drives, each configured RAID 5 volume should be configured to have a hot spare disk available
- Support both iSCSI (1GB, 10GB), FCoE (10GB), FC (4-16GB) with Hot Swappable controllers
- Provide a minimum effective (Usable) total storage capacity of RAID5 configured arrays to allow for the required video storage retention of 30 days from each of the NVR's connected to it
- Expandable to allow for additional 30% effective storage capacity and the connectivity of additional two [2] NVRs
- Support redundant and load balancing SAN connectivity to each NVR Server.
- Support multiple RAID levels on connected storage within an array

- Enough processing power and backplane bandwidth to support the total IOPS required for recording and retrieval of the video to and from the storage array.
- Enough memory bandwidth to support the buffering and queuing of system I/O's and transferred data.
- Equipped with battery backed cache for all array controllers (minimum 512MB)
- Intuitive enterprise level management and monitoring interface that can scale across the multiple SAN's
- Preference for remote monitoring and support features

15.2 The SAN shall be connected on its own dedicated local network; the security contractor shall provide the Cisco Network switches specifications and Media interface types required and coordinate these requirements with the Corporate Security Lead Networking Team. SAN network traffic shall not interfere with the any other network traffic.

15.3 All Patch Cables, labeling and connectivity between the SAN, Servers and SAN Network shall be the responsibility of the Security Contractor.

15.4 The management interface of the SAN shall be connected to the Corporate Security Lead's corporate network to allow for remote management and control.

15.5 The SAN solution and design shall be certified and approved by Milestone Systems to meet the performance requirements of the VMS solution.

15.6 Dell products are preferred, however alternatives approved by Milestone and which meet the above specifications will be considered.

DAS devices can be used instead of SAN where approved by the COT. The specified DAS must be approved by Milestone, achieve the desired recording duration, and allow for 25% video surveillance system growth. Dell and HP products are preferred, alternatives would have to be approved by the COT.

The below are the minimum DAS requirements. Equivalents, or others, approved by Milestone will be considered.

Minimum Specifications
<b>Hardware</b>
Minimum 8GB RAM
Dual Controller Array configuration
RAID Array Controller w/1 GB Battery Backed Cache

DUAL Hot Swappable 10/100/1000 Ethernet Controllers with 4 ports each
<b>Disk Configuration</b>
SATA 7.2k RPM or better disks (Size or Disks Varies with required Storage, min 4TB disks rated for Enterprise DAS Storage and Video streaming applications)
Storage Volume to be configured as a RAID 10 Array

## 16.0 Cameras

- 16.0.1 Install dome cameras in flush surface or drop ceiling with concealed cabling
- 16.0.2 Configure cameras internal access with a new Username/Password credentials and **remove default logins**
- 16.0.3 Configure cameras with secure access protocols, VLANs, QOS and other network settings in coordination with the Corporate Security Lead. Cameras shall be totally secured to authorized access before being connected to the Corporate Security Lead’s Network
- 16.0.4 All Cameras include elevator cab cameras shall be named in coordination with the Corporate Security Lead naming scheme and configured to sync with the Corporate Security Lead’s local NTP server/VMS system
- 16.0.5 Configure each camera stream settings including but not limited to frame rate, bitrate, compression, stream name, day night setting, and other related configuration in coordination with the Corporate Security Lead. All configurations shall be approved by the Corporate Security Lead before setting and configuring the devices
- 16.0.6 Configure and calibrate cameras for the lighting conditions at each camera location including setting shutter speeds, AWB, Exposure levels, Day/Night mode, WDR, AGC, and other related settings to produce optimal video pictures under all operating conditions
- 16.0.7 Ensure Cameras are operating the latest firmware version or as recommended by the manufacturer at time of installation.
- 16.0.8 Backup all camera settings/configurations in addition to the VMS configurations to a CD/DVD and submit to Corporate Security Lead.
- 16.0.9 Ensure outdoor cameras and their heater are properly powered to operate normally in all environmental conditions referenced in this section

16.0.10 All cameras with analytics capabilities shall be setup and calibrated for the supported alarms. Typical alarms to be configured by default for all cameras include:

- Motion in full or designated field of view zones
- Video Masking
- Video Loss/Gain
- Network Loss
- Device I/O's

16.0.11 Configure logging and network troubleshooting capabilities on each IP cameras in coordination with the Corporate Security Lead.

16.0.12 Configure Network Security features and settings on each camera in coordination with the Corporate Security Lead.

16.0.13 For PTZ cameras configure Masks, home position, pre-sets, control sensitivity, image mode and other related settings in coordination with the Corporate Security Lead.

16.0.14 All camera installations and field of view setup shall meet the VSS primary functions identified by the Corporate Security Lead. The following minimum resolution requirements are required for each of the VSS functions below:

- General Observation: >20ppf on farthestmost desired target
- Forensic Review (General Identification) : >40ppf on farthestmost desired target
- Recognition including Facial, vehicle license plate, color, pattern, and cross-line recognition: > 80ppf on farthestmost desired target
- All camera views, resolution and image color and quality, shall pass the approval of the Corporate Security Lead.

## 16.1 IR Illuminators

All IR illuminators specified for specific camera installation projects are to be:

- Mounted and calibrated not to over expose the image quality during night time operation.
- All IR accessories shall be POE Powered unless otherwise approved by the Corporate Security Lead.
- All IR shall be IP66, Vandal resistant and mounted securely or be built-in to the camera. .4 IR 850nm wavelength, equipped with a Photocell and configured to activate on environmental lighting conditions.

## 17.0 Video Encoders

17.1 The following are the minimum performance specifications for Video Encoders to be specified by the successful bidder:

- 17.1.0 Rack mounted
- 17.1.1 Flexible and Expandable allowing for hot swappable blades (applies to encoders for 1 channels or more)
- 17.1.2 Equipped with redundant hot swappable power supply and fans (applies to encoders where more than 8 channels are required)
- 17.1.3 Each encoder channel shall support H.264 video compression, a minimum of two simultaneous streams at 720 (horizontal) × 486 (vertical) NTSC analogue video resolution and 30fps.
- 17.1.4 Each encoder channel shall have a minimum of one [1] configurable input/output .6 Security Contractor shall ensure the encoders support the PTZ protocols and control connectivity (RS-485, RS-422) for connected PTZ analogue cameras
- 17.1.5 Each encoder shall support the following analytics for each video channel and shall trigger an alarm on Milestone Systems XProtect Corporate® VMS:
  - i. Camera repositioning
  - ii. Camera lens is masked, sprayed, covered or blocked
  - iii. Motion detection in defined zones of the camera view, minimum five [5] zones
- 17.1.6 Each Encoder shall support the following alarms and shall be annunciated on the Milestone monitoring interface:
  - i. .1 Video Signal loss /gained per channel
  - ii. .2 Network loss/gained
- 17.1.7 Encoder shall be ONVIF compliant and supports (Profile S)
- 17.1.8 Encoder shall support the following protocols: IPv4/v6, HTTPS, SSL/TLS, QoS Layer 3, FTP, CIFS/SMB, SNMPv1/v2c/v3 (MIB-II), DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP.
- 17.1.9 Shall support remote firmware upgrade.
- 17.2 All Encoders shall be rack mounted in a proper cabinet.
- 17.3 Configure each encoder interface and chassis (where applicable) with secure access protocols, VLANs, QOS and other network settings in coordination with the Corporate Security Lead. Cameras shall be totally secured to authorized access before being connected to the Corporate Security Lead's Network

- 17.4 Each encoder channel shall be named in coordination with the Corporate Security Lead naming scheme and configured to sync with the Corporate Security Lead's local VSS NTP server/VMS system
- 17.5 Configure each channel stream settings including but not limited to frame rate, bitrate, compression, stream name, day night setting, and other related configuration in coordination with the Corporate Security Lead. All configurations shall be approved by the Corporate Security Lead before setting and configuring the devices
- 17.6 Ensure Encoders are operating the latest firmware version
- 17.7 Backup all Encoders settings/configurations in addition to the VMS configurations to a CD/DVD and submit to Corporate Security Lead.
- 17.8 Ensure Encoder chassis is powered through a UPS and backup power to operate normally in all environmental conditions referenced in this section
- 17.9 All encoder channels with analytics capabilities shall be setup and calibrated for the supported alarms. Typical alarms to be configured by default for all cameras include:
  - i. Motion in full or designated field of view zones
  - ii. Video Masking
  - iii. Video Loss/Gain
  - iv. Network Loss
  - v. Device I/O's
- 17.10 Configure logging and network troubleshooting capabilities on each channel and encoder chassis in coordination with the Corporate Security Lead.
- 17.11 Connect and configure PTZ Data control protocols and settings on channels that are connected to analogue PTZ.

## 18.0 Ethernet Media Extenders

The following are the minimum performance specifications for Ethernet Media Extenders to be specified by the successful bidder in the event that the required product is not listed in the Price Form:

1. Any camera that exceeds the standard 100BASE-TX connectivity distance limitation requires: 100Mbps Ethernet extenders to extend transmission with POE pass-through over standard 75Ω coaxial cables
2. Extended Pass-through POE: meets the IEEE 802.3af standard for Power over Ethernet
3. Supports Jumbo Frame Transmission
4. Extends up to a minimum of a minimum of 548m at 100BaseT with POE pass-through .5 Suitable for high bandwidth requirements of Mega-pixel cameras
5. Aluminum Enclosure

## 6. Meets NEMA TS-1/TS-2 environmental requirements

### 18.1 POWER AND ETHERNET OVER COAX

The following are the minimum performance specifications for Power and Ethernet over Coax devices that are to be specified by the successful bidder:

#### 18.1.0 Proposed IP and PoE/PoE+ over Coax solution shall, as a minimum, meet the following requirements:

- a. Provide enough PoE or PoE+ (IEEE 802.3af/802.3at) to Power the IP devices in all conditions and up to 50W (ex: When built-in heater is activated, PTZ, blower where applicable)
- b. Provide adequate output power to power the devices and provide Ethernet transmission over the various types, lengths and quality of wiring existing at the locations in scope
- c. Has minimal end-to-end Latency of  $\leq 3$ ms that shall not affect the Video/Ethernet transmission over Coax
- d. Transceiver unit close to the edge device shall operate normally in outdoor environmental conditions as mentioned under paragraph (2.3.2.1.2 Outdoor) and shall not require an extra power source to operate.
- e. Provide transient overvoltage and electrostatic discharge protection and immunity to a minimum of: 5x20 $\mu$ S 3,000A 6,000V; ESD protection for 200pF 20KV.
- f. Provide an encrypted Coax link with a minimum of 128Bit AES encryption.
- g. Head-end transceivers shall be rack mounted in standard 19" rack cabinets, for single channel transceivers a rack mounting kit shall be used to securely and neatly mount a single transceiver to the rack (placing unit on trays or loosely in the cabinet is not acceptable).

### 18.2 VSS POWER COMPONENT

The following are the minimum performance specifications of VSS Power Components that are to be specified by the successful bidder.

- 18.2.0 All VSS system components including but not limited to (POE Switches, Camera power Supplies, NVR Servers, VMS Servers, Encoders, Media converters, KVM Switches, Environmental and Cabinet Sensors, SAN etc....) shall be powered from a UPS backed by emergency power (where available) allowing for continuous, un-interrupted, operation of the complete VSS system for duration specified by COT during project quote phase. COT will require proof of MSRP from UPS manufacturer with MSRP discount applied as provided in the Price Form. The UPS system shall protect connected equipment from brownouts, overvoltage and other power irregularities.

- 18.2.1 All UPS equipment shall be securely rack mounted in cabinets. UPS equipment shall not be placed on shelves, installed on the ground or placed inside cabinets without proper rack rails or rack mounting kits unless approved by the Corporate Security Lead.
- 18.2.2 The complete IP VSS system and its distributed components shall be connected to a UPS for continued operation (provisioned at maximum power usage) where a backup circuit is available. The required power backup operation window shall include the provisioning for future expansion.
- 18.2.3 In addition to the above requirement the following shall apply for UPS selection and sizing:
- Securely rack mounted in a secure lockable cabinet
  - Sized to allow for a minimum of 40% extra power for future expansion
  - cUL listed and meets the following standards: UL 1449, UL 1778, CAN/CSA-C22.2 NO. 60950-1-07 (R2012)
  - Provides surge protection and filtering
  - Supports USB management, c/w windows software and management application to allow for server controlled shutdown upon reaching a set low battery threshold or internal Web based management interface
  - Alarms when on battery and c/w status LED indicators for normal operating mode, alerts and battery backup mode
  - Maintenance-free, sealed, user-replaceable and leak proof Lead-Acid Battery w/c automatic self-testing circuitry detecting and ensuring proactive alerts for battery replacement and/or faults
  - Resettable circuit breaker and automated recovery, ensures protection of connected loads from surges, spikes, lightning and other power disturbances
  - Medium & Large TR's to be equipped with expandable and upgradable rack mounted UPS units including sliding rack rails allowing for ease of maintenance, upgrades and serviceability
- 18.2.4 All new VSS IP Cameras shall be powered by PoE or PoE+ from respective PoE capable switches or Ethernet with PoE/PoE+ pass through media extenders. No exceptions are accepted unless for special purpose cameras requiring external power where applicable. This exception shall be approved in writing by the Corporate Security Lead.
- 18.2.5 IP and PoE/PoE+ over Coax solution shall be used to power IP cameras in analogue to IP cameras retrofit scenario. All new IP cameras shall be powered by PoE/PoE+ and shall not be connected to existing power supplies that are not connected to a UPS System.
- 18.2.6 PoE power provisioning shall be communicated and coordinated with the Corporate Security Lead and Corporate Security Lead's Networking Team and specified as part of the Cisco Network equipment. No assumptions of PoE/PoE+ power availability shall be made on any Corporate Security Lead provided network access switches unless previously coordinated and requested in writing from the Corporate Security Lead.

## 19.0 Equipment Cabinets/Racks

The Security Contractor shall be sensitive of the equipment room's space availability at the various locations in scope for rack installations. High density and low profile equipment should be considered in the proposed equipment design to reduce space requirements. The security contractor shall advise the Owner of any space required for additional rack quantities beyond what is provided and specified in the project scope. Corporate Security requires a dedicated secured rack for all security installations.

The following are the minimum performance specifications of various cabinets and enclosures that are to be specified by the successful bidder:

### 19.1 NEMA 12 – Rack Cabinets W/ Self-Contained Cooling Unit

- Pre-assembled before delivery
- Fully gasketed openings including gland plate in base
- Closed loop air-conditioning system, adequately sized to match equipment heat dissipation and cooling requirements (shall not require any piping, wiring or drainage) and shall also allow for 25% increase in heat generation of specified equipment. .4 Internal evaporator to eliminate condensation
- M6 Rail Type
- Plexi or Solid Doors
- Key Lockable secure doors and side panels
- Include casters and levelers
- Compatible vertical mounted PDU's
- Include cable management (vertical and horizontal lacing bars, front to back cable managers, bottom brush grommet kit, filler panels etc....) required for a neat cable and equipment installation
- Include grounding kit and ground appropriately
- Cabinet Size and Cooling Requirements shall be approved by Corporate Security Lead

### 19.2 NEMA 12 - Wall Mount Cabinets

- Pre-assembled
- Double hinged allowing access to the front and back side of cabinet

- NEMA 12 Fan Assembly
- Independent Key lockable from and back side
- Lifetime Warranty
- M6 Rail type
- Include cable management (vertical and horizontal lacing bars, front to back cable managers, bottom brush grommet kit, filler panels etc....) required for a neat cable and equipment installation
- Cable management trays, and arms
- Include grounding kit and ground appropriately

### 19.3 Standard Rack Cabinets

- 42 U, Pre-assembled before delivery
- Vented Side Panels, with key locks
- Casters and levelers
- M6 Rails
- Split doors back and front side, with key locks
- 6 x 4" fans top panel
- Include grounding kit and ground appropriately
- Include Vertical PDUs
- Include cable management (vertical and horizontal lacing bars, front to back cable managers, bottom brush grommet kit, filler panels etc....) required for a neat cable and equipment installation
- Cable management trays, and arms

## 20.0 Real-Time Environmental Monitoring Component

- Provide real-time, Ethernet (IP) based environmental monitoring solution at each in of the existing and new VSS designated racks.

- The monitoring unit shall be rack mounted
- Shall have a dual temperature/humidity sensor, intelligent water temperature sensor and door contact sensors for each cabinet door
- The monitoring component shall be connected to the City corporate network
- Capable to notify the Owner of any changes or detections by the sensors in a variety of ways including e-mail and SNMP
- Supports SNMP v1, v2, v3
- Manageable through an intuitive web interface

## 20.1 RACK KVM TRAY

The following are the minimum performance specifications of Rack KVM Trays that are to be specified by the successful bidder.

- Integral KVM Switch with keyboard, LCD monitor, and touch pad in 1U FORM .2 Allows remote network user access through KVMoIP over WAN & LAN
- Full Sized 105-Key keyboard
- Ergonomic hand rest
- Includes Universal Rear Rail Kit
- CE, RoHS approved
- Flip Open Monitor Minimum 19" TFT LCD monitor, 1280 x 1024 @ 60 Hz .8 Dual Rail Flip Open Monitor when Keyboard and Mouse are closed
- Control via on-screen display (OSD) menu, push buttons Selection Buttons on monitor bezel, hotkeys, or mouse.
- Connects to servers through CATx patch cables and required server access modules
- 16-Port CATx KVM
- Provide BIOS Level Access

## 21.0 Labelling

- 21.1 All cables shall be tagged, with a unique number, in common at both ends using a permanent method. Labelling shall agree with record drawings and point allocation tables and to indicate source and destination information.
- 21.2 All terminals shall be permanently tagged and shall agree with record drawings.
- 21.3 All system power supplies shall be labelled with their feed source and breaker number.
- 21.4 All connectors shall be marked with common designations for mating connectors. The connector designations shall be indicated on the record drawings.
- 21.5 All visible panel and control labels shall be silk-screened, engraved and filled, or engraved plastic laminate. Labels shall be permanently attached.
- 21.6 Labelled Doors and Frames in no instance shall any labelled fire door or frame be cut, penetrated, drilled or modified in any way.
- 21.8 Any labelled door or frame which shall require modification to meet the system specifications shall immediately be brought to the attention and written approval of the Project Manager.

## 22.0 Conformity of Work with Plans and Specifications

- 22.1 The Successful Bidder shall perform all Work and furnish all materials and complete the whole of the Work in conformance with the requirements.
- 22.2 Any Work or material not herein specified but which may be fairly implied as indicated in the Contract or obviously necessary for the proper delivery of a fully functional system, shall be done or furnished by the Successful Bidder as if such Work or material had been specified.
- 22.3 The Successful Bidder shall at all times have on the Work site, competent Personnel capable of reading and thoroughly understanding the plans and specifications, and thoroughly experienced in the type of Work being performed. Such Personnel shall include the supervision and direction of all Subcontractors, if any are used. The designated Personnel shall have available at all times the lists/floor plans required.
- 22.4 Upon request, the Successful Bidder shall provide the City of Toronto Corporate Security a list of all Personnel's duties, responsibilities, and obligations for the Work required.

## 23.0 Supply and Install Project Procedures

- 23.0.0 The City of Toronto Corporate Security and the Successful Bidder shall follow the procedures set-out in General Contract Terms and Conditions for all supply and install Work. The standard Security Project Work Package which will be provided to the Successful Bidder has been created to ensure consistent implementation/execution of the individual projects regardless of the projects size and scope.
- 23.0.1 Prior to the execution of any supply and install projects the Successful Bidder shall familiarize and comply with the project procedures set-out in General Contract Terms and Conditions, Supply and Install Procedures Package.

### 23.1 General Specifications

- 23.1.0 The Deliverables being supplied in this RFQ must be new and certified by the Vendor, and free of encumbrance. Refurbished, rebuilt, or used Products will not be acceptable.
- 23.1.1 All specifications are minimum requirements that must be met or exceeded. Bids containing one or more items that do not meet or exceed the minimum general specifications will be declared Non-Compliant.

## 24.0 IT Coordination

- 24.1 Coordinate with the Corporate Security Lead team for all equipment programming. Upon approval, connect, test all equipment and ensure there are fully and properly operating
- 24.2 All security equipment configurations shall be performed by the Corporate Security Lead IT Team in coordination, and support from the Security Contractor
- 24.3 All IP enabled devices with Username/Password parameters shall be configured with a designated temporary credentials and provided to the Corporate Security Lead. Default credentials shall be immediately removed upon initial power up and configuration of the device.
- 24.4 All typical configurations shall be coordinated and approved by the Corporate Security Lead IT Team before configuring the devices. The additional travel time incurred by the successful bidder for deliveries to required sites for programming shall be at no charge to the COT.

## 25.0 Licensing

- 25.1 The City prefers any net new licenses required to be a onetime purchase. Support and maintenance agreements should be independent of the software license.
- 25.2 The Vendor should be able to provide to the City at no additional cost at least one (1) copy of the Documentation for each copy of a licensed software.
- 25.3 The Vendor should be able to grant to the City a perpetual, non-exclusive, irrevocable, transferable, fully paid-up, royalty-free right and license to install, use, and copy (on storage units or media for backup or other contingency purposes), all or any portion of each licensed software, together with all associated Documentation, in accordance with the Terms of the resulting Contract and:
- i. the Vendor should provide to the City at least one (1) copy of each licensed software in installable FORM unless it has specified a greater number of copies;
  - ii. if the City is licensed to use any licensed software on any computer or computer complex, the City may transfer the licensed software to any different computer or computer complex without any fee or other charges being due to the Licensor;
  - iii. if the City is licensed to use any licensed software in conjunction with any operating system, the City may use the licensed software in conjunction with any other operating system without any fee or other charge being due to the Vendor if the licensed software is certified to operate on that other operating system when that use commences, regardless of whether the operating system was in existence or not in existence at the time the licensed software was originally licensed by the City;
- 25.4 If a CPU based license is provided, the CPU based license should be a perpetual license to use the licensed software on one physical CPU and such perpetual CPU license should not be conditional on any Terms and conditions not set out expressly in the Contract. The City may transfer the licensed software from one physical CPU to another physical CPU at any time or times without notice to the Vendor and without any fee or other charges being due to the Vendor. A CPU license for a physical CPU is not limited in any way by the use of multithreading, hyper-threading, or any quantity of logical CPU.
- 25.5 If concurrent user licenses are provided, then the concurrent user license should be a perpetual license to permit the use of the licensed software on a concurrent basis (limited to the number of simultaneous users of the licensed software) and such concurrent user license should not be conditional upon any Terms and conditions not set out expressly in the Contract. The Vendor should provide in the licensed software a utility to manage the list of users who are sharing the concurrent user license(s) and provide a mechanism within the licensed software to ensure that the contracted number of concurrent user license(s) is made available for users. The City may add to the number of users who can share the concurrent user license(s) at any time without notice to the Vendor and without any fee or other charges being due to the Vendor.

- 25.6 If named user licenses are provided, then the named user license should be a perpetual license to permit one (1) individual to use the licensed software and such named user license should not be conditional upon any Terms and conditions not set out expressly in the Contract. The City may transfer the named user license from one (1) individual to another individual at any time or times without notice to the Vendor and without any fee or other charges being due to the Vendor;
- 25.7 The Vendor should have the exclusive title to the licensed software and Documentation or otherwise have the right to grant to the City each license and every right under to each licensed software and the Documentation as contemplated by the Contract without violating any third party Intellectual Property Rights;
- 25.8 Each licensed software and the Documentation should be free from all encumbrances, should not, and will not contain any Disabling Code;
- 25.9 The Documentation should be well written, readily understood, and contain clear and concise instructions for users and system administrators of the licensed software and should include meaningful instructions to enable users and systems administrators to take full advantage of all of the capabilities of the licensed software including installation and system administration documentation to enable a system administrator to allow proper control, configuration and management of the licensed software;
- 25.10 For the duration of the Warranty Period, the licensed software will perform in accordance with the specifications and descriptions contained in the Contract, in the Vendor's published Documentation and specifications, and in the Documentation for the version of the software in use by the City;
- 25.11 The licensed software should be compatible with future releases of the operating system on which it was originally installed within one hundred and twenty (120) calendar days of general availability of the operating system and shall be subsequently maintained to remain so compatible;
- 25.12 The Vendor shall provide to the City, without additional charge, copies of the licensed software and Documentation revised to reflect any enhancements made by the Vendor and such enhancements will be deemed to include all Versions, Releases and other modifications to the licensed software which correct errors, increase the speed, efficiency, capacity or ease of operation of the licensed software, or add additional capabilities or functions to or otherwise improve the capabilities and functions of the licensed software; and
- 25.13 The Warranty Period of licensed software shall commence on the Initial Install Date of such licensed software.
- 25.14 Each software license granted pursuant to the Agreement should survive any expiry or termination of the Agreement.

## 26.0 Software Updates

The Successful Bidder shall provide all software updates and revisions to the City during the length of this contract term warranty period without cost to the City. The Successful Bidder must register and maintain all applicable Formal technical support agreements with manufacturers including but not limited to American Dynamics and Dedicated Micros, Milestones, BriefCam, Software House, CCURE9000, Key Tracer. Registration of the technical support agreements.

The Successful Bidder is responsible to maintain 100% functionality of the CCTV and AV Systems prior to and after scheduled updates are performed.

Where there is integration between City systems, the Successful Bidder must maintain integration compatibility and advise the City if software updates may impact the current integration performance and functionality.

## 27.0 Upgrades and Updates

Throughout the Contract Term and its Warranty period, the Successful Bidder shall provide notice to the Project Manager within 24-hours of all manufacturers' or software developer's release of a version, firmware, and/or patch upgrade and/or update for all security systems owned or operated by the City that pertains to this Contract.

The Successful Bidder shall include; without any additional costs to the City, all manufacturer and/or City of Toronto recommended application and operating system upgrades and updates including licenses, versions, firmware, hot fixes and patches to ensure continuous performance and continuity of City CCTV and AV Systems.

The Successful Bidder shall provide the City with all software upgrades and updates, in original packaging (where available), with original manuals/documentation, and original copies (compact discs, floppies, etc.).

## 28.0 Future System Expansion

The City reserves the right to have other qualified firms expand and/or add to the systems at any time.

The City reserves the right to make changes, alterations, additions, or deletions to any of the City's equipment.

## 29.0 Delivery and Installation

The Vendor must deliver the specified Deliverables as per their Quotation without substitution or deviation. All items shall be delivered F.O.B. Destination.

The Successful Bidder must deliver the specified Products and/or Services as per their Quotation without substitution or deviation.

The Successful Bidder shall provide staff who are qualified to undertake the installation Services required under the Terms of this RFQ. The staff must be certified to install and set-up the Products produced by the manufactures that are listed in the 33.0 Manufactures List.

The Successful Bidder shall restore all property temporarily removed, damaged, or destroyed during the supply, delivery, and installation, of Products to the satisfaction of the City and at no cost to the City. The Successful Bidder, before final payment, shall remove all surplus materials and any debris of every nature resulting from its operation and put the site(s) in a neat, orderly condition; thoroughly clean. If the Successful Bidder fails to clean up at the completion of the supply, delivery, and installation of the Products, then the City may do so and charge the Successful Bidder for the costs thereof, or deduct said costs from any monies still owing to the Successful Bidder.

The Successful Bidder shall furnish all labour, materials, Services, supplies, tools, equipment, apparatus, transportation, facilities and incidentals required and perform all operations necessary to accomplish the complete installation of the Product(s).

## 29.1 Return of Products

29.1.0 Should the Product fail to work upon arrival, or within thirty (30) days of arrival, the Product will be returned for a complete exchange of new working Product (same make and model), at no cost to the City. The Product must be exchanged within five (5) business days of notification. The Warranty Period of the replaced Product will be deemed to date from the day of replacement.

29.1.1 If the Product(s) do not function as warranted and the problem cannot be resolved to the satisfaction of the City, then the Product(s) may, at the sole discretion of the City, be returned for a full refund.

29.1.2 In the event an item has been discontinued by the manufacturer/supplier, the supplier must provide documentation to confirm the product is no longer available and provide a viable substitute that meets or exceed the current specifications at the same price.

The Vendor will be responsible for all costs associated with the return and replacement of any products which have been discontinued. This will include all freight, packaging and handling costs.

The City will not accept any changes related to the discontinued product. The City will not be responsible for any restocking charges associated with returns.

29.1.3 Bidders must not substitute contract approved product(s), commodity(s) or service(s) without prior written approval from City of Toronto Purchasing and Materials Management staff, on either City of Toronto letter head or City of Toronto originating email. Any approved substitution must meet or exceed the approved good, approved commodity or approved service to be substituted, at no additional cost to the City of Toronto.

## 30.0 Warranty

- 30.1 The Successful Bidder shall include a two (2) year Warranty for all parts and labour as per the Warranty conditions of this RFQ.
- 30.2 Warranty shall include all Preventive Maintenance for two (2) full year periods. This entails two site visits per warranty year.
- 30.3 If, within two (2) years after the date of final acceptance of the Work as determined by the Corporate Security Lead, or designated portion thereof, or within two (2) years after acceptance by the Corporate Security Lead of designated equipment, or within such longer period of time as may be prescribed by law, or by the Terms of any applicable special Warranty required by the contract, or applicable codes, any of the Work found to be defective or not in accordance with the contract, the Successful Bidder shall correct it after receipt of a written notice from the City to do so unless the City has previously given the Successful Bidder a written acceptance of such condition. This obligation shall survive termination of the contract. The City shall give such notice promptly after discovery of the condition.
- 30.4 All installed equipment, shall be subjected to its own Preventative Maintenance schedule; the schedule is to be submitted after final acceptance of equipment installation with the submitted as-builts. The Preventative Maintenance must be performed in accordance to NFPA 731 throughout the Warranty period, or a minimum of two times a warranty period whichever is greater, at no further cost to the City.
- 30.5 Nothing contained in the contract shall be construed to establish a period of limitation with respect to any other obligation that the Successful Bidder might have under the contract.
- 30.6 The establishment of the time period of two (2) years after the date of final acceptance, or such longer period of time as may be prescribed by law, or by the Terms of any Warranty required by the contract relates only to the specific obligation of the Successful Bidder to correct the Work, and has no relationship to the time within which its obligation to comply with the contract documents may be sought to be enforced, nor to the time within which proceedings may be commenced to establish the Successful Bidder's liability with respect to his obligations other than specifically to correct the Work.
- 30.7 If this contract in its specifications requires that specific deliverables must perform as a system, this representation and Warranty shall apply to the deliverables, individually, in combination with each other, and as a system. Where the Successful Bidder will be providing any component of a deliverable from or through a Subcontractor, the Successful Bidder shall cause its Subcontractor to comply with this representation and Warranty with respect to the component to be provided by such Subcontractor.
- 30.8 Where the deliverable being provided by the Successful Bidder has an interface with any other product and such interface is necessary for the functionality, operation or performance of its deliverable, the Successful Bidder shall ensure that such product complies with this representation and Warranty and such interface does not in any way impair the ability of its deliverable to comply with this representation and Warranty.

- 30.9 At the Corporate Security Lead's request made in writing at any time before or within 90 calendar days (or such other time period as designated by the City in writing) of its acceptance of the deliverable, the Successful Bidder will, at no charge to the City, demonstrate the compliance techniques and test procedures to be followed by the Successful Bidder or the City or its authorized agent to confirm that the deliverable complies with this representation and Warranty.
- 30.10 Where the Successful Bidder advises the City that its deliverable is not able to comply with this representation and Warranty at this time but will be able to do so by a specified date, the City may at its sole discretion accept the deliverable on the condition that there is compliance by the specified date; however, the City is not obligated or liable to make payment for the deliverable until such condition is satisfied.
- 30.11 In the event of any breach of this Warranty and representation, the remedies available to the City shall include but not be limited to:
- The Successful Bidder restoring the deliverable to the same level of performance as represented and warranted herein;
  - The Successful Bidder repairing or replacing the deliverable with a deliverable conforming with this representation and Warranty;
  - The Successful Bidder granting or securing for the City or its authorized agent permission to make any modifications necessary to make the deliverable compliant with this representation and Warranty and arranging for any necessary waivers of moral rights or other intellectual property rights to make such modifications; and
  - The Successful Bidder granting the City or its authorized agent access to the source code for the information technology used in the deliverable in order to make any modifications necessary to make the deliverable compliant with this representation and Warranty or securing for the City the necessary permission for such access and arranging for any necessary waivers of moral rights or other intellectual property rights to make such modifications, 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 Successful Bidder's sole expense.
- 30.12 The Successful Bidder represents and warrants that any restoration, repair or replacement made will not corrupt any data of the City or introduce any viruses into the City's system. The Successful Bidder agrees that any modification made pursuant to subparagraph 30.5 or 30.6, above, is the property of the City, including all copyright and other intellectual property rights pertaining thereto.
- 30.13 This Warranty shall survive cancellation or other termination of this contract.
- 30.14 Nothing in this representation and Warranty shall be construed to limit any rights or remedies (including indemnities) otherwise available to the City under this contract or at law or equity; and nothing in the contract shall limit the scope of this representation and Warranty and any rights or remedies set out herein, and, in particular, no waiver or disclaimer set out in such agreement (or made otherwise) shall operate to limit the Successful Bidder's liability under this representation and Warranty.

- 30.15 In the event that the Successful Bidder fails to make good such defects within a stipulated time, the City reserves the right to have the Work performed by other qualified suppliers. All costs incurred by the City are to be paid by the Successful Bidder.
- 30.16 The Successful Bidder after the date of final acceptance of all work/orders as determined by the City, or designated portion thereof, provide, in addition to the Warranty Certification a preventative Maintenance schedule for the duration of the Warranty period.
- 30.17 The Successful Bidder shall complete all manufacturer Warranty registration for applicable Products as per the Warranty Terms purchased and provide proof of registration to the City within 30 calendar days of installation.

## 31.0 Warranty Service

- 31.0.1 The Successful Bidder shall provide and maintain its call center telephone number(s) and call placement procedures to City of Toronto Corporate Security and the SCC for dispatching Personnel for warranty services. The telephone number(s) must be a local (Toronto) 10 digit number. The City will not accept any number that results in long distance charges for the City when placing a call from the City of Toronto.
- 31.0.2 The Successful Bidder's Call Centre telephone number(s) must be answered by a live operator and available during Daytime hours (06:00-18:00hrs, Monday through Friday), excluding statutory holidays.
- 1.0.3 The Successful Bidder must also maintain an email address for warranty service requests. Automated email responses are not acceptable.
- 6.0.4 The Successful Bidder shall provide contact lists (one list for during daytime hours and a separate list for afterhours) to ensure the required warranty service resolution times are met.

## 32.0 Service Calls

- 32.1.0 The technician must report to the work site, diagnose the issue and provide a corrective maintenance solution of the initial call for corrective maintenance services. The Vendor must obtain a work order from the City Designated that details the products and number of labour hours required prior to ordering Products and performing any warranty services resulting from the service call.
- 32.1.1 Upon arrival at the location, the technician must notify the Corporate Security Control Centre by phone at 416-397-0000;

32.1.2 Upon departure of the location, the technician must notify the Corporate Security Control Centre by phone at the end of each day, by email to [SecSysSD@toronto.ca](mailto:SecSysSD@toronto.ca), and provide a required, future steps to be taken.

### 32.2 Service Call Resolution Times

Warranty Service Call Priority	Resolution Time
(1) Urgent	48 HOURS
(2) High	Five (5) Business Days

## 33.0 Pass-Through Warranties.

- 33.1 The Successful Bidder will, to the extent permissible, agrees to pass through to the City of Toronto any warranties given by its third party vendors in connection with hardware, software or other products or services used by the Successful Bidder to provide the Services to the extent permitted by the terms and conditions of such warranties and pass through to the City of Toronto all available warranties and provide all available (including extended) applicable original equipment manufacturer and additional warranties for third party Equipment used to provide the Services. The Successful Bidder will obtain and pass through to the City of Toronto any warranties required by the specifications for Equipment procured on behalf of the City of Toronto. The Successful Bidder will, to the extent permissible, pass through to the City of Toronto all available warranties and provide all available (including extended) applicable original equipment manufacturer and additional warranties for Equipment owned by the City of Toronto.
- 33.2 The Successful Bidder shall secure from the applicable Equipment or third party Software manufacturers, and assign and pass through to the City of Toronto, at no additional cost to the City of Toronto, such warranties as may be available with respect to such Equipment and Software. Such assignment shall not, however, relieve the Successful Bidder of any of the warranty obligations contained herein. In the event such warranties are not assignable to the City of Toronto, the Successful Bidder shall enforce, as necessary, such warranties on behalf of the City of Toronto.
- 33.3 In the event that Contractor purchases Goods or Materials in its own name for incorporation in the Work delivered to the City of Toronto, and the Successful Bidder receives a warranty from the vendor of such Goods or Materials, the Successful Bidder shall ensure that such warranty is passed through to, and is enforceable by, the City of Toronto.

## 34.0 Compliance with Standards

The Successful Bidder shall maintain a high level of workmanship and comply with the following codes, standards and procedures. Bidders that have completed and submitted the Confidentiality Agreement will be provided with copies of the City of Toronto standards listed below at the Mandatory Site Meeting.

1. City of Toronto Corporate Cabling Standards
2. City of Toronto Corporate IT Standards
3. City of Toronto Corporate Security Standards
4. City of Toronto Video Security Surveillance Policy
5. City of Toronto Corporate Security Intellex DVR Installation, Configuration, Programming and Naming Standard
6. City of Toronto Corporate Security CCTV and AV Systems Installation Standards
7. City of Toronto Corporate Security CCTV and AV Maintenance Standards
8. City's Workplace Violence Policy
9. City of Toronto Corporate Security Access Control Systems Installation Standards
10. City of Toronto Corporate Security Intercom System Installation Standards
11. City of Toronto Corporate Security Access Control and Intercom System Maintenance Standards
12. City of Toronto Corporate Security – Security Schedules – Drawing Typicals
13. City of Toronto Corporate Security Structured Cabling Standards
14. City of Toronto, Toronto Water Plant Structured Cabling System Standard
15. City of Toronto Acceptable Use Policy
16. City of Toronto CityNet Acceptable Use Agreement
17. Transport Canada Reference Manual for Using Closed Circuit Television in Counter-Terrorism Activities.
18. AC transients UL 964
19. Access Control equipment manufacturer's specifications, latest issue
20. American Society for Testing Materials (ASTM)

21. ANSI/EIA-310 and its addendum
22. ANSI/TIA/EIA-568-B.1 and its addendum
23. ANSI/TIA/EIA-568-B.3 and its addendum
24. Applicable local Building Codes
25. Association Architectural Graphic Standards for Security System Layout SIA/APSC AG-01-1995.12 (R2000.03)
26. BICSI Information Transport Systems Installation Manual – Most current Edition
27. BICSI Network Design Reference Manual – Most current Edition
28. BICSI Telecommunications Distribution Methods Manual – Most current Edition
29. Communications: IEEE RS232C and RS485
30. Canadian Standards Association (CSA International)
  - CSA C22.1-[98], Canadian Electrical Code, Part 1 (18th edition) Safety Standard for Electrical Installations.
  - CAN/CSA-C22.3 No.1-[M87 (R1997)], Overhead Systems.
31. Design: MIL 275E
32. Electrical Standards Authority
33. Electrostatic immunity: IEC 801.2 level 4
34. EMI emissions: FCC part 15
35. Institute of Electrical and Electronic Engineers (IEEE)
36. Intercom equipment manufacturer's specifications, latest issue
37. Manufacturing: ISO 9003
38. National Fire Protection Association (NFPA®)
  - NFPA® pamphlet 51B
  - NFPA® 70, National Electric Code.

- NFPA® 730, Guide for Premises Security 2008 or latest edition
- NFPA® 731, Standard for the Installation of Electronic Premises Security Systems, 2008 or latest edition

39. Ontario Building Code

40. Ontario Fire Code

41. Parks Canada - Standards and Guidelines for the Conservation of Historic Places in Canada

42. Process Control System Implementation Manual

43. Underwriters' Laboratories

- CAN/ULC-S302-M91 - Standard for Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, safes and Vaults
- CAN/ULC-S304-06, Signal Receiving Centre and Premise Burglar Alarm Control Units.
- CAN/ULC-S317-[1996], Installation and Classification of Closed Circuit Video Equipment (CCVE) Systems for Institutional and Commercial Security Systems.
- CAN/ULC-S319-05 Electronic Access Control Systems
- CAN/ULC-S3-1-M88 Standard for Central and Monitoring Station Burglar Alarm systems.
- CAN/ULC-S524-06 – Installation of Fire Alarm Systems
- CAN/ULC-S559-04 – Equipment for Fire Signal Receiving Centres and Systems
- CAN/ULC-S561-03 – Installation and Services for Fire Receiving Centres and Systems
- UL 1076-[1995], Standard for Safety for Proprietary Burglar Alarm Units and Systems.
- UL 1635 Digital Alarm Communicator System Units
- UL 1981 Central Station Automation Systems
- UL 294-[1999], Standard for Safety for Access Control System Units.
- UL 681 Installation and Classification of Burglar and Holdup Alarm Systems
- UL Testing Bulletin
- Underwriters Laboratories (UL) Cable Certification and Follow Up Program

## 35.0 Manufactures List

- Aegis
- ADI
- ADT Canada
- Aiphone Corporation
- Alarm Saf
- Altronix Corporation
- Alpha Technologies
- American Dynamics
- Amseco
- Ameta International Co. Ltd.
- APC by Schneider Electric
- Arecont Vision
- Asterix Security Hardware International Inc.
- Anixer
- ASSA ABLOY Canada
- AutoGate Inc.
- Automatic Systems America Inc.
- Avigilon
- AWID
- Axis Communications, Inc.
- Berk-Tek
- Black Box Network Services
- Boon Edam, Inc.
- Bogen Communication, Inc.
- Bosch Security Systems
- Camden Door Controls
- Cansec Systems Ltd.
- CCTV Direct
- CDVI Americas Ltd.
- CDW
- Cisco Systems
- Commend Inc.
- Computar
- D-Link Canada Inc.
- Dahua Technology
- Dedicated Micros
- Detex
- Digital Watchdog
- DIRAK Inc.
- DITEK Corporation
- DoorKing Inc.

- DSC
- DWG Distribution
- Eyesonic Enterprises Inc.
- FLIR Fibre Technologies
- GAI-Tronics
- RBH Access Technologies Inc.
- RBtec Inc.
- Rofu Security International Group
- Rutherford Controls Int'l. Corp.
- Safety Technology International Inc. (STI)
- Samsung Techwin America
- Santeri Industries
- Schlage
- Schneider Electric
- Senstar Corporation
- Sentrol Inc
- Sennetech Inc.
- Sentry Security Systems
- Smart Vision Direct Inc.
- Software House
- Sony of Canada Ltd.
- Southern Folger
- Southwest Microwave, Inc.
- SPECO Technologies
- Spectris Canada Inc.
- Systech Corporation
- Talk-A-Phone
- TOA Canada Corporation
- Toppan
- Tri-Ed, an Anixter Company
- Tri Tech
- Turnstile Security Systems Inc.
- Tyco Security Products
- Ultratech
- United Security Products
- Visonic
- Von Duprin
- WatchNET Inc.
- Weiser
- Winbo International Ltd.
- Zebra

## 36.0 Supplementary Forms & Policies

- 1 FORM 1 – Confidentiality and Non-Disclosure Declaration
- 2 FORM 2 – Programming and Installation Standards
- 3 FORM 3 - Security Typical
- 4 FORM 4 - IP CCTV Network Cabling Guideline for City Facilities
- 5 Declaration of Compliance with Anti-Harassment/Discrimination Legislation & City Policy / Workplace Violence
- 6 Statutory Declaration (Occupational Health & Safety)
- 7 IT Acceptable Usage Policy

# FORM 1

## CONFIDENTIALITY AND NON-DISCLOSURE DECLARATION

**THIS ACKNOWLEDGEMENT AND DECLARATION** is given to the City of Toronto (the “City”) as of the \_\_\_\_ day of \_\_\_\_\_, 20\_\_ by \_\_\_\_\_ (the “Firm”).

**WHEREAS** the Firm has elected to attend, the Mandatory Pre-bid Meeting held in connection with the City’s Request for Quotations No. XXXXXX for Security Systems and services. The scope of work consists of on-demand services and the Supply/Install of City of Toronto Security Systems for various locations throughout the City of Toronto, all in accordance with the City of Toronto's Purchasing Policies and the City of Toronto Fair Wage Policy and Labour Trades Contractual Obligations in the Construction Industry.

**NOW THEREFORE**, in consideration of the above, the sufficiency thereof is hereby acknowledged, the Firm agrees and declares as follows:

That all information provided at the Mandatory Site Meeting is confidential and is being provided to the Firm only for the purpose of submitting a Quotation in response to the RFQ and, if successful, for the purpose of providing the services under a contract arising out of the RFQ; and

That all correspondence, documentation and information provided by the City to the Firm in connection with, or arising out of the RFQ:

- a) Is and shall remain the property of the City;
- b) Shall be treated by the Firm as confidential;
- c) Shall not be disclosed, in whole or in part, to any third party;
- d) Shall not be used for any purpose other than for replying to the RFQ, and for fulfillment of any subsequent contract arising out of the RFP.

IN WITNESS WHEREOF the Firm executes this Declaration through the signature of its duly authorized signatory.

ON BEHALF OF \_\_\_\_\_  
(Name of Firm)

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

I have the authority to bind the Firm.

## FORM 2

**City of Toronto Programming and Installation Standards – released to successful bidder after Form 1 –  
CONFIDENTIALITY AND NON-DISCLOSURE DECLARATION submitted**

## FORM 3

**City of Toronto Security Typical – released to successful bidder after FORM 1 – CONFIDENTIALITY AND NON-DISCLOSURE DECLARATION**

## FORM 4

**IP CCTV Network Cabling Guideline for City Facilities – released to successful bidder after FORM 1 –  
CONFIDENTIALITY AND NON-DISCLOSURE DECLARATION**



## Declaration of Compliance with Anti-Harassment/Discrimination Legislation & City Policy

Organizations/individuals in Ontario, including the City of Toronto, have obligations under the Ontario Human Rights Code, the Occupational Health and Safety Act, the Employment Standards Act, the Accessibility for Ontarians with Disabilities Act, the Criminal Code of Canada and the Charter of Rights and Freedoms. In addition, the City of Toronto also has policies that prohibit discrimination on the additional grounds of political affiliation or level of literacy, subject to the requirements of the Charter. Organizations are required to have and post policies, programs, information, instruction, plans and/or other supports, and an **appropriate** internal process available to their employees and service recipients to prevent, address and remedy discrimination, racism, harassment, hate and inaccessibility complaints under the applicable legislation and including the additional grounds of discrimination prohibited under City policy. Individuals are obliged to refrain from harassment/hate activity.

The City of Toronto requires all organizations and individuals that contract with the City to sign the following Declaration of Compliance with Anti-Harassment/Discrimination Legislation & City Policy. This Declaration must be signed by your organization and submitted with the contract or Letter of Understanding. The name of your organization and the fact that you have signed this declaration may be included in a public report to City Council.

**Declaration:**

**I/we uphold our obligations under the above provincial and federal legislation. In addition, I/we uphold our obligations under City policies which prohibit harassment/discrimination on a number of grounds including political affiliation and level of literacy.**

**WHERE LEGALLY MANDATED I/we have in place the necessary policies, programs, information, instruction, plans and/or other supports that are consistent with our obligations, and I/we have an internal process available to my/our employees and service recipients to prevent, address and remedy discrimination, racism, harassment, hate and inaccessibility complaints. I/we agree that I/we shall, upon the request of the City, provide evidence of the policies, programs, information, instruction, plans and other supports and an appropriate internal complaint resolution process required under this Declaration which is sufficient to allow the City to determine compliance. I/We acknowledge that failure to demonstrate compliance with this declaration to the satisfaction of the operating Division, in consultation with the City Solicitor, may result in the termination of the contract.**

Multilingual Services: 311 and TTY 416-338-0889. For further information, consult the [Equality, Diversity and Human Rights web page](http://www.toronto.ca/diversity) at <http://www.toronto.ca/diversity>

**Applicant Information (Organization or Individual)**

Organization Name		Position Title	
Organization Representative or Individual First Name		Organization Representative or Individual Last Name	
<input type="checkbox"/> Check this box if First Name and Last Name do not apply to you because you have either a registered Birth Certificate or Change of Name Certificate bearing a Single Name. Provide your name below.			
Single Name			
Street Number	Street Name	Suite/Unit Number	
City/Town	Province	Postal Code	Telephone Number
Organization Representative or Individual Signature			Date (yyyy-mm-dd)



<p><u>Human Resources Policies</u>  <b>Workplace Violence (2019)</b></p> <p>Category: <b>Health and Safety</b>          Sub-Category: <b>General</b></p>	
--	---

**Policy Statement**                      The City of Toronto is committed to working with its employees to provide a safe work environment. The City will not tolerate any acts of violence and will take all reasonable and practical measures to prevent violence and protect employees from acts of violence. Appropriate remedial, disciplinary, and/or legal action will be taken according to the circumstances.

**Purpose of Workplace Violence Policy**                      This policy is supported by the Guidelines for Implementing the Workplace Violence Policy, a Workplace Violence and Threat Report form, a Supervisor Checklist for Workplace Violence, and an information sheet. The policy and its supporting guidelines are intended to:

1. Maintain a work environment free from workplace violence
2. Provide a definition of workplace violence
3. Identify the responsibilities of the workplace parties to maintain a workplace free of actual, attempted or threatened violence
4. Establish measures and procedures for summoning immediate assistance when workplace violence occurs or is likely to occur
5. Establish measures and procedures for workers to report incidents of workplace violence and for the City to investigate and deal with incidents or complaints immediately
6. Provide guidance to divisions on establishing their Workplace Violence program

**Application**                                      *The Workplace Violence policy applies under any circumstances in which City employees experience workplace violence, as defined below. It applies to all employees, contractors of the City, volunteers, students, clients of City services, any person engaged in business with the City, and visitors to City properties.*

*The City's Human Rights and Anti-Harassment Policy should be consulted regarding issues of personal harassment and harassment related to discrimination and inequitable work practices.*

**Definitions**                                      For the purpose of this policy, violence includes:

- the exercise of physical force by a person against a worker, in a workplace, that causes or could cause physical injury to the worker
- the exercise of physical force by a person against another person, in a workplace, that causes or could cause physical injury to the worker
- an attempt to exercise physical force against a worker that could cause physical injury to the worker
- a statement or behaviour that it is reasonable for a worker to interpret as a threat to exercise physical force against the worker, in a workplace, that could cause physical injury to the worker

*The City's Human Rights and Anti-Harassment Policy addresses harassment or intimidation (e.g., behaviours that demean, embarrass, or humiliate and are known or would be expected to be unwelcome).*

**Responsibilities**                                      All employees are responsible for preventing and reporting acts of violence that threaten or perceive to threaten a safe work environment.

**Divisional senior management will ensure that:**

- A divisional workplace violence program is established
- Reasonable preventative measures are undertaken to protect employees and others in City workplaces from workplace violence
- Take reasonable preventative measures to protect employees and others in City workplaces from workplace violence
- Ensure that a process for centralized tracking and review of workplace violence incidents is established and implemented
- Ensure that workplace violence risk assessments are completed, reviewed, revised when needed and reported
- Post this policy in a conspicuous location in each workplace
- Establish and maintain a process for reporting and responding to incidents of violence
- Ensure that the process for reporting and responding to incidents of violence is communicated, maintained and followed
- Ensure that this policy is reviewed at least annually

**Managers/supervisors will:**

- Understand and uphold the principles of this policy
- Communicate this policy and its guidelines to all employees
- Conduct workplace violence risk assessments to determine whether the nature of the workplace, the type of work or conditions of work may place employees at risk of violence
- Consult with Joint Health & Safety Committees (JHSCs)/OHS Representatives, assigned People, Equity & Human Rights (PEHR) /divisional health & safety staff, and where appropriate, Corporate Security, in conducting risk assessments, and develop practical measures and procedures to control identified risks
- Take all reasonable and practical measures to minimize or eliminate risks identified through the risk assessment process, workplace inspections, or the occurrence of a workplace violence incident
- Review risk assessments at least annually, as well as when there are changes to the nature of the workplace, the type of work or the conditions of work. Revise the assessment, as needed
- Conduct further risk assessments when an increase in the number or severity of workplace violence incidents is noted to ensure that appropriate measures are in place to minimize or eliminate risks
- Communicate the results of workplace violence risk assessments and measures to minimize or eliminate risks to staff.
- Provide results of risk assessments (initial and updated) to joint health and safety committees/health and safety representatives
- Maintain and follow the process in the *City's Investigation and Reporting of Work-Related Injuries and Incidents policy* for reporting, investigating, documenting, and debriefing incidents of violence
- Respond promptly when an employee reports being subjected to, witnessing, having knowledge of workplace violence or having reason to believe that workplace violence may occur and take appropriate action.
- Address immediately all incidents of workplace violence, and not condone or permit any behaviour contrary to this policy. Exceptions to this must be clearly defined in the divisional procedures, describing specific behaviours that are unacceptable (e.g., unacceptable behaviours among a specific client group such as young children or clients with developmental, cognitive, or psychiatric disabilities). This exception must be communicated to staff but must not

condone behaviours contrary to this policy.

- Ensure that all known incidents of workplace violence are investigated. To the extent appropriate based on the nature of each incident and the actual or potential threat it posed to worker safety:
  - consult with other parties (e.g., Corporate Security, Health & Safety staff, JHSCs/OHS Representatives, Employee Health and Rehabilitation, Employee Assistance Program, Human Rights Office, Toronto Police Services)
  - take all reasonable and practical measures to minimize or address risks identified by the incident
  - document the incident, its investigation, and corrective action taken
  - promptly share the results of the investigation and corrective actions taken with the joint health and safety committee/health and safety representative and the workers involved in the incident
- Ensure workers are made aware of their rights to:
  - have workplace violence incidents investigated when they are reported
  - report incidents of physical assault or threats of physical assault to the police
  - support from management when reporting incidents of physical assault or threats of physical assault to the police (e.g. time for interactions with the police and making accessible to the police information in the employer's possession with respect to the incident)
- Take all reasonable and practical measures to protect workers, acting in good faith, who report workplace violence or act as witnesses, from reprisal or further violence
- Take every precaution reasonable in the circumstances for worker protection if they become aware, or ought reasonably to be aware, that domestic violence that would likely expose a worker to physical injury may occur in the workplace
- Review annually, in conjunction with review of risk assessments, the effectiveness of actions taken to minimize or eliminate workplace violence and make improvements to divisional procedures, as required
- Provide information to workers, including appropriate personal information, related to a risk of workplace violence from a person with a history of violent behaviour
- Provide workers with information and instruction appropriate for the worker on the City's workplace violence policy and program

**People, Equity & Human Rights (PEHR)/ Divisional Occupational Health and Safety staff will:**

- Assist management to implement this policy, develop divisional procedures, and initiate the annual review of the policy and guidelines

**Joint Health and Safety Committees/OHS Representatives will:**

- Review the Workplace Violence Risk Assessment results and provide recommendations to management to reduce or eliminate the risk of violence
- Review all reports forwarded to the JHSC regarding workplace violence and other incident reports as appropriate pertaining to incidents of workplace violence that result in personal injury or threat of personal injury, property damage, or police involvement
- Participate in the investigation of critical injuries (e.g., incidents that place life in jeopardy, result in substantial blood loss, fracture of leg or arm, etc.)

- Recommend corrective measures for the improvement of the health and safety of workers
- Respond to employee concerns related to workplace violence and communicate these to management
- Participate in the review of the policy and guidelines for continuous improvement

In addition, JHSCs/OHS Representatives may participate in the investigation of reported incidents that result in personal injury or have the potential to result in injury.

**The Occupational Health and Safety Coordinating Committee will:**

- Review annually the effectiveness of the policy and guidelines and make changes as required by consulting with management staff and employee representatives

**All employees will:**

- Maintain a safe work environment, whenever possible
- Not engage in or ignore violent, threatening, intimidating or other disruptive behaviours
- Report promptly and provide details to their supervisor (or the appropriate alternative listed in the attached guidelines) any incident where the employee is subjected to, witnesses, or has knowledge of workplace violence, or has reason to believe that workplace violence may occur

<b>Reprisal</b>	This policy prohibits reprisals against individuals, acting in good faith, who report incidents of workplace violence or act as witnesses. Management will take all reasonable and practical measures to prevent reprisals, threats of reprisal, or further violence. Reprisal is defined as any act of retaliation, either direct or indirect.
<b>Authorities</b>	<i>Occupational Health and Safety Act of Ontario (current)</i> <i>Criminal Code of Canada (current)</i> <i>City of Toronto Corporate Occupational Health and Safety Policy (reviewed annually)</i>
<b>Previous Versions</b>	February 18, 2002 March 25, 2010 February 28, 2012 December 5, 2012 September 16, 2014 February 10, 2016 December 6, 2016 September 27, 2017 OHSCC-endorsed and City Manager-approved
<b>Endorsed by:</b>	Occupational Health and Safety Coordinating Committee (OHSCC), October 30, 2001 Reviewed and re-endorsed by OHSCC, December 12, 2018
<b>Guidelines</b>	<u><i>Guidelines for Implementing the Workplace Violence Policy</i></u>
<b>Effective</b>	January 1, 2019 - December 31, 2019

<b>Approved by</b>	City Manager
<b>Date Approved</b>	February 4, 2013
<b>Reviewed and re-approved by OHSCC</b>	December 12, 2018
<b>Related information</b>	<a href="#"><u>Human Rights and Anti-Harassment/Discrimination Policy</u></a> <a href="#"><u>City of Toronto Corporate Occupational Health and Safety Policy</u></a> <a href="#"><u>Investigation and Reporting of Work-Related Injuries and Incidents Policy</u></a> <a href="#"><u>Guidelines for Implementing the Workplace Violence Policy</u></a>
<b>Related links - external</b>	<a href="#"><u>The Occupational Health and Safety Act of Ontario</u></a> <a href="#"><u>Criminal Code of Canada</u></a>



[Go back](#)



RFQ «QuotationRequestNumber»

**STATUTORY DECLARATION**  
(Occupational Health & Safety)

PROVINCE OF ONTARIO )  
JUDICIAL DISTRICT OF YORK )

IN THE MATTER OF RFQ NO. \_\_\_\_\_ AND ANY ENSUING CONTRACT  
BETWEEN

\_\_\_\_\_

(Company Name)

- AND -

City of Toronto

I, \_\_\_\_\_ of the City/Town/Village of \_\_\_\_\_ in the  
Province

(Name)

of \_\_\_\_\_, do solemnly declare the following:

(Name of Province)

1. I am the \_\_\_\_\_ of the \_\_\_\_\_ and as such

(Insert Title)

(Insert Company Name)

have knowledge of the matters herein stated.

2. \_\_\_\_\_ is a sole proprietorship/partnership/corporation with its head office

(Company Name)

located at \_\_\_\_\_ and has carried on business as  
a \_\_\_\_\_

(contractor/state other type of

business)

since on or about \_\_\_\_\_

(Insert Date)

3. \_\_\_\_\_ since \_\_\_\_\_ had in place a Health and Safety

Policy

(Company Name)

(Insert Date)

under Section 25(2) (j) of the *Occupational Health and Safety Act*, R.S.O. 1990, c. 0.1 as amended, (the "Act")  
and

has/have developed and maintain(s) on an annual basis a program to implement the written Occupational Health  
and Safety

Policy. A copy of the policy and program for \_\_\_\_\_ (Insert Company Name) will be  
delivered to the

City of Toronto upon request by the City and will be available for inspection at the City of Toronto, solely for the  
purposes of



the above noted Contract.

4. \_\_\_\_\_ since \_\_\_\_\_ had in place a Workplace Violence and a  
 (Company Name) (Insert Date)

Workplace Harassment Policy under Section 32.0.1(1) of the *Occupational Health and Safety Act*, R.S.O. 1990, c. 0.1 as amended, (the "Act") and has/have developed and maintain(s) on an annual basis a program to implement the written Workplace Violence and Workplace Harassment Policy. A copy of the policy and program for \_\_\_\_\_ (Insert Company Name) will be delivered to the City of Toronto upon request by the City and will be available for inspection at the City of Toronto, solely for the purposes of the above noted Contract.

5. \_\_\_\_\_ (Insert Company Name) will employ for the Work under this Contract a supervisor or supervisors who are competent persons as defined by section 1(1) of the Act, and specifically a person or persons who:

- (a) are qualified because of knowledge, training and experience to organize the Work and its performance;
- (b) are familiar with the Act and the regulations made thereunder that apply to the Work; and
- (c) have knowledge of any potential or actual danger to health and safety associated with the Work.

6. \_\_\_\_\_ (Insert Company Name) will employ for the purpose of

this project the following competent supervisors:

\_\_\_\_\_  
 (Insert name of supervisors)

No supervisors other than those named shall work on this Contract.

7. The supervisors employed by \_\_\_\_\_ (Insert Company Name) has successfully completed the necessary health and safety courses to be considered a competent person to undertake the Work described in the Contract.

AND I/We make this solemn Declaration conscientiously believing it to be true, and knowing that it is of the same force and

effect as if made under oath and by virtue of "The Canada Evidence Act".

DECLARED BEFORE ME AT THE )  
 )  
 OF )  
 )  
 IN THE ) \_\_\_\_\_  
 ) Signing Officer for Company  
 THIS DAY OF 20\_\_ )  
 )  
 A Commissioner etc. )

## City of Toronto Acceptable Use of Information Technology Assets Policy

### 1. Policy Statement

- 1.1 The City of Toronto provides Authorized Users with access to the City's Information Technology Assets to be used for the purpose of conducting legitimate business activities and advancing the goals and objectives of the City of Toronto.
- 1.2 This Policy establishes principles and requirements for the acceptable use of the City's Information Technology Assets.

### 2. Definitions

- 2.1 **Accountability Officer(s)** refers to the Auditor General, Integrity Commissioner, Lobbyist Registrar and the Ombudsman at the City of Toronto.
- 2.2 **Authorized Users** are all individuals who have been granted access to the City's Information Technology Assets. This includes, but is not limited to, employees, consultants, contractors, subcontractors, individuals on secondment to the City, students and volunteers at the City of Toronto and Accountability Officers and anyone working or volunteering for or in their Offices subject to Section 3-10 F(5), Chapter 3, Accountability Officers, of the Toronto Municipal Code.
- 2.3 **Confidential Information** includes, but is not limited to, privileged information, draft by-laws or staff reports, third party information, personal information, technical or financial or scientific information and any other information collected, obtained or derived for or from City records that must or may be kept confidential under the *Municipal Freedom of Information of Privacy Act*, the *Personal Health Information Protection Act, 2004* or the *City of Toronto Act, 2006*.
- 2.4 **Information Technology Assets** are any system, service, hardware, and network assets that are owned by or supplied to Authorized Users by the City. This includes, but is not limited to, desktop computers, monitors, printers, notebooks, mobile devices, digital projectors, scanners, storage devices, networks and network devices, software, internet access, email, communication and business applications, telephones and voice mail, facsimile machines, and photocopiers.
- 2.5 **Systems Monitoring** refers to monitoring the City's Information Technology Assets used by Authorized Users for the collection and review of aggregate,

broad-based, or statistical data to assess, maintain, update or ensure reliability, security, confidentiality and integrity of City's Information Technology Assets. Systems monitoring is not directed at an identifiable individual(s).

- 2.6 **User Monitoring** refers to recording, accessing and reviewing or analyzing one or more identified Authorized User's activity on, or use of, the City's Information Technology Assets.

### 3. Application

- 3.1 This Policy applies to all Authorized Users with access to any of the City's Information Technology Assets.
- 3.2 Accountability Officers are responsible for the application of and compliance with this Policy in their Offices, including user monitoring where required, pursuant to Chapter 3, Accountability Officers, of the Toronto Municipal Code.
- 3.3 Exceptions
  - 3.3.1 This Policy does not apply to Members of Council or anyone working or volunteering for or in their offices. Council Members are governed by the Code of Conduct for Members of Council, the Human Resources Management and Ethical Framework for Members' Staff, and applicable City policies and protocols.

### 4. Principles

- 4.1 The City's Information Technology Assets are corporate resources and are to be used in accordance with this Policy and other applicable City of Toronto by-laws, policies and relevant federal and provincial legislation.
- 4.2 Authorized Users shall exercise good judgment and responsibility when using the City's Information Technology Assets.
- 4.3 The City's Information Technology Assets shall be used in an ethical and professional manner.
- 4.4. The City's Information Technology Assets will be used in a manner that safeguards the integrity, privacy and confidentiality of the City's assets, information, and data.
- 4.5 Authorized Users are responsible for their use of the City's Information Technology Assets at all times, including non-business hours.

- 4.6 Authorized Users shall not expect absolute privacy when using the City's Information Technology Assets, including such limited personal use as permitted in accordance with Section 7 of this Policy.
- 4.7 Authorized Users shall not have any expectation that any use of City's Information Technology Assets, including limited personal use, is exempt from Systems Monitoring and/or User Monitoring in accordance with this Policy.
- 4.8 Each Authorized User's Manager or Supervisor shall ensure that the Authorized User is aware of and understands their role and responsibility under this Policy and related City by-laws, policies and relevant provincial and federal legislation.

## **5. User Accountability and Responsibility**

### **5.1 Security**

- 5.1.1 Authorized Users are to exercise good judgment and reasonable care in protecting Information Technology Assets from theft, damage or illegal access and against systems designed to disrupt, damage or place excessive load on the assets.
- 5.1.2 Authorized Users are responsible for safeguarding, protecting, and not sharing password(s) used to access the City's Information Technology Assets.
- 5.1.3 Any breach to the security of City's information technology systems or damage to or loss of Information Technology Assets will be immediately reported by the Authorized User to the I&T Service Desk and their Supervisor/Manager.

### **5.2 Information Management**

- 5.2.1 All Authorized Users are responsible for the proper management of information in accordance with related provincial and federal legislation, and City of Toronto by-laws and policies referenced in Section 11 of this Policy.
- 5.2.2 Authorized Users must protect confidential information that belongs to the City, its service users, residents, partners or vendors, in accordance with the requirements of relevant provincial, and federal legislation, contractual restrictions, and related City of Toronto by-laws, and policies.

- 5.2.3 When conducting City business, Authorized Users are responsible for maintaining an accessible record and information in accordance with City by-laws, policies and relevant provincial and federal legislation.
- 5.2.4 All information, records and data related to City business and created or legally acquired using the City's Information Technology Assets must be stored on the City's network server or on an Information Technology Asset owned or under contract to the City.
- 5.2.5 Authorized Users are encouraged not to use system, service, hardware, and network assets not owned by or supplied by the City for the performance of the Authorized User's duties and responsibilities. Authorized Users shall not, under any circumstances, use any system, service, hardware, and network assets not owned by or supplied by the City for the performance of the Authorized User's duties and responsibilities where such use:
  - 5.2.5.1 compromises the security of the City's Information Technology Assets;
  - 5.2.5.2 results in a breach of provincial or federal legislation, or of the City of Toronto by-laws and policies referenced in Section 11 of this Policy;
  - 5.2.5.3 results in the release of confidential information that belongs to the City, its service users, residents, partners or vendors, contrary to the requirements of relevant provincial and federal legislation contractual restrictions, or related City of Toronto by-laws and policies; and/or
  - 5.2.5.4 results in the City incurring any unauthorized costs associated with Authorized Users accessing the City's network remotely.
- 5.2.6 Authorized Users who elect to use system, service, hardware, and network assets not owned by or supplied by the City for the performance of the Authorized User's duties and responsibilities may, through such use, make the system, service, hardware, and network assets used for this purpose subject to provincial and federal access to information legislation contractual restrictions, and related City of Toronto by-laws and policies, and shall cooperate with the City in fulfilling any resultant obligations that arise from such use.
- 5.2.7 Authorized Users who elect to use system, service, hardware, and network assets not owned by or supplied by the City for the performance

of the Authorized User's duties and responsibilities shall ensure that information, records, and data created, accessed, acquired, managed, or reviewed through such use is moved to and stored on the City's Information Technology Assets at the first available opportunity, following which it is deleted from the system, service, hardware, and network assets not owned by or supplied by the City.

### 5.3 Remote Access

- 5.3.1 Authorized Users with remote access to the City's network must connect using authorized methods and systems and ensure that the Information Technology Asset or the system, service, hardware, and network assets not owned by or supplied by the City is safe to use and will not negatively impact the City's network.
- 5.3.2 Authorized Users must maintain the privacy, confidentiality and integrity of corporate business information accessed through remote access.
- 5.3.3 All corporate information produced, accessed, or altered through remote access must be stored on the City's network or on an Information Technology Asset owned or under contract to the City.
- 5.3.4 The City will not incur any unauthorized costs associated with Authorized Users accessing the City's network remotely.
- 5.3.5 The City retains the right to terminate Authorized Users' remote access at any time.

## 6. Ownership

### 6.1 Assets

- 6.1.1 The City's Information Technology Assets are the sole property of the City of Toronto.
- 6.1.2 All Authorized Users must provide, when requested by management or delegated staff, any Information Technology Asset.

### 6.2 Information and Records

- 6.2.1 All information and records created or legally acquired using the City's Information Technology Assets are the sole property of the City of Toronto with the exception of records which arise from the permitted

personal use of Information Technology Assets in accordance with Section 7.

## **7. Personal Use**

- 7.1 Reasonable and limited personal use of Information Technology Assets is permitted, provided that it:
  - 7.1.1 Does not interfere with the Authorized User's duties and responsibilities.
  - 7.1.2 Is lawful and in compliance with applicable City of Toronto by-laws and policies, and relevant federal or provincial legislation.
  - 7.1.3 Does not compromise the security of the City's Information Technology Assets.
  - 7.1.4 Is not used for private gain, whether monetary or non-monetary, or advancement or the expectation of private gain.
  - 7.1.5 Does not result in the City incurring an expense unless it is incurred in accordance with the Business Expense Policy.
- 7.2 Authorized Users are responsible for properly managing personal files. The City is not liable nor will it incur any expense to protect or back-up personal files.
- 7.3 Authorized Users are encouraged to not store their own personal information or personal files on the City's Information Technology Assets. Users that elect to store their own personal information or personal files acknowledge that they are doing so at their own risk.

## **8. Unacceptable Use of Information Technology Assets**

- 8.1 Unacceptable use of the City's Information Technology Assets includes, but is not limited to:
  - 8.1.1 Using the City's Information Technology Assets to access or carry out any activities that are obscene, lewd, or pornographic.
  - 8.1.2 Using the City's Information Technology Assets to carry out any activities that are harassing, embarrassing, discriminatory or defamatory to another individual, employee, or group, or that are in breach of the employee's duty of fidelity to the City of Toronto.

6

- 8.1.3 Using Information Technology Assets to carry out any activities that contravene federal, provincial legislation and City of Toronto by-laws and policies.
- 8.1.4 Activities that will interfere with the normal operations of the City's Information Technology Assets, including intercepting or altering information transmitted.
- 8.1.5 Violating terms of applicable software licensing agreements or intellectual property laws, including installing software without a license.
- 8.1.6 Disclosing or distributing confidential information without authorization or contrary to City policies and by-laws and relevant federal or provincial legislation.
- 8.1.7 Circumventing the City's security schemes and protection.
- 8.1.8 Unauthorized use, infringement, theft, reconfiguration, movement, or relocation of City's Information Technology Assets and/or data, information or records located on the City's Information Technology Assets.

## **9. Monitoring**

### **9.1 Systems Monitoring**

- 9.1.1 The City of Toronto has the right to conduct Systems Monitoring at any time, at will and in its sole discretion, including the right to filter and quarantine both inbound and outbound content, as may be necessary to protect the integrity, security, confidentiality, or reliability of the City's Information Technology Assets.
- 9.1.2 As part of System Monitoring, the City of Toronto may recover deleted files and data stored or accessed using the City's Information Technology Assets.

### **9.2 User Monitoring**

- 9.2.1 The City of Toronto reserves the right, but does not have a duty, to conduct User Monitoring.
- 9.2.2 The City may exercise its right to perform User Monitoring:

9.2.2.1 If in the opinion of the City Solicitor there are reasonable grounds and/or a reasonable belief based on credible information received to support User Monitoring, including but not limited to information or belief that:

- i. An Authorized User is violating this Policy or other City of Toronto by-laws and policies, or any relevant federal and provincial legislation in their use of the City's Information Technology Assets.
- ii. An Authorized User is using the City's Information Technology Assets in a fashion incompatible with the User's employment with the City or grant of access to the City's Information Technology Assets.
- iii. The results from general Systems Monitoring provide reasonable grounds to focus on and review a specific Authorized User's activity.

9.2.2.2 In the alternative, if necessary to:

- i. protect and maintain the City's Information Technology Assets or other assets and interests from an immediate or imminent threat.
- ii. support the City of Toronto's efforts to comply with legal requirements, or defend itself in proceedings.

9.2.2.3 For other legitimate business, corporate or human resources purposes, including as a result of the absence of an employee.

9.2.3 User Monitoring pursuant to Section 9.2.2, User Monitoring, will be conducted in accordance with the User Monitoring Procedures referenced in Section 11.1.11, and the following principles:

9.2.3.1 If effective alternatives to User Monitoring are available in identifying inappropriate use or responding to a legitimate business, corporate, or human resources purpose, they shall be employed.

9.2.3.2 The least intrusive but effective means of User Monitoring shall be used.

- 9.2.3. Results of User Monitoring shall remain confidential, subject to the requirements of the investigation (including matters arising from the investigation), and/or other City by-laws, policies and relevant provincial and federal legislation.
- 9.2.3.4 Any decision to prosecute or refer User Monitoring or investigation results to the Toronto Police Service or other regulatory agencies for independent investigation will be made in accordance with the Toronto Public Service By-law, Chapter 192, Public Service of the Toronto Municipal Code.
- 9.2.4 User Monitoring by any individual for private or personal interest, curiosity, or without cause and appropriate authorization is prohibited and shall be considered a violation of this Policy.
- 9.3 Section 9.2 of this Policy does not apply to Accountability Officers when user monitoring is necessary as part of the fulfillment of their statutory mandate and responsibilities under Part V of the *City of Toronto Act, 2006*.
  - 9.3.1 In circumstances, where an Accountability Officer is conducting user monitoring for their own Office or their staff, the Accountability Officer is responsible for applying Section 9.2 as deemed appropriate by the Accountability Officer.

## 10. Compliance

- 10.1 Failure to comply with this Policy may result in disciplinary action up to and including dismissal and/or legal proceedings where warranted.
- 10.2 In an event of a conflict or difference the federal and provincial legislation supersedes this Policy.
- 10.3 This Policy supersedes other City or divisional policies, standards and guidelines that govern the use of Information Technology Assets in an event of conflict or difference, subject to the principle that specific provisions of the other policies, standards, and guidelines continue to apply despite a more general provision being set out in this Policy.
- 10.4 This Policy shall be reviewed every three to five years and the City reserves the right to amend this Policy at any time.

## 11. Related By-laws, Policies and Procedures

- 11.1 This Policy is to be implemented and interpreted with other related by-laws and policies, including:
  - 11.1.1 Toronto Municipal Code, Chapter 192, Public Service  
<http://www.toronto.ca/legdocs/municode/toronto-code-192.pdf>
  - 11.1.2 Application of City Policies to Social Media Use:  
[http://insideto.toronto.ca/social\\_media/pdf/socialmediause.pdf](http://insideto.toronto.ca/social_media/pdf/socialmediause.pdf)
  - 11.1.3 City of Toronto Human Rights and Anti-Harassment/Discrimination Policy:  
[Human Rights and Anti-Harassment/Discrimination Policy](#)
  - 11.1.4 Corporate Information Security Policy:  
[http://insideto.toronto.ca/itweb/policiesstandards/information\\_security.htm](http://insideto.toronto.ca/itweb/policiesstandards/information_security.htm)
  - 11.1.5 IT Asset Management Policy:  
<http://insideto.toronto.ca/itweb/policiesstandards/pdf/asset-management.pdf>
  - 11.1.6 Toronto Municipal Code, Chapter 3, Accountability Officers  
[http://www.toronto.ca/legdocs/municode/1184\\_003.pdf](http://www.toronto.ca/legdocs/municode/1184_003.pdf)
  - 11.1.7 Toronto Municipal Code, Chapter 217, Records, Corporate (City)  
[Toronto Municipal Code, Chapter 217](#)
  - 11.1.8 Business Expense Policy  
[http://insideto.toronto.ca/accounting\\_services/pdf/business\\_expense\\_policy.pdf](http://insideto.toronto.ca/accounting_services/pdf/business_expense_policy.pdf)
  - 11.1.9 Information Management Accountability Policy  
<https://www.toronto.ca/wp-content/uploads/2018/07/8ec6-information-management-accountability-policy.pdf>
  - 11.1.10 Protection of Privacy Policy  
<https://www.toronto.ca/wp-content/uploads/2017/08/9023-ProtectionOfPrivacyFinalAODA.pdf>
  - 11.1.11 User Monitoring Procedures  
<http://insideto.toronto.ca/itweb/policy/pdf/user-monitoring-procedures.pdf>

Approved By:  
Peter Wallace  
City Manager  
February 26, 2018