

**ONTARIO
SUPERIOR COURT OF JUSTICE**

B E T W E E N :

VANESSA FAREAU and RANSOME CAPAY

Plaintiffs

- and -

BELL CANADA and HER MAJESTY THE QUEEN IN RIGHT OF ONTARIO

Defendants

Proceeding under the *Class Proceedings Act, 1992*

SUPPLEMENTARY AFFIDAVIT OF NADINE BLUM

I, Nadine Blum, of the City of Toronto, Province of Ontario, **DO SOLEMNLY AFFIRM:**

1. I am a lawyer at Goldblatt Partners LLP, one of the two class counsel firms in this action. I have direct knowledge of the matters to which I depose in this affidavit. Where the information in this affidavit is not based on my direct knowledge, but is based upon information and belief from other sources, I have stated the source of that information and I believe the information to be true. Nothing in this affidavit is intended to waive solicitor-client or other privilege.
2. I previously affirmed an affidavit in this matter on December 21, 2020, which was included in the moving record.
3. On May 3, 2021, Goldblatt Partners LLP received a letter from the Ministry of the Solicitor General, Freedom of Information and Protection of Privacy Services, dated April 30, 2021 (the "FOI Letter"). The FOI Letter enclosed records relating to the exclusive contract

between Synergy Inmate Phone and the province of Ontario for the operation of the inmate systems in Ontario correction facilities (the “Synergy Contract”).

4. Attached as **Exhibit “A”** is a copy of the FOI Letter and Synergy contract received from the Ministry of the Solicitor General, Freedom of Information and Protection of Privacy Services regarding request number: SOLGEN-A-00514.

5. The Synergy Contract included a table of rates for various types of phones calls from the Offender Telephone Management System. The table of rates is located at p. 55 of the contract and FOI document.

6. I swear this affidavit in support of a motion for certification of this action as a class proceeding and for no other or improper purpose.

AFFIRMED BEFORE ME before me remotely by Nadine Blum stated as being located in the City of Toronto, in the Province of Ontario, on May 13, 2021, in accordance with O. Reg. 431/20 Administering Oath or Declaration Remotely.



A Commissioner for taking Affidavits (or as may be)



NADINE BLUM

Geetha Philipupillai LS#: 74741S

This is **Exhibit "A"** referred to in the
Affidavit of Nadine Blum
affirmed before me this 13th day of May, 2021
in accordance with O. Reg 431/20,
Administering Oath or Declaration Remotely

A handwritten signature in black ink, appearing to be the initials 'JB' or similar, written in a cursive style.

A COMMISSIONER, ETC.

Ministry of the Solicitor General ministère du Solliciteur général

Freedom of Information and
Protection of Privacy Services
200 First Avenue West
North Bay ON P1B 3B9

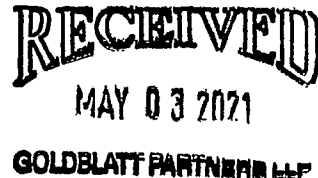
Services d'accès à l'information et de la
Protection de la vie privée
200 First Avenue West
North Bay ON P1B 3B9



Telephone (705) 494-3080
Toll Free 1-855-273-3080
Facsimile (705) 494-3081
www.ontario.ca/mes4

Téléphone (705) 494-3080
Sans Frais 1-855-273-3080
Télécopieur (705) 494-3081
www.ontario.ca/s199

April 30, 2021



Geetha Philipupillai
Goldblatt Partners
20 Dundas St W, Suite 1039
Toronto, Ontario M5G 2C2

Dear Geetha Philipupillai:

SUBJECT: REQUEST NUMBER SOLGEN-A-2021-00514

In response to your request for access to information under the Freedom of Information and Protection of Privacy Act, please be advised that total access is granted to copies of records relating to the exclusive contract between Synergy Inmate Phone and the province of Ontario for the operation of inmate systems in Ontario correctional facilities.

Attached is a copy of the records being released. This access decision was made by the undersigned. You are entitled to appeal this decision within 30 days to:

Information and Privacy Commissioner/Ontario (IPC)
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8
(416) 326-3333

Should you decide to file an appeal, please provide the IPC with the following information:

- 1) a copy of this decision letter;
- 2) a copy of your request for access to information;
- 3) the mandatory appeal fee of \$25.00 in the form of a cheque or money order payable to the Minister of Finance.

.../2

Geetha Philipupillai
Page two

Should you have any questions regarding the foregoing, please do not hesitate to contact Tracy Buttigieg, Senior Program Analyst & Advisor, at 705-492-6245.

Sincerely,

A handwritten signature in cursive script, appearing to read "Enza Ragone".

Enza Ragone
Coordinator
Freedom of Information and
Protection of Privacy Services

Attachment



Agreement

Between

**HER MAJESTY THE QUEEN
in right of Ontario as represented by
the Solicitor General**

and

Synergy Inmate Phone Solutions, Inc.

Offender Telephone Management System

Effective Date: March 2, 2020

Agreement No.: COS-0124

Agreement

THIS AGREEMENT ("Agreement"), made in triplicate, for an Offender Telephone Management System is effective as of March 2, 2020 ("Effective Date"),

BETWEEN:

HER MAJESTY THE QUEEN
in right of Ontario as represented by
the Solicitor General

(referred to as "the Ministry")

AND:

Synergy Inmate Phone Solutions, Inc.

(referred to as the "Vendor")

In consideration of their respective agreements set out below, the parties covenant and agree as follows:

ARTICLE 1 – INTERPRETATION AND GENERAL PROVISIONS

1.01 Defined Terms

The following words or expressions have the following meanings when used in this Agreement:

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

"Bid" means all documentation submitted by a Bidder in response to the RFB or in respect of the RFB;

"Bidder" means the legal entity that submits a Bid in response to this RFB;

"Canadian Radio-television and Telecommunications Commission" or the **"CRTC"** means the independent public authority in charge of regulating and supervising Canadian broadcasting and telecommunications;

"Category 3" or **"CAT 3"** means unshielded twisted pair cable used in telephone wiring as defined jointly by the Electronic Industries Alliance (EIA) and the Telecommunications Industry Association (TIA) and published in TIA/EIA-568-B;

"Category 5" or **"CAT 5"** means shielded twisted pair cable used in computer network wiring as defined jointly by the American National Standards Institution (ANSI) and the Telecommunications Industry Association (TIA) published in ANSI/TIA-568-A;

“Category 6” or **“CAT 6”** means shielded twisted pair cable used in computer network wiring as defined jointly by the Electronic Industries Alliance (EIA) and the Telecommunications Industry Association (TIA) and published in TIA/EIA-568;

“Commencement Date” has the meaning ascribed thereto in Section 3.07;

“Conflict of Interest” includes, but is not limited to, any situation or circumstance where:

- (a) in relation to the RFB process, the Bidder has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to (i) having or having access to information in the preparation of its Bid that is confidential to the Crown and not available to other Bidders; (ii) communicating with any person with a view to influencing preferred treatment in the RFB process, including the giving of a benefit of any kind, by or on behalf of the Bidder to anyone employed by or otherwise connected with, the Ministry; or (iii) engaging in conduct that compromises or could be seen to compromise the integrity of the open and competitive RFB process and render that process non-competitive and unfair; or
- (b) in relation to the performance of its contractual obligations in a Crown contract, the Vendor’s other commitments, relationships or financial interests (i) could or could be seen to exercise an improper influence over the objective, unbiased and impartial exercise of its independent judgement; or (ii) could or could be seen to compromise, impair or be incompatible with the effective performance of its contractual obligations;

“Contract” means the aggregate of: (a) the Agreement, including Schedule 1 (Description of Deliverables, Calling Rates and Supplementary Terms), and any other schedule attached at the time of execution; (b) the RFB, including any addenda and attachments; (c) the Bid; and (d) any amendments executed in accordance with the terms of the Agreement;

“Conversation Opinion Test as documented in Annex A of Recommendation P.800” means the methods and procedures for conducting subjective evaluations of transmission quality published by ITU-T;

“Corporate Policy on Information Sensitivity Classification” means the Government of Ontario’s information technology standard that addresses the confidentiality, integrity and availability requirements of information and information systems, found in Attachment #1;

“Credit Check” is a security screening check based on results provided by a Canadian credit bureau to determine if an individual has any adverse credit information. As part of this check, information collected may include credit score and any relevant bankruptcies, legal proceedings, collection actions and court orders. Information obtained as part of the search will only be used for the purpose of assessing an individual’s clearance status;

“Criminal Record and Judicial Matters Check (CRJMC)” is a search through the Canadian Police Information Centre (CPIC) maintained by the Royal Canadian Mounted Police (RCMP) and a search through provincial and municipal police databases, using an individual’s name and date of birth, for information relating to the offence provisions of federal legislation including the *Criminal Code (Canada)*, the *Controlled Drugs and Substances Act (Canada)* and the *Youth Criminal Justice Act (Canada)*. The search will include records of previous convictions, convictions for which a pardon has been granted (where disclosure is authorized under the *Criminal Records Act (Canada)*), findings of guilt under the *Youth Criminal Justice Act (Canada)*, findings of guilt that have resulted in absolute or conditional discharges (disclosed within one (1) and three (3) years respectively, any outstanding charges and related information (e.g., an arrest warrant), as well as court orders (excludes mental health related orders and family court restraining orders). The RCMP may require verification of identity through fingerprint comparison before the information can be released;

“Driver’s Record Check” is conducted where driving is a requirement for the contract where a valid driver’s licence is required. It involves a check of provincial databases for information regarding driving history using the individual’s driver licence number. This check provides a three, five or ten year history of *Highway Traffic Act and Criminal Code of Canada* convictions and any current suspensions, along with the driver’s current listed address and licence status;

“Deliverables” means everything developed for or provided to the Ministry in the course of performing under the Contract or agreed to be provided to the Ministry under the Contract by the Vendor or the Vendor’s Personnel, as further defined, but not limited by Schedule 1, including, but not limited to, any goods or services or any and all Intellectual Property and any and all concepts, techniques, ideas, information, documentation and other materials, however recorded, developed or provided;

“Employer” means a person who employs one or more workers or contracts for the services of one or more workers and includes a contractor or Subcontractor who performs work or supplies services and a contractor or Subcontractor who undertakes with an owner, contractor or Subcontractor to perform work or supply services;

“Expiry Date” means the day preceding the fifth anniversary of the Commencement Date, or, if the Ministry elects to extend the term of this Agreement, the last day of the final extension period;

“Facility” or “Facilities” means one or more of Ontario’s 25 correctional institutions located across the province;

“Fee” means the monthly payment the Vendor shall pay towards the Ministry’s administrative and operational costs;

“FIPPA” means the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, as amended;

“GO ITS” means an official publication concerning the standards, guidelines, technical reports and preferred practices adopted by the Government of Ontario;

“Graphical User Interface” or **“GUI”** means the software that the Ministry uses to graphically monitor and control its PLC for correctional operations;

“Hearing Aid Compatible” or **“HAC”** means the ability to work, are compatible, and do not cause interference with hearing aids and cochlear implants in terms of acoustic coupling or inductive coupling;

“I & IT” means information and information technology;

“Indemnified Parties” means each of the following and their directors, officers, advisors, agents, appointees and employees: Her Majesty the Queen in right of Ontario and the members of the Executive Council of Ontario;

“Industry Standards” include, but are not limited to (a) the provision of any and all labour, supplies, equipment and other goods or services that are necessary and can reasonably be understood or inferred to be included within the scope of the Contract or customarily furnished by Persons providing Deliverables of the type provided hereunder in similar situations in Ontario and; (b) adherence to commonly accepted norms of ethical business practices, which shall include the Vendor establishing, and ensuring adherence to, precautions to prevent its employees or agents from providing or offering gifts or hospitality of greater than nominal value to any person acting on behalf of or employed by Her Majesty the Queen in right of Ontario;

“Intellectual Property” means any intellectual, industrial or other proprietary right of any type in any form protected or protectable under the laws of Canada, any foreign country, or any political subdivision of any country, including, without limitation, any intellectual, industrial or proprietary rights protected or protectable by legislation, by common law or at equity;

“ITU-T” means the telecommunication standardization sector of the International Telecommunication Union that coordinates standards for telecommunications headquartered in Geneva, Switzerland;

“Ministry Address” and **“Ministry Representative”** mean:

Ministry of the Solicitor General
External Oversight and Compliance Branch
25 Grosvenor St., George Drew Building, 16th Floor
Toronto, Ontario, M7A 1Y6

Ministry Representative: Khalid Mohiq, Resources Planning Coordinator
Telephone: (416) 327-7213
Facsimile: (416) 327-2435
E-mail: Khalid.Mohiq@ontario.ca

Back-up Ministry Representative: Rita Regala, Manager
Telephone: (416) 846-6955

Facsimile: (416) 327-2435
E-mail: Rita.Regala@ontario.ca

“Network Management System” and **“NMS”** means the software and network provided by the Vendor for the Ministry to use for the configuration, monitoring and reporting of inmate telephone services;

“OPS Confidential Information” means all information of the Ontario Public Service that is of a confidential nature, including all confidential information in the custody or control of the OPS, regardless of whether it is identified as confidential or not, and whether recorded or not, and however fixed, stored, expressed or embodied, which comes into the knowledge, possession or control of the Vendor in connection with the Agreement. For greater certainty, OPS Confidential Information shall:

- (a) include: (i) all new information derived at any time from any such information whether created by the OPS, the Vendor or any third-party; (ii) all information (including Personal Information) that the OPS is obliged, or has the discretion, not to disclose under provincial or federal legislation or otherwise at law; but
- (b) not include information that: (i) is or becomes generally available to the public without fault or breach on the part of the Vendor of any duty of confidentiality owed by the Vendor to the OPS or to any third-party; (ii) the Vendor can demonstrate to have been rightfully obtained by the Vendor, without any obligation of confidence, from a third-party who had the right to transfer or disclose it to the Vendor free of any obligation of confidence; (iii) the Vendor can demonstrate to have been rightfully known to or in the possession of the Vendor at the time of disclosure, free of any obligation of confidence when disclosed; or (iv) is independently developed by the Vendor; but the exclusions in this subparagraph shall in no way limit the meaning of Personal Information or the obligations attaching thereto under the Contract or at law;

“Ontario Public Service” and **“OPS”** means the ministries and other administrative units of Her Majesty the Queen in right of Ontario (“Ontario”) over which ministers of Ontario preside, and includes agencies, boards and commissions;

“Other Security Screening Check” means a higher level check that may be required when the duties or tasks establish a risk level greater than can be addressed through a CRJMC, Driver’s Record or Out of Country check. Other security screening checks which may be conducted in addition to the CRJMC are those included in the *Police Record Checks Reform Act*, out of scope of the Act or permitted by regulatory exemption to the Act. Checks are determined on the basis of a Ministry risk assessment;

“Offender Tracking Information System” or **“OTIS”** means the Ministry’s I & IT system that keeps track of inmates;

“Out-of-Country Driver’s Record Check (US and/or International)” means the driver’s record check that is conducted where driving is a requirement for the

contract where a valid driver's licence is required. When the individual has lived outside Canada for more than six (6) months consecutively within the last five (5) years, an out of country driver records check from the jurisdiction(s) in which they have resided is required. This check includes information such as current suspensions, along with the driver's current listed address and licence status;

“Out-of-Country Police Certificate (US and/or International)” is a summary of an individual's criminal record or a declaration of the absence of any criminal record from a law enforcement agency in another country outside of Canada. Police certificates are different in each state/country and may be called police clearance certificates, good conduct certificates, judicial record extracts, etc. Where an individual has lived outside of Canada for more than six (6) months consecutively within the last five (5) years, an out-of-country police certificate from the jurisdiction(s) in which they have resided is required;

“Person” if the context allows, includes any individuals, firms, partnerships or corporations or any combination thereof;

“Personal Identification Number” or **“PIN”** means a numeric sequence created by each individual inmate to be used in conjunction with a specific account number for the purpose of 2FA;

“Personal Information” means recorded information about an identifiable individual or that may identify an individual;

“Proceeding” means any action, claim, demand, lawsuit or other proceeding;

“Programmable Logic Controller” or **“PLC”** means the Ministry's industrial digital computer adapted for the control of correctional operations;

“Record”, for the purposes of the Contract, means any recorded information in the custody or control of the Ministry, including any Personal Information, in any form: (a) provided by the Ministry to the Vendor, or provided by the Vendor to the Ministry, for the purposes of the Contract; or (b) created by the Vendor in the performance of the Contract;

“Requirements of Law” mean all applicable requirements, laws, statutes, codes, acts, ordinances, approvals, orders, decrees, injunctions, by-laws, rules, regulations, official plans, permits, licences, authorisations, directions and agreements with all Authorities that now or at any time hereafter may be applicable to either the Contract or the Deliverables or any part of them;

“RFB” means the Request for Bids, which includes the Qualification, Technical, and Commercial Envelopes as set out on the Ontario Tenders Portal eTendering System, as well as any addenda and attachments to it; dated July 4, 2019 for Offender Telephone Management System, reference number COS-0124 issued by the Ministry for the Deliverables;

“Subcontractors” means in the case of each party, any contractor of that party or any of its subcontractors at any tier of subcontracting;

“Telecommunications Act” means the Canadian *Telecommunications Act*, S.C. 1993, c. 38, as amended and its regulations;

“Telephone System” means the hardware and actual telephone calls as controlled by the Network Management System;

“Term” means the period of time from the Effective Date up to and including the earlier of (i) the Expiry Date; or (ii) the date of termination of the Contract in accordance with its terms;

“Third-Party Intellectual Property” means any Intellectual Property owned by a party other than Her Majesty the Queen in right of Ontario or the Vendor;

“TTY” is an acronym for Teletype, which is a device that converts voice into typed script for the deaf and hard of hearing;

“Two Factor Authentication” or **“2FA”** means a two factor process utilizing two different pieces of information to verify the identity of an individual;

“Uninterruptable Power Source” or **“UPS”** means an electrical apparatus that provides emergency power to a load when the input power source or main power fails to provide instantaneous protection from input power interruptions;

“Vendor Address” and **“Vendor Representative,”** mean:

Synergy Inmate Phone Solutions, Inc.
6114 – 53 Avenue
Beaumont, Alberta, T4X 1V6

Vendor Representative: Mike Kinnee, President, Canadian Operations
Telephone: (780) 721-7685
Facsimile: (587) 764-0670
E-mail: mike@synergyinmatephones.com

“Vendor’s Personnel” includes the directors, officers, employees, agents, partners, affiliates, volunteers or Subcontractors of the Vendor;

“Voice over Internet Protocol” or **“VoIP”** means technology to provide telephone service where voice is transmitted as IP packets over a packet-switched network;

“Vulnerable Sector Check (VSC)” means all information disclosed in a Criminal Records and Judicial Matters Check. Every criminal offence with which the individual has been charged that resulted in a finding of not criminally responsible on account of mental disorder (disclosure prohibited if the request is made more than five years after the date of the finding or if the individual received an absolute discharge) and includes any non-conviction information authorized for exceptional disclosure in accordance with section 10 of the *Police Records Check Reform Act, 2015*, S.O., 2015, as amended.

1.02 No Indemnities from Ministry

Notwithstanding anything else in the Contract, any express or implied reference in any document (including subcontracts) related to the Deliverables under the Contract, to the Ministry providing an indemnity or any other form of indebtedness or contingent liability that would directly or indirectly increase the indebtedness or contingent liabilities of Ontario, whether at the time of execution of the Agreement or at any time during the Term, shall be void and of no legal effect.

1.03 Entire Agreement

The Contract embodies the entire agreement between the parties with regard to the provision of Deliverables and supersedes any prior understanding or agreement, collateral, oral or otherwise with respect to the provision of the Deliverables, existing between the parties at the date of execution of the Agreement.

1.04 Severability

If any term or condition of the Contract, or the application thereof to the parties or to any Persons or circumstances, is to any extent invalid or unenforceable, the remainder of the Contract, and the application of such term or condition to the parties, Persons or circumstances other than those to which it is held invalid or unenforceable, shall not be affected thereby.

1.05 Interpretive Value of Contract Documents

In the event of a conflict or inconsistency in any provisions in the Contract: (a) the main body of the Agreement shall govern over the Schedules to the Agreement; (b) the Agreement (including its Schedules) shall govern over the RFB and the Bid; and (c) the RFB shall govern over the Bid.

1.06 Interpretive Value of Headings

The headings in the Contract are for convenience of reference only and in no manner modify, interpret or construe the Contract.

1.07 Force Majeure

Neither party shall be liable for damages caused by delay or failure to perform its obligations under the Contract where such delay or failure is caused by an event beyond its reasonable control. The parties agree that an event shall not be considered beyond one's reasonable control if a reasonable business person applying due diligence in the same or similar circumstances under the same or similar obligations as those contained in the Contract would have put in place contingency plans to either materially mitigate or negate the effects of such event. Without limiting the generality of the foregoing, the parties agree that force majeure events shall include natural disasters and acts of war, insurrection and terrorism but shall not include shortages or delays relating to supplies or services, or any strike, work refusal or other labour dispute or disruption (subject to the terms in Section 2.08 with respect to labour disputes). If a party seeks to excuse itself from its obligations under the Contract due to a force majeure event, that party shall immediately notify the other party of the delay or non-performance, the reason for such delay or non-performance and the anticipated period of delay or non-performance. If the anticipated or actual delay or non-performance exceeds twenty (20) Business Days, the other party may

immediately terminate the Contract by giving notice of termination and such termination shall be in addition to the other rights and remedies of the terminating party under the Contract, at law or in equity.

1.08 Business Continuity Plan

The Vendor shall implement a business continuity plan to address continuity of service in the event of any circumstances that could lead to a business disruption including, but not limited to, a pandemic, utility failure or Vendor or Ministry labour disruption. Upon the Ministry's request, the Vendor shall submit such business continuity plan to the Ministry within five (5) Business Days for review and approval. Despite any such review or approval by the Ministry, the Vendor shall be solely responsible for ensuring the effectiveness of its business continuity plan.

1.09 Notices by Prescribed Means

Notices, shall be in writing and shall be delivered by postage-prepaid envelope, personal delivery, e-mail or facsimile and shall be addressed to, respectively, the Ministry Address to the attention of the Ministry Representative and to the Vendor Address to the attention of the Vendor Representative. Notices shall be deemed to have been given (a) in the case of postage-prepaid envelope, five (5) Business Days after such notice is mailed; or (b) in the case of personal delivery, e-mail or facsimile one (1) Business Day after such notice is received by the other party. In the event of a postal disruption, notices must be given by personal delivery, e-mail or by facsimile. Unless the parties expressly agree in writing to additional methods of notice, notices may only be provided by the methods contemplated in this section.

1.10 Governing Law

The Contract shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein.

1.11 Time of the Essence

Time is of the essence of every provision of the Contract. Any waiver or extension of any timeline by the Ministry in any instance shall apply only as may be specified in writing by the Ministry to the Vendor, and there shall be no implied waiver of this provision.

1.12 Currency

All references to currency in the Agreement shall be to Canadian dollars.

ARTICLE 2 – NATURE OF RELATIONSHIP BETWEEN MINISTRY AND VENDOR

2.01 Vendor's Power to Contract

The Vendor represents and warrants that it has the full right and power to enter into the Contract and there is no agreement with any other Person that would in any way interfere with the rights of the Ministry under the Contract.

2.02 Representatives May Bind the Parties

The parties represent that their respective representatives have the authority to legally bind them to the extent permissible by the Requirements of Law.

2.03 Vendor Not a Partner, Agent or Employee

The Vendor shall have no power or authority to bind the Ministry or to assume or create any obligation or responsibility, express or implied, on behalf of the Ministry. The Vendor shall not hold itself out as an agent, partner or employee of the Ministry. Nothing in the Contract shall have the effect of creating an employment, partnership or agency relationship between the Ministry and the Vendor (or any of the Vendor's Personnel) or constitute an appointment under the *Public Service of Ontario Act, 2006*, S.O. 2006, c.35, Schedule A, as amended.

2.04 Responsibility of Vendor

The Vendor agrees that it is liable for its acts and omissions and those of the Vendor's Personnel. This section is in addition to any and all of the Vendor's liabilities under the Contract and under the general application of law. The Vendor shall advise these individuals and entities of their obligations under the Contract and shall ensure their compliance with the applicable terms of the Contract. This section shall survive the termination or expiry of the Contract.

2.05 No Subcontracting or Assignment

The Vendor shall not subcontract or assign the whole or any part of the Contract without the prior written consent of the Ministry. Such consent shall be in the sole discretion of the Ministry and subject to the terms and conditions that may be imposed by the Ministry. Without limiting the generality of the conditions which the Ministry may require prior to consenting to the Vendor's use of a Subcontractor, every contract entered into by the Vendor with a Subcontractor shall adopt all of the terms and conditions of the Contract as far as applicable to those parts of the Deliverables provided by the Subcontractor. Without limiting the foregoing, the Vendor shall ensure that any Subcontractor it retains to provide any Telecommunication Services under the Contract complies with all applicable requirements of the *Telecommunications Act*. Nothing contained in the Contract shall create a contractual relationship between any of the Vendor's Personnel and the Ministry.

2.06 Duty to Disclose Change of Control

In the event that the Vendor undergoes a change in control the Vendor shall immediately disclose such change in control to the Ministry and shall comply with any terms and conditions subsequently prescribed by the Ministry resulting from the disclosure.

2.07 Conflict of Interest

The Vendor shall (a) avoid any Conflict of Interest in the performance of its contractual obligations; (b) disclose to the Ministry without delay any actual or potential Conflict of Interest that arises during the performance of its contractual obligations; and (c) comply with any requirements prescribed by the Ministry to resolve any Conflict of Interest. In addition to all other contractual rights or rights available at law or in equity, the Ministry may immediately terminate the Contract upon giving notice to the Vendor where (a) the Vendor fails to disclose an actual or potential Conflict of Interest; (b) the Vendor fails to comply with any requirements prescribed by the Ministry to resolve a Conflict of Interest; or (c) the Vendor's Conflict of Interest cannot be resolved.

Without limiting the foregoing, the Vendor shall ensure it has policies in place to avoid any Conflict of Interest or potential security breach that may arise in respect of any of the Vendor's Personnel who form or continue a relationship or connection of a personal or business nature with an inmate or ex-inmate or with someone known to be in a close relationship with an inmate or ex-inmate, and shall comply with Section 30(2) of the *Ministry of Correctional Services Act*, and any associated Ministry direction.

This section shall survive the termination or expiry of the Contract.

2.08 **Labour Disputes**

(a) If a strike, work refusal or other labour dispute or disruption involving any Person for whom the Vendor is responsible is pending, occurs or is threatened, the Vendor shall:

- (i) immediately inform the Ministry and continue to keep the Ministry informed throughout the course of the dispute;
- (ii) continue to perform all Deliverables while ensuring that appropriate steps are implemented to resolve the dispute;

provided that the Vendor shall in no event be required by virtue of this Section 2.08 to breach any of its obligations at law or under any of its collective bargaining agreements.

(b) The Vendor shall not be liable for any damages caused by delay in performing any Deliverables where such delay is caused by a strike, work refusal or other labour dispute or disruption on the part of any Person for whom the Ministry is responsible that prevents the Vendor from having access to any Facility or Ministry office as required for the Vendor to perform the Deliverables in question. If such a strike, work refusal or other labour dispute or disruption is pending, occurs or is threatened, the Ministry reserves the right to reschedule any access by the Vendor or any Vendor's Personnel at the affected Facilities or Ministry offices without liability to the Vendor. For greater certainty, where the Vendor is prevented from having access to a Facility or Ministry office in such circumstances, the Vendor shall continue to provide Deliverables for all other Facilities or Ministry offices that are not affected, and shall work cooperatively with the Ministry to reschedule the work for the affected Facilities or Ministry offices or find other means of providing such Deliverables where possible. In no event shall the Ministry be required to breach any of its obligations at law or under any of its collective bargaining agreements to facilitate access by the Vendor to any Facilities or Ministry offices.

2.09 **Contract Binding**

The Contract shall enure to the benefit of and be binding upon the parties and their respective successors, executors, administrators and permitted assigns.

ARTICLE 3 - PERFORMANCE BY VENDOR

3.01 Performance

The Vendor hereby represents and warrants that:

- (i) it is, and will continue to be, registered with the CRTC and has and will maintain during the Term all required licences and comply with all applicable requirements of the *Telecommunications Act* and any other Requirements of Law as required to provide the Deliverables;
- (ii) the Deliverables shall be provided fully and diligently in a professional and competent manner by Persons qualified and skilled in their occupations and furthermore that all Deliverables will be provided in accordance with (a) the Contract; (b) the policies and documents approved by the Ministry under Section 3.02; (c) Industry Standards; and (d) Requirements of Law.

If any of the Deliverables, in the opinion of the Ministry, are inadequately provided or require corrections, the Vendor shall forthwith make the necessary corrections at its own expense as specified by the Ministry in a rectification notice issued pursuant to Section 10.02.

3.02 Preparation of Policies

Not later than thirty (30) Business Days after the Effective Date, the Vendor shall prepare and submit for the Ministry's approval, the following policies and documents:

- (1) the Vendor's proposed criminal proceedings policy, as further described in Section 11.04;
- (2) the Vendor's proposed training plan, materials and manuals; and
- (3) such information as the Ministry may require demonstrating that all calling charges are in accordance with the requirements of the Contract;

3.03 Approval of Proposed Policy

The Ministry shall notify the Vendor within twenty (20) Business Days of receiving a proposed policy or document from the Vendor pursuant to Section 3.02 whether or not the Ministry approves the proposed policy or document. If the Ministry does not approve a proposed policy or document, the Ministry shall notify the Vendor, which shall then be required to address the Ministry's concerns and submit a revised policy or document for Ministry approval within ten (10) Business Days of receipt of the Ministry's notice or such other timeframe specified by the Ministry in its notice.

3.04 No Variation of Policies; Annual Review

- (a) The Vendor shall not update or vary the contents of any of the Vendor's approved policies and documents without the Ministry's prior written consent, which consent may be arbitrarily withheld.

- (b) The Vendor shall comply with and shall conduct a review of its operations at least once each year to confirm compliance with the approved policies and documents.

3.05 Installation of Network Management System, Telephone System and Acceptance Testing

The Vendor shall install the Network Management System, the Telephone System, and any related equipment in accordance with its implementation plan and schedule as approved in writing by the Ministry. The initial installations must be approved by the Ministry in writing before the Vendor may commence subsequent installations as set out in Section 3.08.

The Vendor's implementation plan must provide for the Network Management System and related equipment being installed first at designated Ministry locations within sixty (60) Business Days of the Effective Date, with all equipment being installed at all Facilities by October 1, 2020.

3.06 Staff Training

The Vendor shall provide training to the Ministry in accordance with the Vendor's training plan as approved in writing by the Ministry, including both initial training before implementing the Network Management System and Telephone System, as well as ongoing training in accordance with the requirements of the Contract.

3.07 Commencement Date

Upon completion of acceptance testing to the Ministry's satisfaction at the designated Ministry locations, the Ministry will notify the Vendor in writing and set a date ("Commencement Date") as of which the Vendor shall be required to commence providing telephone services and as of which the Vendor shall be required to pay the Ministry a monthly Fee as described in Section 6.01.

3.08 Subsequent Installations

The Deliverables shall be installed at all of the remaining Facilities in accordance with the Vendor's implementation plan approved by the Ministry after Ministry written acceptance of the initial installations described in Section 3.05. The Vendor shall provide staff training in respect of those installed Deliverables at each Facility as set out in Schedule 1 and in accordance with the Vendor's training plan approved by the Ministry. The Vendor shall notify the Ministry of the completion of the installations at each Facility and the completion of associated training.

3.09 Disruption

The Vendor shall use its best efforts not to disrupt or to interfere with the Ministry's day-to-day operations and business in the course of the equipment installation and providing the Deliverables under the Contract.

3.10 Compliance with Occupational Health and Safety Requirements

The Vendor must ensure that it and any Subcontractor hired by the Vendor works in accordance with the *Occupational Health and Safety Act*, R.S.O. 1990, c. O.1 (OHSA) and its regulations and any applicable OPS and site-specific health and safety requirements. The Vendor acknowledges that it is the Employer of the

subcontractor. The Vendor shall include in any of its agreements with its Subcontractors, the ability to terminate the Subcontractor for non-compliance with OHSAA or its regulations, with the rules and policies of the Vendor or for failing to protect the safety of its workers.

3.11 Use and Access Restrictions; Cooperation

The Vendor acknowledges that unless it obtains specific written preauthorization from the Ministry, any access to or use of OPS property, technology or information that is not necessary for the performance of its contractual obligations with the Ministry is strictly prohibited. The Vendor further acknowledges that the Ministry may monitor the Vendor to ensure compliance with this section. This section is in addition to and shall not limit any other obligation or restriction placed upon the Vendor.

3.12 Notification by Vendor or Ministry

During the Term, the parties shall advise each other promptly of (a) any contradictions, discrepancies or errors found or noted in the Contract; (b) supplementary details, instructions or directions that do not correspond with those contained in the Contract; and (c) any omissions or other faults that become evident and should be corrected in order to provide the Deliverables in accordance with the Contract and Requirements of Law.

3.13 Condonation Not a Waiver

Any failure by the Ministry to insist in one or more instances upon strict performance by the Vendor of any of the terms or conditions of the Contract shall not be construed as a waiver by the Ministry of its right to require strict performance of any such terms or conditions, and the obligations of the Vendor with respect to such performance shall continue in full force and effect.

3.14 Changes By Written Amendment Only

Any changes to the Contract shall be by written amendment signed by the parties. No changes shall be effective or shall be carried out in the absence of such an amendment.

3.15 Vendor to Comply With Reasonable Change Requests

The Ministry may, in writing, request changes to the Contract, which may include altering, adding to, or deleting any of the Deliverables. The Vendor shall comply with all reasonable Ministry change requests and the performance of such request shall be in accordance with the terms and conditions of the Contract. If the Vendor is unable to comply with the change request, it shall promptly notify the Ministry and provide reasons for such non-compliance. In any event, any such change request shall not be effective until a written amendment reflecting the change has been executed by the parties.

For greater certainty, notwithstanding the foregoing, the Ministry reserves the right to add or delete Facilities for which the Vendor is required to provide Deliverables at any time during the Term of the Agreement upon written notice to the Vendor, and the Vendor shall be required to cooperate with respect to such additions or deletions and to install its equipment, or remove it, as the case may be, as expeditiously as possible and in accordance with a schedule approved in writing by the Ministry.

No changes may be made without the Ministry's prior written approval and the Ministry shall not be responsible for any costs associated with any changes made pursuant to this section. Any such approved changes shall not result in any increases to the Vendor's calling rates or a reduction in the percentage rate set by the Ministry used to calculate the Fee payable by the Vendor to the Ministry.

3.16 Non-Exclusive Contract, Work Volumes

The Vendor acknowledges that it is providing the Deliverables to the Ministry on a non-exclusive basis during the Term. The Ministry makes no representation regarding the volume of goods and services required under the Contract. The Ministry reserves the right to contract with other parties for the same or similar goods and services as those provided by the Vendor and reserves the right to obtain the same or similar goods and services internally. The number of telephones and offender capacity in Schedule 1 is an estimate only and does not represent a guarantee of the number of telephones to be installed in each Facility or the number of inmates who will be accessing them.

3.17 Ministry Rights and Remedies and Vendor Obligations Not Limited to Contract

The express rights and remedies of the Ministry and obligations of the Vendor set out in the Contract are in addition to and shall not limit any other rights and remedies available to the Ministry or any other obligations of the Vendor at law or in equity.

3.18 Accessibility

The Vendor shall ensure that the Deliverables comply with the requirements of the AODA with respect to features designed to make the telephones supplied under the Contract accessible by persons with disabilities. In addition, the Vendor's delivery of the Deliverables shall comply with all applicable requirements, specifications and standards for accessibility established in accordance with the Ontario *Human Rights Code*, R.S.O. c. H.19, the *Ontarians with Disabilities Act*, S.O. 2001, c. 32, and the *Accessibility of Ontarians with Disabilities Act, 2005*, S.O. 2005, c.11, any regulations made thereunder and any direction from the Ministry.

3.19 French Language Services

The Vendor's Network Management System shall at a minimum support automated voice messages and voice menu options in both English and French to be communicated to inmates and call recipients.

3.20 Records to be Maintained

The Vendor shall maintain accurate records of the Vendor's property and equipment provided to the Ministry under the Contract, and shall provide such records to the Ministry Representative upon request.

ARTICLE 4 – COLLABORATIVE BUSINESS RELATIONSHIP MANAGEMENT

4.01 Overview

The Ministry is committed to working with the Vendor towards a collaborative business relationship and a governance framework that supports the planning of

organizational roles, responsibilities and authorities. The following stages shall govern the collaborative business relationship between the Ministry and the Vendor:

1. Collaboration
2. Creation
3. Team Cohesiveness

4.02 **Collaboration**

The Ministry and the Vendor shall establish a formal joint work foundation setting out their respective roles and responsibilities and establishing a joint management team ("Team"). This joint work foundation shall be documented and maintained throughout the Term of the Agreement.

The Team shall meet on a quarterly basis, or more frequently as may be required. The schedule for the meetings shall be set once the Team is established.

The Team shall create a defined process identifying their joint objectives, as well as a joint relationship management plan ("Plan"). The Plan shall formalize the overall management of the collaborative business relationship and encompass the principles of cooperative behaviour.

The Plan shall create and identify a process that at a minimum deals with the following key areas:

- Risk management
- Quality process review
- Service delivery and performance management
- Issue resolution

The Plan shall be maintained by the Team throughout the relationship and periodically reviewed to ensure it reflects current and future developments.

4.03 **Creation**

The Team shall establish a creation process in order to bring forward ideas and innovations, and to support their implementation. At a minimum, the process shall:

- provide a mechanism for the capture of innovation and ideas for improvement;
- provide a method for performing analysis and evaluation of ideas and innovations;
- establish a method for reviewing the success or failure of creation initiatives.

4.04 **Team Cohesiveness**

The Ministry Representative and Vendor Representative shall oversee the Team, undertake regular reviews, provide overall support for successful service delivery, assist in overcoming any potential internal barriers, manage challenges within the collaboration as they arise, and promote overall collaborative behaviour and trust.

The Team shall ensure that measurable objectives are established that align with and demonstrate achievement towards the overall goals of the collaboration. A defined process shall be implemented and maintained to measure and evaluate the achievement of these goals, and to ensure that the objectives remain relevant throughout the Term of the Contract.

The Team shall implement a process for issue resolution. The process shall identify any necessary escalation procedures, and the level of authority within each party to address the escalation. Should the escalation process not function, the Ministry may issue a rectification notice in accordance with Section 10.02.

ARTICLE 5 – VENDOR’S CALLING RATES

5.01 Calling Rates – Inmate Telephones

The Vendor’s calling rates for local and long distance calls (collect and debit) made by inmates from an inmate telephone in a Facility shall consist of the calling rates as set forth in Schedule 1 as increased by the amount of any percentage rate set by the Ministry in accordance with Section 6.01, and may not be changed during the Term of the Agreement except as set forth below.

5.02 Conventional Public Pay Telephones

The Vendor shall set the calling rates for local and long distance calls made from any conventional public pay telephones in a Facility provided that such rates shall be no greater than the published residential rates established by the Incumbent Local Exchange Carrier (ILEC) for a comparable call placed from a conventional public pay telephone in the local community outside of the applicable Facility.

5.03 CRTC Tariffs

Despite any other provision in the Contract, the calling rates charged by the Vendor to inmates or call recipients shall not exceed the maximum amount authorized under any applicable tariff approved by the CRTC. In the event that a tariff applies, the Vendor shall provide the Ministry with prior written notice of any such tariff and documentation satisfactory to the Ministry substantiating the applicable CRTC tariff before implementing a calling rate at the Facilities pursuant to a tariff.

5.04 Changes to the Fee and Vendor’s Calling Rates

The Ministry may change the Fee annually upon written notice to the Vendor at least forty-five (45) Business Days before the anniversary of the Commencement Date when the change is to take effect. If the Ministry increases or reduces the Fee, the Vendor may adjust its calling rates accordingly, subject to the approval of the Ministry.

The Vendor may submit a request to change its calling rates to the Ministry, during the Term of the Agreement, should there be an applicable CRTC approved tariff. At the time of requesting any change, the Vendor shall provide the Ministry with any applicable CRTC approved tariffs and other documentation to demonstrate compliance with the requirements herein. Any proposed change to the Vendor’s calling rates shall be subject to the Ministry’s prior written

approval before being implemented at the Facilities.

ARTICLE 6 - PAYMENT

6.01 Payment

As of the Commencement Date, the Vendor shall track its gross revenues generated from all calls made from all telephones (both inmate telephone and conventional public pay telephones) supplied by the Vendor under the Contract in order to calculate the monthly Fee to be paid to the Ministry. The Fee shall be calculated based on a percentage of the above gross revenues. For greater certainty, in determining gross revenue, all forms of call payment including any connection fees shall be included and there shall be no adjustment for any associated expenses or taxes incurred by the Vendor in providing the Deliverables. Gross revenue shall not include taxes collected by the Vendor. The Ministry may change the percentage rate of the Fee on an annual basis, upon providing the Vendor with a minimum of 45 Business Days' written notice.

6.02 Payment Process

The following process shall apply to the Vendor's payment of the Fee:

- (a) The Vendor shall provide the Ministry with payment for the month's Fee for all Facilities no later than thirty (30) days following the last day of the month in which the applicable revenues were generated. Payment of such monthly Fee shall be accompanied by a report that shall include the reference number assigned to the Contract by the Ministry, the gross revenues and Fee in respect of each Facility, and the total Fee in respect of all Facilities.
- (b) In the event that there is a discrepancy between the amount of the Fee and the amount supported by Ministry generated reports, the Vendor shall provide further documentation to support the amount of the payment no later than thirty (30) days following the last day of the month to which it relates.
- (c) The Vendor may make the Fee payments under the Contract by way of cheque made payable to the Minister of Finance (Ontario) and sent to the Ministry Representative for processing.

6.03 Inmate Telephone Accounts

As further described in the Deliverables, the Vendor shall create inmate telephone accounts. The Ministry will advise the Vendor as to when to add monies to a specific account, in an encrypted format. Upon receipt of the notice, the Vendor shall credit the inmate telephone account for the specified amount for immediate use. On a weekly basis, the Vendor shall submit electronically the invoice and the following encrypted files that support the invoice:

- (a) invoice list report (preliminary invoice detailed by inmate and total amount per account);
- (b) invoice credit report (any credits owing to the inmates detailed by inmate);
and
- (c) final invoice list (invoice credit report offset against invoice list report)

The Vendor shall have a mechanism to immediately inform the Ministry in real time, in an encrypted format, the amount remaining in an inmate telephone account, at the time the Ministry notifies the Vendor of its closing or reconciliation of that specific inmate telephone account. Any amount remaining in an inmate telephone account upon closing shall also be set out, by inmate account number, in the weekly invoice credit report. The credit amount shall be offset against any monies owing to the Vendor. Once the invoice is received, the Ministry shall pay the Vendor within thirty (30) Business Days.

6.04 Interest Bearing Account

The Ministry may provide payment before the Vendor's immediate need for the advanced funds to be allotted for the inmate telephone accounts. The Vendor, therefore agrees that it must place the funds in an interest bearing account in the name of the Vendor at a Canadian financial institution.

6.05 Interest

If the Vendor earns any interest on the advanced funds, the Ministry may demand from the Vendor the payment of an amount equal to the interest.

6.06 No Charges

Save for the Ministry providing the Vendor with payments from the inmates' trust accounts to be put towards their telephone accounts, there shall be no charges payable by the Ministry under the Contract to the Vendor.

6.07 Vendor Responsible for Operating Costs

The Vendor shall be responsible for all operating costs of providing the Deliverables except any costs incurred by the Ministry in the performance of the Ministry's obligations.

6.08 Payment and Collection of Taxes and Duties

The Vendor shall pay or charge and remit, as required, all applicable taxes, including excise taxes incurred by or on the Vendor's behalf with respect to the Contract.

6.09 Interest on Late Payment

The Vendor shall pay interest on any late payment of the Fee providing that such late payment was through no fault of the Ministry. The interest rate for such late payment shall be the rate of interest fixed by order by the Lieutenant Governor in Council from time to time pursuant to Section 10(4) of the *Financial Administration Act*.

6.10 Document Retention and Audit

For seven (7) years after the Expiry Date or any date of termination of the Contract, the Vendor shall maintain all necessary records to substantiate (a) all charges and payments under the Contract and (b) that the Deliverables were provided in accordance with the Contract and with Requirements of Law. During the Term, and for seven (7) years after the Term, the Vendor shall permit and assist the Ministry in conducting audits of the operations of the Vendor to verify (a) and (b) above. The Ministry shall provide the Vendor with at least ten (10) Business Days prior notice of its requirement for such audit. The Vendor's

obligations under this section shall survive any termination or expiry of the Contract.

ARTICLE 7 – CONFIDENTIALITY, RECORDS AND FIPPA

7.01 Confidentiality and Promotion Restrictions

Any publicity or publications related to the Contract shall be at the sole discretion of the Ministry. The Ministry may, in its sole discretion, acknowledge the Deliverables provided by the Vendor in any such publicity or publication. The Vendor shall not make use of its association with the Ministry without the prior written consent of the Ministry. Without limiting the generality of this section, the Vendor shall not, among other things, at any time directly or indirectly communicate with the media in relation to the Contract unless it has first obtained the express written authorization to do so by the Ministry.

7.02 OPS Confidential Information

During and following the Term, the Vendor shall (a) keep all OPS Confidential Information confidential and secure; (b) limit the disclosure of OPS Confidential Information to only those of the Vendor's Personnel who have a need to know it for the purpose of providing the Deliverables and who have been specifically authorized to have such disclosure; (c) not directly or indirectly disclose any OPS Confidential Information (except for the purpose of providing the Deliverables, or except if required by order of a court or tribunal), without first obtaining: (i) the written consent of the Ministry and (ii) in respect of any OPS Confidential Information about any third-party, the written consent of such third-party; (d) provide OPS Confidential Information to the Ministry on demand; and (e) return all OPS Confidential Information to the Ministry promptly after the termination or expiry of the Term, with no copy or portion kept by the Vendor.

7.03 Restrictions on Copying

The Vendor shall not copy any OPS Confidential Information, in whole or in part, unless copying is essential for the provision of the Deliverables. On each copy made by the Vendor, the Vendor must reproduce all notices that appear on the original.

7.04 Injunctive and Other Relief

The Vendor acknowledges that breach of any provisions of this Article may cause irreparable harm to the Ministry or to any third-party to whom the Ministry owes a duty of confidence, and that the injury to the Ministry or to any third-party may be difficult to calculate and inadequately compensable in damages. The Vendor agrees that the Ministry is entitled to obtain injunctive relief (without proving any damage sustained by it or by any third-party) or any other remedy against any actual or potential breach of the provisions of this Article.

7.05 Notice and Protective Order

If the Vendor or any of the Vendor's Personnel become legally compelled to disclose any OPS Confidential Information, the Vendor will provide the Ministry with prompt notice to that effect in order to allow the Ministry to seek one or more protective orders or other appropriate remedies to prevent or limit such disclosure, and it shall co-operate with the Ministry and its legal counsel to the

fullest extent. If such protective orders or other remedies are not obtained, the Vendor will disclose only that portion of OPS Confidential Information which the Vendor is legally compelled to disclose, only to such Person or Persons to which the Vendor is legally compelled to disclose, and the Vendor shall provide notice to each such recipient (in co-operation with legal counsel for the Ministry) that such OPS Confidential Information is confidential and subject to non-disclosure on terms and conditions equal to those contained in the Agreement and, if possible, shall obtain each recipient's written agreement to receive and use such OPS Confidential Information subject to those terms and conditions.

7.06 FIPPA Records and Privacy Compliance

The Vendor and the Ministry acknowledge and agree that FIPPA applies to and governs all Records and may require the disclosure of such Records to third parties. Furthermore, the Vendor agrees:

- (a) to keep Records secure and, without limiting the foregoing, to keep all NMS and Telephone System records and data in a secure location within Canada;
- (b) to provide Records to the Ministry within seven (7) calendar days of being directed to do so by the Ministry for any reason including an access request or privacy issue;
- (c) not to access any Personal Information unless the Ministry determines, in its sole discretion, that access is permitted under FIPPA and is necessary in order to provide the Deliverables;
- (d) not to directly or indirectly use, collect, disclose or destroy any Personal Information for any purposes not directly related to the performance of its obligations under the Contract and authorized by the Ministry;
- (e) to ensure the security and integrity of Personal Information and keep it in a physically secure and separate location safe from loss, alteration, destruction or intermingling with other records and databases and to implement, use and maintain the most appropriate products, tools, measures and procedures to do so, including the use of secure private networks and encryption of data;
- (f) to restrict access to Personal Information to those of the Vendor's Personnel who have a need to know it for the purpose of providing the Deliverables and who have been specifically authorized by the Ministry Representative to have such access for the purpose of providing the Deliverables;
- (g) to notify the Ministry in writing immediately upon becoming aware of any inadvertent or unauthorized access, use, disclosure or disposal of any Personal Information or OPS Confidential Information stored by the Vendor or carried on the Vendor's infrastructure or network;
- (h) that any confidential information supplied to the Ministry may be disclosed by the Ministry where it is obligated to do so under FIPPA, by an order of a court or tribunal or pursuant to a legal proceeding;

and the provisions of this paragraph shall prevail over any inconsistent provisions in the Contract.

7.07 Survival

The provisions of this Article shall survive any termination or expiry of the Contract.

ARTICLE 8 – INTELLECTUAL PROPERTY

8.01 Ministry Intellectual Property

The Vendor agrees that all Ministry Intellectual Property and every other right, title and interest in and to all concepts, techniques, ideas, information and materials, however recorded, (including images and data) provided by the Ministry to the Vendor shall remain the sole property of Her Majesty the Queen in right of Ontario at all times.

8.02 Vendor's Intellectual Property

All Intellectual Property rights vested in the Vendor or any of the Vendor's Personnel before the Effective Date, and any Intellectual Property created by the Vendor or any of the Vendor's Personnel or Subcontractors during the Term of the Contract independently of the performance of the Vendor's obligations under the Contract, are and shall remain vested in and the property of the Vendor or the Vendor's Personnel or supplier as the case may be.

8.03 Intellectual Property Rights in the Deliverables

Subject to any Intellectual Property owned by the Vendor before the Effective Date of the Contract or any Third-Party Intellectual Property, the Ministry shall own all Intellectual Property rights in any reports or other Deliverables developed for the Ministry under the Contract, including the data contained in the Network Management System. For greater certainty, the ownership rights granted herein shall not apply to any concepts, ideas, techniques or know-how relied upon by the Vendor to develop such Deliverables. To the extent the Deliverables contain any such Third-Party Intellectual Property or Vendor Intellectual Property, the Vendor hereby grants to the Ministry a perpetual, world-wide, non-exclusive, irrevocable, transferable, royalty-free, fully paid-up right and license: (a) to use, modify, reproduce and distribute, in any form, the Deliverables; and (b) to authorize other Persons, including agents, contractors or Subcontractors, to do any of the former on behalf of the Ministry.

8.04 No Restrictive Material

The Vendor shall not incorporate into any of the Deliverables, including any Records, anything that would restrict the right of the Ministry to modify, further develop or otherwise use the Deliverables in any way that the Ministry deems necessary, or that would prevent the Ministry from entering into any contract with any contractor other than the Vendor for the modification, further development of or other use of the Deliverables.

8.05 Vendor Representation and Warranty Regarding Third-Party Intellectual Property

The Vendor represents and warrants that the provision of the Deliverables shall not infringe or induce the infringement of any Third-Party Intellectual Property

rights. The Vendor further represents and warrants that it has obtained assurances with respect to any Third-Party Intellectual Property and any Vendor Intellectual Property that any rights of integrity or any other moral rights associated therewith have been waived.

8.06 Moral Rights

At the request of the Ministry, at any time or from time to time, the Vendor shall execute and cause the Vendor's Personnel and from any other party in the position to assert such rights in relation to any of the Deliverables to execute an irrevocable written waiver of any moral rights and other rights of integrity in the applicable Deliverable(s) in favour of the Ministry, which waivers may be invoked without restriction by any person authorized by the Ministry to use the Deliverables. Any such waiver shall be in a form acceptable to the Ministry. The Vendor shall deliver such written waiver(s) to the Ministry within ten (10) Business Days of the receipt of the request from the Ministry.

8.07 Copyright Notice

The Vendor shall place a copyright notice on recorded Deliverables, as may be specified by the Ministry through the Collaborative Business Relationship framework set out in Article 4, it provides to the Ministry under the Contract in the following form: "© Queen's Printer for Ontario, [***insert year of publication***]"

8.08 Further Assurances Regarding Copyright

At the request of the Ministry, at any time or from time to time, the Vendor shall execute and agrees to cause anyone in the position to assert copyright in (including the Vendor's Personnel) in relation to the Deliverables to execute a written assignment of copyright for any Deliverables to be owned by the Ministry in a form acceptable to the Ministry. The Vendor shall deliver such written assignment(s) to the Ministry within 10 Business Days of the receipt of the request from the Ministry. The Vendor shall assist the Ministry in preparing any Canadian copyright registration that the Ministry considers appropriate. The Vendor will obtain or execute any other document reasonably required by the Ministry to protect the Intellectual Property of the Ministry.

8.09 No Use of Ontario Government Insignia

The Vendor shall not use any insignia or logo of Her Majesty the Queen in right of Ontario except where required to provide the Deliverables, and only if it has received the prior written permission of the Ministry to do so.

8.10 Software Licence

During the Term of the Contract, the Vendor grants to the Ministry a world-wide, non-exclusive, irrevocable, royalty-free, fully paid-up right and license to the Ministry to use the Vendor's software and any software sublicensed by the Vendor and any updates thereto, solely in executable object code format and solely as required for the purposes of the Contract. The Ministry acknowledges that title to all Intellectual Property in the software shall remain with the Vendor or the software licensor, as applicable. The Ministry agrees not to copy, modify, disassemble or decompile the software provided by the Vendor or to authorize any third party to do so.

8.11 Ministry May Prescribe Further Compliance

The Ministry reserves the right to prescribe the specific manner in which the Vendor shall perform its obligations relating to this Article.

8.12 Survival

The obligations contained in this Article shall survive the termination or expiry of the Contract.

ARTICLE 9 – INDEMNITY AND INSURANCE

9.01 Vendor Indemnity

The Vendor shall indemnify and hold harmless the Indemnified Parties from and against all liabilities, costs, damages and expenses (including legal, expert and consultant fees), actions, claims, demands, lawsuits or other proceedings, (collectively, "Claims"), by whomever made, sustained, brought or prosecuted, arising out of, or in connection with, anything done or omitted to be done by the Vendor or the Vendor's Personnel in the course of the performance of the Vendor's obligations under, or otherwise in connection with, the Contract. The obligations contained in this section shall survive the termination or expiry of the Agreement.

9.02 Vendor's Insurance

The Vendor hereby agrees to put in effect and maintain for the Term, at its own cost and expense, with insurers having a secure A.M. Best rating of B+ or greater, or the equivalent, all the necessary and appropriate insurance that a prudent person in the business of the Vendor would maintain including, but not limited to the following:

commercial general liability insurance on an occurrence basis for third party bodily injury, personal injury and property damage, to an inclusive limit of not less than \$2,000,000 per occurrence, \$2,000,000 products and completed operations aggregate.

The policy is to include the following:

- the Indemnified Parties as additional insureds with respect to liability arising in the course of performance of the Vendor's obligations under, or otherwise in connection with, the Contract;
- contractual liability coverage;
- cross-liability clause;
- employers liability coverage (or compliance with the paragraph below entitled "Proof of W.S.I.A. Coverage" is required);
- 30 day written notice of cancellation, termination or material change;
- tenants legal liability coverage (if applicable and with applicable sub-limits); and
- non-owned automobile coverage with blanket contractual coverage for hired automobiles.

9.03 Proof of Insurance

The Vendor shall provide the Ministry with certificates of insurance, or other proof as may be requested by the Ministry, that confirms the insurance coverage required under Section 9.02 of this Agreement, and renewal replacements on or before the expiry of any such insurance. Upon the request of the Ministry, a copy of each insurance policy shall be made available to it. The Vendor shall ensure that each of its Subcontractors obtains all the necessary and appropriate insurance that a prudent person in the business of the Subcontractor would maintain and that the Indemnified Parties are named as additional insureds with respect to any liability arising in the course of performance of the Subcontractor's obligations under the subcontract for the provision of the Deliverables.

9.04 Proof of W.S.I.A. Coverage

If the Vendor is subject to the *Workplace Safety and Insurance Act, 1997, S.O. 1997, c.16, Schedule A ("WSIA")*, it shall submit a valid clearance certificate of WSIA coverage to the Ministry prior to the execution of this Agreement by the Ministry. In addition, the Vendor shall, from time to time at the request of the Ministry, provide additional WSIA clearance certificates. The Vendor covenants and agrees to pay when due, and to ensure that each of its Subcontractors pays when due, all amounts required to be paid by it/its Subcontractors, from time to time during the Term, under the WSIA, failing which the Ministry shall have the right, in addition to and not in substitution for any other right it may have pursuant to the Contract or otherwise at law or in equity, to pay to the Workplace Safety and Insurance Board any amount due pursuant to the WSIA and unpaid by the Vendor or its Subcontractors and to recover such amount from the Vendor together with all costs incurred by the Ministry in connection therewith.

9.05 Vendor Participation in Proceedings

The Vendor shall, at its expense, to the extent requested by the Ministry, participate in or conduct the defence of any Proceeding against any Indemnified Parties referred to in this Article and any negotiations for their settlement. The Ministry may elect to participate in or conduct the defence of any such Proceeding by notifying the Vendor in writing of such election without prejudice to any other rights or remedies of the Ministry under the Contract, at law or in equity. Each Party participating in the defence shall do so by actively participating with the other's counsel. The Vendor shall not enter into any settlement unless it has obtained the prior written approval of the Ministry. If the Vendor is requested by the Ministry to participate in or conduct the defence of any such Proceeding, the Ministry agrees to co-operate with and assist the Vendor to the fullest extent possible in the Proceedings and any related settlement negotiations. If the Ministry conducts the defence of any such Proceedings, the Vendor agrees to co-operate with and assist the Ministry to the fullest extent possible in the Proceedings and any related settlement negotiations. This section shall survive the termination or expiry of the Contract.

ARTICLE 10 – TERMINATION AND EXPIRY

10.01 Immediate Termination of Contract

The Ministry may immediately terminate the Contract upon giving notice to the Vendor where:

- (a) the Vendor is adjudged bankrupt, makes a general assignment for the benefit of its creditors or a receiver is appointed on account of the Vendor's insolvency;
- (b) the Vendor breaches any provision in paragraphs 7.01, 7.02, 7.03, 7.05, 7.06 or 7.07 of Article 7 (Confidentiality, Records and FIPPA) of this Agreement;
- (c) the Vendor breaches the Conflict of Interest paragraph in Article 2 (Nature of Relationship Between Ministry and the Vendor) of this Agreement;
- (d) the Vendor, prior to or after executing this Agreement, makes a material misrepresentation or omission or provides materially inaccurate information to the Ministry;
- (e) the Vendor undergoes a change in control which adversely affects the Vendor's ability to satisfy some or all of its obligations under the Contract;
- (f) the Vendor subcontracts for the provision of part or all of the Deliverables or assigns the Contract without first obtaining the written approval of the Ministry;
- (g) the Vendor's acts or omissions constitute a substantial failure of performance; or
- (h) the Ministry has issued a rectification notice to the Vendor setting out the manner and time-frame for rectification and the Vendor has failed to, within fifteen (15) Business Days of receipt of such notice, either (a) comply with that rectification notice or (b) provide a rectification plan satisfactory to the Ministry in accordance with Section 10.02

and the above rights of termination are in addition to all other rights of termination available at law, or events of termination by operation of law.

10.02 Rectification Notice

Subject to the above section, and the Plan set out in Article 4 Collaborative Business Relationship Management, where the Vendor fails to comply with any of its obligations under the Contract, the Ministry may issue a rectification notice to the Vendor setting out the manner and timeframe for rectification. Within ten (10) Business Days of receipt of that notice the Vendor shall either (a) comply with that rectification notice; or (b) provide a rectification plan satisfactory to the Ministry.

10.03 Vendor's Obligations on Termination

Upon the expiry or termination of the Contract, the Vendor shall, in addition to its other obligations under the Contract and at law:

- (a) at the request of the Ministry, provide the Ministry with any completed or partially completed Deliverables, and return Ministry property in accordance with Section 10.04;

- (b) provide the Ministry with a report detailing (i) the current state of the provision of Deliverables by the Vendor at the date of termination; and (ii) any other information requested by the Ministry pertaining to the provision of the Deliverables and performance of the Contract;
- (c) execute such documentation as may be required by the Ministry to give effect to the termination of the Contract; and
- (d) comply with any other instructions provided by the Ministry, including but not limited to instructions for facilitating and cooperating with respect to the transfer of its obligations to another Person.

This section shall survive the expiry or termination of the Contract.

10.04 Return of Property

- (a) Subject to Subsection 10.04(b), upon the termination or expiry of the Contract, the Vendor shall promptly deliver to the Ministry:
 - (1) all OPS Confidential Information;
 - (2) all recordings in a format approved by the Ministry; and
 - (3) any other Ministry property or information used in performing the Deliverables.
- (b) The Vendor may:
 - (1) retain all materials not specifically set out in Subsection 10.04(a); and
 - (2) retain copies of documents required by the Vendor to comply with its obligations under Requirements of Law and deliver the originals to the Ministry.

The Vendor's obligations in this section shall survive the termination or expiry of the Agreement.

10.05 Vendor's Payment upon Termination

The Vendor shall only be responsible for providing the Fee to the Ministry up to and including the Expiry Date. For greater certainty, the Vendor shall only be responsible for providing the Fee to the Ministry while the telephones remain operational and not once they have been decommissioned. Termination shall not relieve the Vendor of its warranties and other responsibilities relating to the Deliverables performed.

10.06 Termination in Addition to Other Rights

The express rights of termination in this Agreement are in addition to and shall in no way limit any rights or remedies of the Ministry under the Contract, at law or in equity.

10.07 Expiry and Extension

Unless terminated earlier or extended in accordance with the terms hereof, the Contract shall expire on the original Expiry Date. The Ministry may extend the term of the Agreement on the same terms, conditions and covenants as set out

in the Contract (except the option to extend, which shall not apply to the final extension period) for up to two additional periods of up to one year each by providing the Vendor with written notice at least six months before the original Expiry Date or the expiry of the then current extension period, as applicable. Each notice of extension shall set forth the precise duration of the extension.

10.08 Decommissioning of Vendor's Equipment and Transition

The Vendor shall decommission and remove all of its equipment at the Facilities by the original Expiry Date if the Ministry does not exercise any of its options to extend the term of the Agreement pursuant to Section 10.07. If the Ministry extends the term of the Agreement, the Vendor shall decommission and remove all of its equipment at the Facilities by the end of the last extension period. The Ministry shall provide the Vendor with at least six months prior written notice of the requirement to decommission and remove its equipment from all of the Facilities. The Vendor shall then decommission and remove its equipment in accordance with a schedule approved in writing by the Ministry, and shall coordinate the decommissioning and removal of its equipment with any new telephone services provider as directed by the Ministry.

10.09 Vendor's Property

Except as expressly set out otherwise in the Contract, the Vendor or its applicable Vendor's Personnel or Subcontractors shall retain ownership of all equipment (including telephone equipment, carts and computers), hardware and associated software used to supply the Deliverables, whether or not affixed at a Facility.

ARTICLE 11 – SECURITY CLEARANCE AND ACCESS TO FACILITIES

11.01 Definitions

"Company Level Check" is a security screening check, which requires checks to be conducted on all directors and officers of the company, regardless of whether they will have direct involvement in the work associated with the Deliverables which was deemed to require security screening. In order to be issued a company level clearance, all directors and officers of the company and the Company Security Officer ("CSO") must consent to a Security Screening Check and obtain Security Clearances;

"Company Security Officer" or **"CSO"** is a person that plays an administrative role in the security screening process on behalf of his or her company. The CSO must hold a valid Security Clearance issued by the Ministry prior to performing that role. The CSO will act as the main point of contact between the Ministry and the Bidder/Vendor and is responsible for the verification of identity for persons requiring screening for contracted work where required;

"Security Screening Check" is the process conducted by the Ministry to gather information on designated persons in order to provide a Security Clearance. There are five (5) levels of Security Screening Checks. The Security Screening Check form (LE221E) provides a description of the levels. At a minimum a Level 1 and 2 Security Screening Check will be conducted. The Ministry shall confirm the level of check to be conducted on the Security Screening Check form (LE221E) provided to the Bidder/Vendor upon reaching this stage in the process;

“Security Clearance” means a decision made by the Ministry, based on the information from the Security Screening Check, to provide a Security Clearance for designated persons and if applicable, a company level Security Clearance.

11.02 Security Screening Check

- (a) Security Clearances are not provided in perpetuity and are subject to revocation by the Ministry at its sole discretion at any time. Security Screening Checks shall be renewed at the intervals as may be specified by CSS, SCO, MGCS.
- (b) On notification from MGCS, the Vendor shall, during the Term, provide to the CSS, SCO, MGCS, completed Security Screening Checks for all persons engaged in the performance of the services who are either not cleared or for whom a renewal is required. All documents shall be provided through the Vendor’s designated Company Security Officer. Where Other Checks are required, CSS, SCO, MGCS will advise on process.
- (c) All Security Screening Checks shall be provided in form and content acceptable to the CSS, SCO, MGCS and shall include all required consents.
- (d) If a person or company has been deemed by the Ministry to require a Security Clearance they shall not engage in the performance of the services unless they have been provided a Security Clearance by the CSS, SCO, MGCS.

11.03 Changes

- (a) During the Term of this Agreement, the Vendor shall report to the CSS, SCO, MGCS, within five (5) Business Days thereof, any change to:
 - (i) any information provided as part of a Security Screening Check process;
 - (ii) employees, agents and Subcontractors or, where a Company Level Check is required , partners, directors and officers, who are or will be engaged in providing the security screening documents or engaged in the performance of the services.
- (b) The CSS, SCO, MGCS shall assess the above information and may instruct the Vendor to comply with any instructions arising which may include requests for provision of information to amend existing Security Clearances or provide for new Security Clearances.

11.04 Criminal Proceedings Policy

The Vendor shall develop a comprehensive policy that addresses how the Vendor will deal any Persons for whom the Vendor is responsible who are charged with or convicted of a criminal offence. The policy must address the responsibility of the Person to report any criminal charges and convictions to the Vendor and the Ministry. The policy must address the status of the Person prior to conviction and subsequent thereto. The Vendor’s written policy shall be subject to the prior written approval of the Ministry.

11.05 Security Issues

Despite any Security Clearance granted to the Vendor or any of the Vendor’s Personnel, the Ministry retains the right in its sole discretion to deny any Person

access to any or all of the Facilities or any Ministry offices. Without limiting the foregoing, the Ministry, in its sole discretion, may at any time prohibit the Vendor's Personnel from accessing any Facility or Ministry office, including in the event of a riot, lockdown or other security event at a Facility. If the Ministry prohibits such access by the Vendor, the provisions of Section 2.08(b) shall apply with necessary amendments.

11.05 Default under Agreement

During the Term of this Agreement, the Vendor shall be deemed to be in default under this Agreement if it fails to comply with the requirements of this Article 11.

11.07 Security Clearance Costs

The Ministry shall not bear the cost of the Vendor obtaining any Security Screening Checks or otherwise complying with the requirements in this Article 11.

ARTICLE 12 – PUBLICATION OF DATA

- 12.01 It is Ontario's intention, in accordance with the Open Data Directive and as part of its commitment to open data, to publish and allow the public to use:
- (i) procurement contract data, including the name of the Vendor; and,
 - (ii) data created or collected as an output of a contract,
- except where Ontario chooses not to publish the data in accordance with the Open Data Directive.

The Vendor expressly consents to the publication for public use of information as set out in items (i) and (ii) above.

Remainder of page intentionally left blank.

ARTICLE 13 - Counterparts and Delivery

13.01 This Agreement may be executed in any number of counterparts that, taken together, shall constitute one and the same agreement. To evidence the fact that it has executed this Agreement, a party hereto may send a copy of its executed counterpart to the other party hereto by e-mail. Such party shall be deemed to have delivered its executed counterpart of this Agreement on the date it sent such e-mail. In such event, such party shall forthwith deliver to the other party hereto an original counterpart of this Agreement executed by such party.

IN WITNESS WHEREOF the parties hereto have executed this Agreement effective as of the date first above written.

Her Majesty the Queen in right of Ontario
as represented by the Solicitor General

Signature: 

Name: Shelley Underlander

Title: ADM 050

Date of Signature: Feb. 25/20

Pursuant to delegated authority

Synergy Inmate Phone Solutions, Inc.

Signature: 

Name: Charles Slaughter

Title: President

Date of Signature: FEB 19, 2020

I have authority to bind the Vendor.

Schedule 1: Description of Deliverables, Calling Rates and Supplementary Terms

A. Description of Deliverables

A.1 Objectives

Positive communication between inmates and their families, friends, organizations and agencies within the community make significant contributions towards inmate rehabilitation and successful reintegration into society. To assist them in their rehabilitation and reintegration, the Ministry provides inmates with reasonable and direct access to telephones while in custody.

In order to continue providing inmates with positive communication opportunities, the Ministry requires the services of the Vendor to supply, deliver and install a new inmate Telephone System that aligns with the Ministry's policy and operational objectives to:

- protect victims of crime, witnesses and other members of the public from harassment and intimidation by inmates while in correctional facilities;
- restrict the ability of inmates to conduct criminal activity while in the custody and control of the Ministry; and
- provide inmates with reasonable access to telephone services, at reasonable rates, for maintaining connections with family, legal counsel, and with community organizations and agencies such as: the John Howard Society, the Elizabeth Fry Society and the Ontario Ombudsman.

The Ministry requires the Vendor to provide complete, end-to-end, and ready to use services to meet the telephone call requirements as further detailed below. The Vendor's Telephone System must be delivered in a secure manner and must be the same for all of the Ministry's 25 Facilities.

It is anticipated that there will be an annual average of 38.5 million minutes of local calls and 5 million minutes of long distance calls placed from the Facilities, though the Ministry makes no guarantee as to the number of telephone calls that will be made on a given day. The Telephone System for inmate calls must have sufficient capacity to use 100% of all telephones concurrently.

The Vendor must comply with the requirements of *Telecommunications Act* to provide the services. Any applicable requirements such as license(s) and registration with the Canadian Radio-television and Telecommunications Commission (CRTC) must be maintained by the Vendor throughout the Term of the Agreement.

The Vendor shall assume all costs associated with providing all the Deliverables; the Ministry will not pay for any costs associated with any of the Deliverables.

A.2 High Level Summary of Deliverables

The Vendor shall provide a telephony system for the Ministry's Facilities as further described herein. All equipment supplied by the Vendor for the purpose of providing the Deliverables must be new and not previously used, refurbished, repaired, or re-imaged, unless recycled through manufacturing methods which render such recycled raw materials into new raw materials.

The following Deliverables are required for all of the Ministry's 25 Facilities:

- installation of new conventional public pay telephones and the provision of payphone services independent from the inmate telephone services;
- provision of new visitation handsets
- provision of a secure Network Management System for use by the Ministry for the configuration and monitoring of inmate telephone services, as well as generating reports;
- provision of both the inmate telephone services and conventional public pay telephone services with uninterrupted service, meaning the telephone services are available at all times, subject to any planned outages or circumstances beyond the Vendor's control;
- the supply, installation and maintenance of all telephony components for the required telephone services including: network redundancy, all computing and networking apparatuses, telephones, disconnect switches, cabling to support network system equipment, equipment stands, racks, cabinets, backup power and surge protection devices;
- setting up of accounts and PINs for inmates;
- verification of inmate identity using Two Factor Authentication;
- provision of maintenance services and technical support for the Network Management System, telephones and associated equipment to maximize performance and resolve any service outages; and
- provision of training to Ministry staff on use of the Network Management System, telephones and any associated equipment.

A.2.1 Conventional Public Pay Telephones

The Ministry requires the installation of new conventional public pay telephones in each of its Facilities for use in designated secure and non-secure areas of the Facilities. The Ministry requires the number of conventional public pay telephones set out in Table 2 of section A.2.3.1 –Facility Telephones.

The Vendor shall certify that its public pay telephone service contains no "back doors" and has been tested to detect security vulnerabilities. Conventional public pay telephones must not be subject to enhanced security features, such as call blocking, nor shall they be programmed to only allow access to specific Ministry approved telephone numbers. The conventional public pay telephones must only allow for out-going calls, that are either user pay or collect, and must be

Accessible in accordance with the *Accessibility for Ontarians with Disabilities Act, 2005*, as amended, and regulations thereunder. For greater certainty, the Vendor shall ensure that at a minimum there is at least one conventional public pay telephone per Facility that is TTY enabled, wheelchair accessible and adapted for the visually impaired.

A.2.2 Network Management System

The Ministry requires the Vendor to supply a Network Management System for its inmate Telephone System, with uninterrupted access, as well as technical support for the Network Management System.

The Network Management System must be accessible via a secure web portal. Ministry staff must be able to access the Network Management System through personal computers. Access must be limited to authorized personnel using accounts with Two Factor Authentication. The Network Management System must allow for different access levels and functionality, as determined by the Ministry.

The Network Management System must include technology that will allow the Ministry to configure, monitor and report on inmate telephone services. This shall include:

- i. adding or removing one or more of the functionalities and features on the telephone devices as often as required and at as the discretion of the Ministry;
- ii. deactivating specific unique identifier accounts;
- iii. configuring a time limit for inmates to record a name;
- iv. configuring a limit on the number of times a particular telephone number can be called in one (1) calendar day from all Facilities or from an individual account;
- v. configuring telephone numbers for each Facility, or by inmate account;
- vi. configuring call length limits generally, and by specific account;
- vii. configuring automated call block notification;
- viii. configuring telephone key pad to automatically disable immediately following call acceptance and remain disabled for the duration of the call;
- ix. recording all instances and dates where three-way calling detection settings were used, and maintaining a log of those instances;
- x. configuring hours that calls can be made at each Facility;
- xi. disabling one or more telephone units within a Facility; and
- xii. reporting capabilities as set out in section A.2.11.1 - Reporting and Data Requirements.

The Network Management System must support compliance with applicable Government of Ontario I & IT policies and GO-ITS standards, which may be amended from time to time. All GO-ITS policies and standards can be found at <https://www.ontario.ca/page/information-technology-standards>.

Specifically, the Ministry requires that access to the Network Management System complies with the Corporate Policy on Electronic Identity, Authentication and Authorization. The Network Management System shall support High Assurance, as defined by the aforementioned policy. Controls to this end shall include password protections, secure logs, enhanced monitoring and audit, secure issuance of credentials through a local registration authority, granular role-based access control and user profiles, and self-serve reset of passwords. The Vendor shall support the Ministry in maintaining ongoing compliance with these requirements, and any amendments thereto.

The Network Management System shall comply with the applicable GO-ITS 25.0 requirements indicated as a "must" in sections 3.1, 3.3, 3.4, and 3.5.

The Network Management System shall support a secure, web-based management interface for use by authorized Ministry staff. Web application security associated with this interface shall comply with those GO-ITS 25.13 requirements relevant to the proposed platform. All remote access to the Network Management System shall comply with the applicable GO-ITS 25.7 section 2 requirements labelled "must".

The Network Management System shall be updated and patched against deficiencies and vulnerabilities in a timely manner, with competent support to resolve technical issues and provide for effective incident response if required. Patching metrics and vulnerability management shall comply with GO-ITS 42.0 requirements labelled "must".

If the Network Management System meets the GO-ITS 25.21 definition of a cloud service, or relies in part on cloud services, the Vendor shall ensure that the Network Management System complies with the requirements indicated as a "must" in GO-ITS 25.21 section 2.5. The Vendor shall provide the Ministry with the supporting evidence for GO-ITS 25.21 section 2.6 audit/reporting requirements.

Any encryption used to protect communications or to ensure integrity or identities within the Network Management System shall comply with the specifications set out in GO-ITS 25.12 Appendix A.

Some Facilities have a PLC controlled with a GUI located in monitoring stations overlooking inmate day-areas. The PLC and GUI are owned and operated by the Ministry. For those Facilities that have a PLC controlled with a GUI, the Vendor shall provide an electronic relay interface with the PLC so that the GUI may allow staff in the monitoring stations the ability to disconnect all telephones located in the areas monitored by the stations. Moreover, the Vendor shall ensure that the disconnection of the telephones may be controlled from the Network Management System.

The Vendor shall provide a digital copy of all the data stored in the Network Management System, in a comma-delimited format, to the Ministry at the expiration or termination of the Agreement, with no copy or portion retained by the Vendor. The data required to be stored is set out in section A.2.11.1. This digital copy shall be provided in accordance with the Vendor's Transition Out Plan, as described in section A.5.1 Vendor Transition Out Plan.

The Vendor shall provide training to the Ministry to effectively access and use the Network Management System in accordance with section A.6. The Vendor shall conduct acceptance testing on the Network Management System, with the Ministry, in accordance with section A.5.

Technical support resources must be available to the Ministry seven days a week between the hours of 8 a.m. and 5 p.m. Eastern Time to assist with trouble shooting or site-specific issues.

A.2.3 Inmate Telephones

The Vendor shall provide two (2) types of non-coin operated inmate telephones: stationary inmate telephones and portable inmate cart phones.

Stationary inmate telephones shall be physically mounted to a vertical surface.

Portable inmate cart phones are readily movable phones on wheels. Portable inmate cart phones may be wired and plugged into telephone jacks that are available throughout the Facility.

All inmate telephones must:

- i. have physical characteristics that can withstand greater than normal physical stress on the telephone and handset;
- ii. be durable, tamper proof and ruggedized for use in a Facility;
- iii. have an appropriate method of connection for safe and secure operation (a detachable connection at both the wall jack and the phone for portable inmate cart phones and a concealed connection for stationary inmate telephones);
- iv. have a tamper-resistant exterior, armoured un-detachable handset cord and a sealed handset of a sturdy coating;
- v. be fitted with a volume control device, which will allow the inmate to increase or decrease the volume of the handset; and
- vi. be Hearing Aid Compatible (HAC).

A minimum of two (2) stationary inmate telephones and two (2) portable inmate cart phones per Facility must be Accessible in accordance with the *Accessibility for Ontarians with Disabilities Act, 2005*, as amended, and the regulations made thereunder.

The Vendor shall ensure that the portable inmate cart phones:

- vii. do not obscure visibility above the phone so that the correctional officer may visually see the inmate;
- viii. are stable and do not pose a risk to health and safety standards; and
- ix. allow inmates to dial through the food slot door of each cell, which begin from a height of 744 to 1334 mm off the ground.

The portable inmate cart phones shall be adjustable to three different heights, so as to accommodate the differences between the heights of the food slot doors.

A.2.3.1 Facility Telephones

The Ministry requires the number of telephones set out in Table 1 – Total Number of Required Facility Telephones, to be divided up amongst the Ministry's 25 Facilities. The Ministry, in consultation with the Vendor shall determine the distribution and location of the additional phones. The number of inmate telephones, both stationary and portable cart, as well as conventional public pay telephones may change from time to time, at the sole discretion of the Ministry.

Table 1 – Total Number of Required Facility Telephones

Conventional Public Pay Phones	Stationary Inmate Telephones	Portable Inmate Cart Phones
38	1,243	140

Table 1 above represents the total number of telephones the Ministry requires.

The Ministry reserves the right to determine the location of each telephone. The Vendor may be required to install, remove or relocate inmate telephones or conventional public pay telephones during the Term of the Agreement, at the sole discretion of the Ministry.

In addition, the Vendor shall supply one stationary inmate telephone and one portable inmate cart telephone to be used by the Ministry for acceptance testing, as set out in section A.5, prior to the full roll out of the Vendor's Telephone System and Network Management System, and as may be necessary in response to any issues that arise during the Term of the Agreement.

A.2.3.1.1 Visitation Handsets

The Vendor shall supply the Ministry with equipment for visitation phones for each of the Facilities, at no cost. The visitation handsets shall be constructed in a similar fashion to the inmate telephones provided under this Agreement. The Vendor shall be responsible for the decommissioning of the current visitation

handsets, and the installation and ongoing maintenance of the new visitation handsets, at no cost to the Ministry.

The visitation handsets shall not be capable of making outside calls and shall specifically be programmed not to record.

The Vendor shall provide the exact specifications of the visitation handsets to the Ministry for review and approval. The Vendor shall not install the visitation handsets without the prior written approval of the Ministry. The visitation handsets shall be subject to acceptance testing in accordance with section A.5 Transition between Service Providers and Implementation Plan.

A.2.3.2 Inmate Calls

The Vendor's inmate Telephone System shall allow inmates to make both collect calls and direct debit calls. Inmate telephones shall only permit out-going telephone calls; no incoming calls shall be allowed. All calls are to be PIN based, as further set out in section A.2.3.3. The Ministry requires that inmates have the ability to make the following different types of calls:

- 1) debit and collect local calls
- 2) debit and collect long-distance calls terminating in Canada
- 3) debit and collect long-distance calls terminating in the United States
- 4) debit and collect long-distance calls terminating internationally

For greater certainty, and despite anything to the contrary in the Vendor's Bid, destination-number-based prepaid, where the call is prepaid by the recipient of the call, and credit collect calls, where the called party pays by credit card at the time of the call, shall not be allowed during the Term of the Agreement.

In the event that an inmate does not have funds in the inmate's telephone account, and the recipient's telephone does not accept collect calls, the Vendor shall provide the inmate with a free two-minute courtesy call to one specific destination number. This free courtesy call to the specific destination number may be made once every 30 days.

The Vendor shall post the calling rates for each of the different types of calls near each inmate telephone or group of inmate telephones, as designated by the Ministry. The Vendor shall provide an easy-to-read information handout for inmate distribution, and posters containing pictograms for posting, outlining how to use the inmate telephones. The information handouts and posters shall be in both English and French, and must be pre-approved in writing by the Ministry prior to their distribution or posting.

The Vendor shall provide voice connection quality rated as having a mean opinion score of 4.0 or better as outlined in the standard by the ITU-T using the

mean opinion score evaluation process of the Conversation Opinion Test as documented in Annex A of Recommendation P.800.

Inmate calls shall be limited in duration, as directed by the Ministry. The Network Management System must have the ability to allow for adjustments in call length limits, as often and as frequently as the Ministry requires in its sole determination. Call length shall be configurable to allow for longer calls to numbers identified by the Ministry. When an inmate call is nearing the maximum time limit, the Vendor's inmate Telephone System shall automatically provide a prompt that the time limit is approaching and that the call will be terminated within a specified amount of time, as configured by the Ministry.

Currently, there is no limit as to the number of telephone calls an inmate can place on any given day. The Network Management System must allow for the creation and enforcement of configuring the maximum number of times a particular telephone number can be called in one (1) calendar day from all Facilities or from an individual inmate account.

The hours for inmate telephone use are set by each individual Facility's Superintendent, and thus may vary as between each Facility. The Network Management System must provide for the ability to control the hours that the telephones are available for use on a daily basis, including temporarily suspending the use of all the telephones in one or more Facilities.

The Network Management System must have the capability to allow the Ministry to both automatically and manually render telephones out of service during designated periods, for specific Facilities or specific individual inmate telephones within a Facility. All telephones must have the capability to be shut off through relays, either hard wired or software based through the Network Management System. This capability must be able to be managed through the Network Management System.

The Ministry must preapprove any call display, voice-over message scripts and prompts, and the sequence of operations programming of the call itself, prior to their use.

The Vendor shall ensure that all dialling services, such as three-digit numbers and all the 310-xxxx numbers for services that either support call redirection or call conferencing, are disabled from inmate telephones. The Vendor shall allow access to toll-free numbers that are identified and preapproved by the Ministry.

Access to a Vendor provided live operator is not permitted at any time during the inmate calling process. The Vendor shall provide automated menu options on the phone for inmates to select before calls to assist inmates with possible call functionality issues or issues with the balance remaining in the inmate telephone account.

Inmates shall be required to hang up before dialling a new number. Concurrent calling of the same telephone number from more than one inmate telephone shall not be permitted unless to a Ministry preapproved telephone number.

The Vendor shall block all three-way and conference calls. The Telephone System must be able to detect chain dialling and secondary dial tones, and immediately disconnect them. The Network Management System shall provide the ability to monitor and log the time, dates and settings used.

All calls must be carried on secure networks resistant to unauthorized eavesdropping, sniffing interceptions of data and recording.

A.2.3.3 Personal Identification Number and Authentication Requirements

Upon entering a Facility, an inmate's Personal Information is entered into a Ministry database called the Offender Tracking Information System (OTIS). Once the Personal Information is entered into OTIS, the inmate is assigned an identification number, known as the OTIS number. This number remains with the inmate for life, and should an inmate be readmitted to a correctional facility, the OTIS number would remain the same.

The Vendor shall create telephone accounts for each inmate using the OTIS number as the unique identifier. Once an account is set up, inmates shall then be afforded the opportunity to create their own PIN to be used for authentication purposes along with their OTIS number. The Vendor shall ensure that the inmate may change their PIN as often as the inmate wishes without intervention from the Ministry.

Once inmates have set up their PIN, the Vendor shall allow inmates to record a name immediately after enrolment and may re-record as may be necessary from time to time without intervention from the Ministry. The recorded name shall be stored and played back to the called party with all subsequent call attempts. The time allotted to record a name shall be configurable through the Network Management System.

In order to create the telephone accounts and maintain their accuracy, the Ministry requires that the Vendor accept data automatically transferred from OTIS, via secure server, to be pushed automatically at least every 15 minutes. The Ministry will push the OTIS number automatically to the Vendor in order to create the account. The Vendor shall be responsible for all costs associated with this data transfer, including housing the data on a secure server in Canada.

The data transferred between OTIS and the Vendor's Telephone System shall automatically update the account status in the Telephone System. All data to be transferred from OTIS is Personal Information and must be encrypted both at rest

and in transit. All encryption shall be in compliance with the requirements of GO-ITS 25.12 Security Requirements for the Use of Cryptography, Appendix A.

The Vendor shall:

- generate an account for each inmate that is the same as the inmate's OTIS number;
- have the account available for inmate use within five (5) minutes of the OTIS information being pushed to the Vendor; and
- allow the inmate to create a PIN once the account is available, record their name for future playback, and require the inmate to enter both their OTIS number and PIN prior to making a call, in order to verify the identity of the caller using Two Factor Authentication.

A.2.4 Inmate Telephone Accounts

The Vendor shall create and manage inmate telephone accounts to allow inmates to make direct debit calls. The Vendor shall create these inmate telephone accounts using the inmate's OTIS number as the unique identifier for the inmate. No other Personal Information will be provided to the Vendor.

All money allotted to a specific inmate telephone account shall be for the sole use of that inmate. The Vendor shall not deduct any administrative fees from an inmate telephone account. Funds in an inmate telephone account shall have no value outside of the services provided and may not be transferred to other inmates.

In order to keep inmates apprised of available funds in their inmate telephone account, the Vendor shall:

- provide inmates with the balance on their accounts both at the beginning and end of each call in the language (English or French) initially selected by the inmate, as further set out in section A.2.6;
- inform inmates if there are insufficient funds to initiate or to continue a call; and
- provide a warning to inmates prior to disconnecting a call due to insufficient funds.

Inmate telephone accounts shall be treated as inmate property in accordance with the *Ministry of Correctional Services Act*, as amended, and the regulations made thereunder. All funds in the inmate telephone account shall have no expiry date and shall remain available for the inmate to use until such time that the Ministry advises the Vendor to close the account. Upon being advised to close an account, the Vendor shall ensure that no further debit calls may be made from that account.

Payment into the inmate telephone accounts shall be in accordance with Section 6.03 of the Agreement – Inmate Telephone Accounts. For greater certainty, payments into telephone accounts shall not be made by third parties, nor shall they be made by telephone, online, in-person or via kiosk.

A.2.5 Privacy Requirements

The Vendor's Network Management System and Telephone System shall maintain rigorous system security to prevent unauthorized access or use of system data. System design requirements shall protect Ministry data systems from viruses and other forms of contamination.

All data shall be confined to secure private networks and all traffic that traverses across the Internet shall be encrypted in accordance with GO-ITS 25.12 Security Requirements for the Use of Cryptography (including Appendix A specifications) and Information Security Classification Operating Procedures, Mandatory Requirements for Medium and High Sensitivity Information, attached hereto as Appendix #1.

The Vendor shall only collect the information identified herein, and shall not use this information for any purpose other than the purposes expressly set out herein, without the prior written consent of the Ministry. The Vendor shall submit to the Ministry the details of the data fields it intends to collect for approval from the Ministry prior to collecting any information or metadata. For each data field, the Vendor shall set out:

- why the information is required;
- how the information will be used;
- what information will be collected;
- where the information will be stored;
- who will have access to the information and under what conditions; and
- what process and notifications shall be followed prior to sharing, storing and transferring the information.

The Ministry shall develop and provide the Vendor with a process for complaints about the Vendor's privacy practices to be escalated to the Ministry. The Vendor shall create, document and submit for Ministry approval a privacy process and policy in respect of the Deliverables. The privacy process and policy must align with that of the Ministry's, which will be provided to the Vendor. The Vendor shall incorporate any feedback from the Ministry into its privacy process and policy, as necessary, in order to obtain Ministry approval. The Vendor shall not commence the transition of services until Ministry approval is obtained. For greater certainty, the Vendor shall ensure that, at a minimum, its privacy process and policy details:

- how the Vendor will manage questions and complaints about its privacy practices;
- how the Vendor will manage incidents involving any privacy or security breach;
- the plan for data breach reporting, disclosure, communication and testing should a breach occur, and documented with an incident response plan and a breach response protocol;
- conducting independent privacy audits or assessments;
- a defined system access policy that manages Vendor Personnel access to the data, which includes:
 - a process to grant specified Vendor Personnel with account access;
 - ensuring that the level of account access is only what is required to perform duties using role-based access;
 - a process to periodically review account access;
 - a process to promptly revoke account access when no longer needed;
 - regular monthly reporting of both active and inactive system accounts, the names of those individuals and the associated level of access; and
 - access must be auditable and auditing capabilities must comply with GO-ITS 25.0 General Security Requirements, including the access logging and audit requirements outline in sections 3.1.2, 3.4.2 and 3.4.3.

The Vendor shall ensure that the Vendor Personnel providing the Deliverables receive training with respect to its privacy process and policy. The Vendor shall update its training and retrain its Vendor Personnel, as necessary or as may be directed by the Ministry.

The Vendor shall notify the Ministry in writing immediately should there be a cyber-threat or actual privacy breach relating to Personal Information.

A.2.6 Voice-over Messages

The Vendor's Telephone System, both for inmate telephones and conventional public pay telephones, shall prompt the user to select either English or French for all further voice-over messages for that call.

Once a call is placed from an inmate telephone, prior to the call being connected, the Vendor's inmate Telephone System shall provide an automated voice-over message to the call recipient in the language selected by the inmate. The voice-over message shall inform the call recipient as to who is calling using the full name of the inmate as recorded, and prompt the call recipient to accept or decline the call prior to connection, using voice or a keypad entry. The recorded

voice-over messages shall be subject to Ministry review and approval prior to implementation, so as to ensure content and recording quality.

A.2.7 Provincially Allowed Telephone Numbers

The Vendor shall allow for the programming of numbers, such as lawyers' telephone numbers or other common access numbers that shall be accessible on inmate telephones in one or more Facilities. These telephone numbers shall be programmable through the Network Management System. These allowed telephone numbers shall be updated as often and as frequently as required by the Ministry.

The Vendor shall allow for the programming of these telephone numbers to be exempt from Ministry identified security programming features and functions, including three-way call detection. Inmates must be able to navigate an automated attendant system using the key pad for these identified telephone numbers.

A.2.8 Call Blocking

The Vendor's Telephone System shall instantly prevent inmate telephone calls from being completed to specified telephone numbers that are identified as blocked by the Ministry. Call blocking features may vary from being:

- province-wide at all Facilities;
- Facility specific;
- telephone specific; and
- inmate account specific.

When attempts are made to call a blocked number, the Vendor shall deliver an automated message to the inmate that the call cannot be completed at this time.

The Vendor shall maintain an electronic log of all occasions when inmate calls were blocked. This log shall be accessible to the Ministry through the Network Management System. The Vendor shall allow the Ministry to update the blocked telephone numbers locally through the Network Management System, as often as required. The Vendor shall immediately inform the Ministry by an automated mechanism should an inmate attempt to call a blocked telephone number.

A.2.9 Restricted Number Calling

Through the Network Management System, the Ministry must be able to restrict, as required, the telephone numbers that a given inmate may call. For greater certainty, the Telephone System would only allow the inmate to call the specified numbers.

A.2.10 Recording and Monitoring

With the exception of the recording of the inmate's name to inform the call recipient as to who is calling, at no time shall the Vendor listen to, stream the voice information, record or store any of the inmate recordings or telephone calls.

A.2.10.1 Individual Cases Based on Warrant or Court Order by Law Enforcement

On occasion, law enforcement authorities may be authorized to record specific inmate telephone calls, as may be authorized by a warrant or court order. In these instances, the Vendor shall assist law enforcement in recording the calls, if required.

A.2.10.2 Recording and Monitoring of Inmate Calls by the Ministry

The Network Management System shall allow for call monitoring, interception, recording and storage of an inmate call, should the Ministry require. These activities shall be restricted to authorized Ministry staff, as specified by the Ministry in writing.

The Telephone System shall provide notice of the potential interception of a telephone conversation to both parties to the conversation by way of a voice-over message or other means.

The Network Management System shall allow the Ministry to specify the calls to be monitored, intercepted, or recorded and sorted by date and time, OTIS number, phone location, or number called.

The Network Management System shall maintain a log that identifies all occasions when call interception took place. The log shall list the date, time, OTIS number, number called and identify the individual who intercepted the call.

A.2.11 Call Tracking and Call Traffic Reports

The Vendor's Network Management System shall have the capability to track telephone use and calls via an automated process. This process shall enable the Ministry to identify specific telephone numbers called from specific inmate telephones or from specific OTIS numbers, as required.

The Network Management System shall have the ability to produce call details including:

- OTIS number used to make the call;
- telephone used to make the call;
- the telephone number called;
- type of call made; and
- the time and duration of the call.

The Network Management System shall allow for the call tracking reports to be generated by the Ministry, at any Facility, at any time and without interruption. The Network Management System shall keep an electronic log of the account used to download the data reports, for audit purposes.

The Vendor shall provide the Ministry with direct real-time access to all call record data generated during the Term of the Agreement.

A.2.11.1 Reporting and Data Requirements

The Network Management System shall be capable of generating data points that would allow for extraction of content in an Open Format. At a minimum, the following data points are required:

- OTIS number
- Phone number called
- Call start time
- Call end time
- Total duration of call
- Total cost of call
- Phone set used
- Facility
- Security features used (e.g. whether blocked, reason for termination, interception, etc.)
- Call failure

The Vendor shall also provide the Ministry on a monthly basis a system service report for each Facility that at a minimum outlines the following:

- the number of instances that the Vendor was contacted by the Ministry for system-related service issues;
- the number of instances that the Vendor contacted the Ministry for system-related service issues;
- the number of occasions on which the Vendor provided on-site and off-site technical assistance or repairs set out in section A.7;
- the average time needed to resolve each service issue or technical repair relating to the Telephone System, including both hardware and software; and
- data demonstrating whether the Vendor has met the key performance indicators set out in section A.8.

A.3 Technology Infrastructure, Systems and Applications

In most Facilities, the cabling from the main telecom rooms to the communications closets is Category 3 (CAT 3) twisted pair cabling. Cabling from communications closets to existing telephones range from CAT 3 to Category 6

(CAT 6) twisted pair cabling. Any costs associated with wiring upgrades and associated conduit that are necessary for the operation of the inmate telephones and conventional public pay telephones shall be the responsibility of the Vendor. Any such additional wiring will become the property of the Ministry once installed. The Ministry will not install any additional cabling, analog or digital (CAT 3, CAT 5, CAT 6, fibre optic cabling etc.) required beyond the minimum CAT 3 wiring already in existence within the Facilities and owned by the Ministry. All wiring must comply with GO-ITS Number 80.0 Cabling and Wiring for Voice/Data Communications in Government Buildings.

The Vendor shall install all technical components required to ensure the optimal operation of the entire business solution and be responsible for the safe and secure operation of its intended purpose. All equipment, other than the wiring currently installed in each Facility's main telecom room, shall be supplied, owned, supported and maintained by the Vendor. This equipment shall include, but not be limited to, inmate telephones, BIX (Building Industry Cross-connect) blocks, digital equipment (i.e. digital analog converters), on/off switches and computers for the Network Management System.

The Vendor shall supply all necessary power conditioners, line filters, UPS devices or any other devices to be connected between a Ministry power outlet and the Vendor's equipment. In the event of a power failure, all the powered components in the Facilities that are necessary for the operation of the Vendor's equipment must have a UPS that will keep all the components operational for a minimum of one hour. The Vendor shall ensure network transmission processes and features are implemented to prevent loss of data or corruption of data in the event of a network or system failure during transmission.

The Vendor shall provide reliable inmate telephone service with separate redundant connectivity at each Facility for the purpose of maintaining functionality in the event of a primary data circuit failure.

The Vendor shall ensure that all telephone services and voice recordings are subject to time stamping and synchronization, with reference to an accurate and redundant time source.

The Vendor shall deploy all security and technology updates and patches on its hardware and software in accordance with the GO-ITS 42 Security Requirements for Enterprise Vulnerability Management policy.

The Vendor should have access to a mirror image copy of the system that can be accessed and updated when the connection is not available, in order to ensure service continuity. The Vendor shall immediately notify the Ministry in writing upon becoming aware of any data corruption. Moreover, the Vendor shall take all necessary steps to protect data integrity by:

- encrypting the data both in transit and at rest or using integrity-validating cryptographic schemes and constructions;
- enforcing multi-factor authentication for any access to data;
- intrusion detection and file integrity monitoring or validation; and
- conducting penetration testing, security audits and physical inspections on a regular basis.

Should the Vendor require a backup of the data outside of the set backup schedule, the Vendor shall provide the Ministry with three (3) Business Days' advanced written notice of the need to back up the data and the reasoning behind it. Should there be an unforeseeable need for this backup, the Vendor shall provide the Ministry with written notice upon becoming aware of these circumstances. Following this unscheduled backup, the Vendor shall delete the data, and provide written confirmation of deletion of the data to the Ministry.

A.4 Modernization

The Ministry has an ongoing interest in identifying innovative, cost effective products and services related to the Deliverables.

In the event that the Vendor acquires or develops, throughout the Term of the Agreement, any products or services that may enhance or support the Deliverables, or reduce the costs of the calls while continuing to meet the needs of the Ministry, the Vendor shall notify the Ministry in writing. The proposed products or services shall include support or enhancements to, but not take away from, the original functionalities of the Deliverables. The Ministry will evaluate the proposed supports and enhancements, and will work with the Vendor, in determining whether to implement the changes. The Vendor shall not modify or change any products or services without the prior written approval of the Ministry.

A.5 Transition between Service Providers and Implementation Plan

The Vendor shall work in a cooperative manner with:

- the Ministry's current service provider during the transition and implementation of the Vendor's system, for transitioning in; and
- any new service provider, for transitioning out, during the Vendor's decommissioning and removal of its equipment prior to expiry of the Agreement.

The Vendor shall develop a detailed implementation plan which shall set out a schedule identifying the order in which the Vendor shall install the equipment and begin providing services at the Facilities. The order in which the equipment shall be installed shall be subject to Ministry approval.

The Vendor shall create an acceptance testing plan for approval by the Ministry. The Ministry may provide feedback to the Vendor to incorporate into the acceptance testing plan, and the Vendor may be required to resubmit the acceptance testing plan for approval.

The acceptance testing plan shall set out step by step the necessary test procedures, and data and voice input and output anticipated to meet all requirements of the Deliverables:

- Conventional public payphones;
- the Network Management System;
- the Telephone System;
- inmate phones;
- all types of calls;
- all operational requirements;
- PINs;
- inmate telephone accounts;
- voice prompts;
- provincially allowed telephone numbers;
- call blocking;
- restricted number calling;
- recording and monitoring;
- reporting.

The initial installation and acceptance tests shall take place at the Toronto South Detention Centre, in Toronto. The initial installation, acceptance testing by both the Ministry and Vendor, and any correction required as a result of the acceptance testing must be completed prior to the installation of the Network Management System and Telephone System Ministry-wide. All acceptance testing shall include "dummy" data, and not live data.

The Vendor shall not proceed with executing the implementation plan and installation of the inmate telephones and conventional public pay phones without the prior written approval of the Ministry.

Installation of the inmate telephones and conventional public pay telephones, and any required staff training, must be completed at each Facility prior to service going live at the Facility. Vendor Personnel on site to install equipment must be accompanied by Ministry personnel at all times.

All testing shall be undertaken at no cost to the Ministry.

A.5.1 Vendor Transition Out Plan:

The Vendor shall create a transition out plan that details how the Vendor plans to transition out at the end of the Term of the Agreement to another service provider, if required, and the plan shall address such elements as:

- a) migrating inmate account information with minimal error, verification, or disruption;
- b) migrating the data on the blocked call list and the provincially allowed telephone numbers at province-wide, regional, and institutional levels; and
- c) each stage of deactivation, deletion and destruction of Personal Information including an audit trail to ensure disposal is done in a secure manner and in accordance with the GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices and Digital Storage Media policy. The Vendor shall provide the Ministry with written confirmation following each stage of deactivation, deletion and destruction.

Prior to the expiry of the Agreement, the Vendor shall work collaboratively with a new service provider, to transition the services, as required.

A.6 Staff Training

The Vendor shall provide the Ministry with a staff training plan. The training plan shall include details for both onsite and offsite training. The Vendor shall provide the Ministry in conjunction with the training plan, equipment specific information, such as an operating manual for the Telephone System, and a separate operating manual for the Network Management system. These operating manuals shall be provided in both printed and electronic formats. The Vendor shall also outline all the security and risk management features of the Telephone System and Network Management System to be used as part of the training.

The staff training plan, operating manuals, and security and risk management features shall be submitted to the Ministry for approval. The Vendor shall not commence staff training until such time as it receives Ministry written approval of the training.

The Vendor shall provide Ministry personnel with refresher training, on an as required basis, due to system upgrades or as may be directed by the Ministry, so as to ensure effective system management.

There shall be no cost to the Ministry associated with the training or training materials.

A.7 Equipment Servicing, Repairs, and Troubleshooting

The Vendor must have the ability to remotely identify and diagnose problems with the Telephone System and Network Management System. The Vendor shall immediately notify the Ministry upon becoming aware of an issue and take steps to resolve the issue in accordance with the response times below to ensure that any unscheduled repairs, servicing and troubleshooting are meeting the key performance indicators specified in Section A.8. For any scheduled repairs and maintenance, they shall be completed during telephone shut-off time.

The Telephone System and Network Management System shall provide the Ministry with mechanisms to report operational issues, and to allow for the Vendor to conduct and complete repairs in a timely manner. Access to Facilities may require 30 to 60 minutes to clear through security and administrative procedures. In addition, access may be limited due to reasons such as a riot, lockdown, strike or other security events. In such a case, the Vendor shall continue to provide the Deliverables for all Facilities that are not affected by such event, and shall work with the Ministry to reschedule the work for any affected Facilities.

The Vendor shall, on an annual basis, provide a recommended preventative maintenance schedule to the Ministry for approval. The Vendor shall also provide the Ministry, on an annual basis, with a schedule for asset replacements should their replacement be anticipated during the Term of the Agreement. All scheduled Facility visits shall be arranged with the Ministry Representative.

The Vendor shall comply with the following Telephone System service requirements:

- The Vendor shall have technical support staff available from 8:00 a.m. to 5:00 p.m. Eastern Time, seven days a week, for support calls or emails from the Ministry.
- The Vendor shall acknowledge all support calls or emails from the Ministry within one (1) hour.
- The Vendor shall advise the Ministry of all planned system outages and any system changes at least five (5) Business Days in advance for Ministry approval. Note that outages should be planned when inmates are not allowed to use the telephones unless otherwise directed by the Ministry.
- The Vendor shall advise the Ministry of any unplanned system outages and changes that impact the Deliverables within one (1) hour of becoming aware of the issue.

After receipt of a trouble notification from the Ministry, the Vendor shall commence technical repairs, adhering to the following timelines:

- Within two (2) hours of any such notification if:
 - all inmate telephones are affected or where service is interrupted or unavailable at any one Facility; or
 - service at a Ministry central location is interrupted, unavailable, or any other problem affecting any of the telephones.

- Within eight (8) hours of any such notification if the issue affects a minimum of 50% to less than 100% of the inmate telephones at any Facility.

- Within 24 hours of any such notification if the issue affects:
 - less than 50% of the inmate telephones at any Facility; or
 - the conventional public pay telephones at any Facility.

The Vendor shall notify the affected Facilities to coordinate a repair visit within these timelines if the problem cannot be resolved remotely.

All repairs and troubleshooting to restore service must not use or disclose Personal Information.

All costs associated with the repair and replacement of defective or damaged inmate telephones, visitation handsets and conventional public pay telephones, the Telephone System and the Network Management System shall be the responsibility of the Vendor.

The Network Management System must alert the Ministry by e-mail of the opening and closing of all troubleshooting tickets. Each troubleshooting ticket shall clearly document the name of the Facility, the time and nature of the reported problem, the name of the individual reporting the issue, and a concise description of the length of time and repair steps taken leading to a resolution.

A.7.1 Vendor Self-Reporting and Repairs

The Vendor shall immediately notify the Ministry by e-mail of any unreported Telephone System or Network Management System issue that the Vendor identifies while servicing a Facility or from report diagnostics. The Vendor shall log the issue, open a troubleshooting ticket, and continue with the same reporting process for equipment servicing, repairs and troubleshooting.

A.8 Performance Management

The Vendor's performance shall be subject to key performance indicators ("KPIs") in order to enable the Ministry to assess the quality of the Vendor's performance of the Deliverables.

The KPIs and their corresponding targets shall be reported on a monthly basis and are as follows:

Key Performance Indicator	Target
Percentage of time inmate telephone service available, including any planned outages, system changes and circumstances beyond the Vendor's control	99%
Percentage of Conventional Public Pay Telephones in service at any one time.	99%
Average time to restore service to the Ministry for a Ministry wide system outage affecting all inmate telephones	24 hours or less
Average time to restore service at a Facility for a Facility wide outage affecting inmate telephones	48 hours or less
Average time to restore service for an individual inmate telephone outage	72 hours or less
Mean score of voice quality using the mean opinion score evaluation process of the Conversation Opinion Test as documented in Annex A of Recommendation P.800	4.0 or more
Invoice submitted accurately and on time	100%

The Team, as further set out in Section 4.02 of the Agreement, may establish additional KPIs and corresponding targets.

B. Calling Rates

The following Table 2 sets out the calling rates for each type of inmate call required by the Ministry. The rates shall remain fixed throughout the Term of the Agreement, unless amended in accordance with Article 5 – Vendor's Calling Rates.

Table 2 – Call Types and Rates

Types of Calls	Years 1-5 \$ Rate	Optional Year 6 \$ Rate	Optional Year 7 \$ Rate
Local Call Debit Flat Rate - call up to 20 minutes	0.441	0.391	0.391
Local Call Collect Flat Rate - call up to 20 minutes	0.541	0.041	0.041
Canada Wide Debit Call Connection Fee	0.441	0.241	0.241
Canada Wide Debit Call Rate Per Minute	0.031	0.031	0.031
Canada Wide Collect Call Connection Fee	0.000	0.000	0.000
Canada Wide Collect Call Rate Per Minute	0.061	0.061	0.061
United States of America Debit Call Connection Fee	0.000	0.000	0.000
United States of America Debit Call Rate Per Minute	0.061	0.031	0.031
United States of America Collect Call Connection Fee	0.000	0.000	0.000
United States of America Collect Call Rate Per Minute	0.061	0.061	0.061
Americas (Excluding Canada and the US) Debit Call Connection Fee	2.500	2.500	2.500
Americas (Excluding Canada and the US) Debit Call Rate Per Minute	0.021	0.021	0.021
Americas (Excluding Canada and the US) Collect Call Connection Fee	0.000	0.000	0.000
Americas (Excluding Canada and the US) Collect Call Rate Per Minute	0.010	0.010	0.010
Africa and Middle East Call Rates Debit Call Connection Fee	2.500	2.500	2.500
Africa and Middle East Call Rates Debit Call Rate \$ Per Minute	0.010	0.010	0.010
Africa and Middle East Call Rates Collect Call Connection Fee	0.000	0.000	0.000
Africa and Middle East Call Rates Collect Call Rate \$ Per Minute	0.010	0.010	0.010
Asia Debit Call Connection Fee	2.500	2.500	2.500
Asia Debit Call Rate Per Minute	0.010	0.010	0.010
Asia Collect Call Connection Fee	0.000	0.000	0.000
Asia Collect Call Rate Per Minute	0.010	0.010	0.010
Oceania Debit Call Connection Fee	2.500	2.500	2.500
Oceania Debit Call Rate Per Minute	0.021	0.021	0.021
Oceania Collect Call Connection Fee	0.000	0.000	0.000
Oceania Collect Call Rate Per Minute	0.010	0.010	0.010
Europe Debit Call Connection Fee	2.500	2.500	2.500
Europe Debit Call Rate per Minute	0.021	0.021	0.021
Europe Collect Call Connection Fee	0.000	0.000	0.000
Europe Collect Call Rate Per Minute	0.010	0.010	0.010

Attachment # 1

Corporate Policy on Information Sensitivity Classification

Government of Ontario Corporate Policy on Information Sensitivity Classification



Ministry of Government and Consumer Services

Cyber Security Division

Corporate Policy on Information Sensitivity Classification

August 2018

TABLE OF CONTENTS

Table of Contents.....	2
Preamble	3
Authority.....	3
Application and scope.....	4
Principles	4
Mandatory requirements	5
Classifying and Safeguarding Information	5
Information Labelling	6
Assessing and Safeguarding Information Systems	7
Ongoing Risk Management.....	8
Information Owner and Custodian.....	8
Training and Awareness.....	8
Storing, Emailing & Transporting Information	8
Service Delivery Partner Obligations.....	9
Classifying Information from Other Organizations or Jurisdictions	9
Appropriate Recordkeeping Processes to Identify Which Records to Retain, Transfer or Dispose Of	9
Appropriate Disposal of Information	9
Paper Documents.....	9
Roles and responsibilities	10
Users.....	10
Program Owners	10
Cyber Security Division	10
Infrastructure Technology Services.....	11
Information Privacy & Archives (IPA)	11
Glossary.....	12
Contact Information.....	15

PREAMBLE

Effective information security involves addressing the confidentiality, integrity and availability requirements of information and information systems.

- **Confidentiality** requirements relate to the relative harm or injury that would result from unauthorized access or inadvertent release of information. This may be assured through a variety of business processes and technical means.
- **Integrity** requirements relate to the harm or injury that would result if an information asset was compromised by manipulation. This is usually assured via technical means being implemented to prevent unauthorized access to information systems, thereby limiting the possibility of tampering.
- **Availability** requirements relate to the harm or injury that could result if particular information is not available for authorized access and use. This is usually addressed through contingency plans and efforts to ensure the resilience of information systems.

Although all three aspects of information security are important, confidentiality is most likely to be ensured by user behaviour, whereas integrity and availability are most commonly assured through technical means.

It should be noted that the methods and degree of protection recommended to ensure confidentiality will not necessarily be identical to those used to ensure integrity or availability. Similarly, the same information asset may require that different safeguards be implemented to ensure its confidentiality when it is created, stored or shared in different technical contexts (e.g., printed documents; documents stored on an internal application; or documents that are accessible via the Internet).

Nevertheless, the type and degree of safeguard(s) recommended to ensure the security of a given information asset must always be proportionate to the risk of unauthorized access, inadvertent release, manipulation or non-availability.

AUTHORITY

This policy is issued by the Secretary of Treasury Board and Management Board of Cabinet under authority of the Management and Use of Information & Information Technology (I&IT) Directive which delegates the responsibility to establish, amend, replace or rescind policies on the management of I&IT, and also to set out more detailed operational requirements for ministries, I&IT clusters and agencies.

APPLICATION AND SCOPE

This policy applies to:

- Information in all its forms that is created, received, or held by/on behalf of the Government of Ontario: and,
- Information systems and resources that are used by/on behalf of Government of Ontario ministries to create, enter, process, communicate, transport, disseminate, store or dispose of such information.

This policy applies to all provincial ministries, board-governed, non-board governed and advisory agencies, and any other agency defined under the Agencies & Appointments Directive unless an exemption has been granted by Management Board of Cabinet.

These requirements also apply in situations where information is created, entered, processed, transmitted, or stored by third party service delivery partners and their subcontractors.

Appropriate safeguards must be implemented to secure information, information systems and other program resources to a degree that is consistent with the requirements outlined here or as may be outlined in other applicable Ontario Public Service (OPS) policies or laws. Additional safeguards for information systems may also be recommended in a Threat Risk Assessment/Risk Mitigation Plan, Vulnerability Management Report or other documents that identify risks to information security.

PRINCIPLES

The following statements provide the principles on which this policy is based.

- Information and information systems are critical government assets, like physical infrastructure and financial resources, and must be safeguarded deliberately, appropriately and consistently throughout their life cycle.
- Efforts taken to safeguard information must be proportionate to the possible harm or injury that could result if confidentiality, integrity and availability are not assured.
- A thorough analysis of all security risks to information systems may include not only the protection requirements for the information's confidentiality, but also its integrity and availability.
- Reducing risks and managing protection costs are both important considerations when planning, selecting, and implementing safeguards. Accountability for risks rests with the Ministries.
- Mandatory user training is a fundamental component of a successful information sensitivity classification program.

MANDATORY REQUIREMENTS

Classifying and Safeguarding Information

All information must be evaluated, classified and safeguarded in accordance with its sensitivity level. Ratings are to be based on a consideration of the legal obligations and business requirements to protect the confidentiality of the information, as well as the harm and injury that may be caused by the information's unauthorized access, manipulation or inadvertent disclosure.¹ The aggregate value of multiple pieces of information must also be considered when information is stored together. For example, multiple records of Medium Sensitivity information (including personal information) may be reclassified to High Sensitivity, if the information is stored together and the potential for harm or injury increases as a result of the aggregation.

Wherever possible, information of varying classification levels should be segregated and stored with other similarly classified information to avoid under or over-safeguarding. This must be done in a manner that meets the requirements of the Corporate Policy on Recordkeeping. If information of various classifications must co-exist within a system, or in some other context that does not enable adequate technical segregation, all co-existing information must be safeguarded in accordance with the highest classification level identified.

If High Sensitivity information relates to national or provincial interests or national or provincial security, additional safeguards must be implemented. Please follow the federal guidelines for classified assets and information found here: <https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-eng.html>

¹ Personal Information must be classified as Medium Sensitivity at minimum.

Information Labelling

HIGH SENSITIVITY	Unauthorized disclosure could result in loss of life or impact to public safety, significant loss of confidence in or embarrassment to government, extremely serious personal or enterprise injury, major economic impact, sabotage or terrorism, or significant financial loss or social hardship.
MEDIUM SENSITIVITY	Unauthorized disclosure could result in serious personal or enterprise injury, loss of confidence in or embarrassment to government, or a moderate economic impact, sabotage or terrorism, or significant financial loss or social hardship.
LOW SENSITIVITY	Unauthorized disclosure could result in minor injury to persons, minor financial loss, slight embarrassment, or inconvenience.
UNCLASSIFIED	Disclosure will not result in any harm or injury, and does not require prior authorization.

As evidence of having been classified, all information must be labelled with one of the four sensitivity ratings described above. The label applied to a particular piece of information will indicate its confidentiality requirement and will guide the safeguards that must be implemented to ensure that confidentiality can be maintained. Selecting and applying the appropriate label will involve a careful consideration of the harm and injury that could result from the information's unauthorized access or disclosure.

At this time, the OPS does not mandate labelling information to indicate its integrity or availability requirements as these aspects of information security are more commonly achieved through the implementation of safeguards and/or technical measures aimed at protecting information systems.

Assessing and Safeguarding Information Systems

The sensitivity of all information systems must be assessed and a Statement of Sensitivity (SoS) must document the aggregate sensitivity rating of the information and assets involved. The SoS, often prepared as part of a Threat Risk Assessment, will then guide the implementation of safeguards aimed at ensuring the confidentiality, integrity and availability of an information system or systems.

<p>HIGH SENSITIVITY</p>	<p>Unauthorized disclosure, unauthorized modification or loss of availability could result in loss of life or impact to public safety, significant loss of confidence in or embarrassment to government, extremely serious personal or enterprise injury, major economic impact, sabotage or terrorism, or significant financial loss or social hardship.</p>
<p>MEDIUM SENSITIVITY</p>	<p>Unauthorized disclosure, unauthorized modification or loss of availability could result in personal or enterprise injury, loss of competitive advantage, loss of confidence in or embarrassment to government, moderate financial loss, or damage to public trust or reputation.</p>
<p>LOW SENSITIVITY</p>	<p>Unauthorized disclosure, unauthorized modification or loss of availability could result in minor injury to persons, minor financial loss, slight embarrassment, or inconvenience.</p>
<p>UNCLASSIFIED</p>	<p>Disclosure, modification or unavailability will not result in any harm or injury, and disclosure does not require prior authorization.</p>

Information systems with low confidentiality requirements may, nevertheless, have a medium or high requirement for protection of the information's integrity (e.g., websites that host government news releases may not include any personal or sensitive information but must be adequately protected against unauthorized access and/or manipulation). Similarly, systems that support time critical service delivery may have high availability requirements which may translate into requirements for robust protections to ensure their continuous availability, even though they may not contain any personal or highly sensitive information. Although integrity and/or availability are valid information security objectives, efforts to maintain them must not be allowed to undermine or negatively impact efforts to ensure confidentiality.

Ongoing Risk Management

The classification assigned to a particular information asset should be reviewed periodically to ensure that it remains appropriate. Over time, the sensitivity of some information assets may change; assigned classifications should be amended to indicate any change as this may also result in a corresponding change to the measures required to safeguard the information.² If required, information should be re-labelled and the Statement of Sensitivity for information systems should be updated. Similarly, all recommended safeguards should also be reviewed from time to time to ensure that they remain robust and a suitable means of ensuring information security.

Information Owner and Custodian

Information owners must be identified for all information. Information owners are the individuals who create the information, or those who have been delegated formal responsibility for the information. Only the information owner can classify or reclassify sensitive information.

As custodians of personal information, Government of Ontario ministries are also responsible for classifying and protecting the personal information of the people of Ontario. Ministries have an obligation to protect personal information according to the rules of the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPA) which prohibit an institution from disclosing those categories of personal information except under very specific, defined and limited circumstances.

Training and Awareness

The requirements in this policy must be conveyed to all Ontario Public Service employees, as well as to contractors and third-party service delivery partners that ministries may engage to assist them with program delivery. Learning tools will also be provided to help all users meet their obligation to routinely implement these requirements.

Storing, Emailing & Transporting Information

To learn more about how to adequately safeguard all sensitive information, whether in transit or at rest, please see the Information Sensitivity Classification Guidelines.

When in digital format, high sensitivity information must be encrypted in storage and transit, including via email, using only approved encryption methods (see GO-ITS 25.12 Security Requirements for the Use of Cryptography for details).

² For example, before a news release about a major government announcement is made, the information involved may be considered high sensitivity. However, upon its release to the public, the same information would then be re-labelled as unclassified.

If high sensitivity information must be stored or transported on mobile computing or digital storage devices (including laptops, USBs and portable hard drives) the information must be encrypted and its handling must comply with all requirements outlined in GO-ITS 25.10 Security Requirements for Mobile Devices.

Service Delivery Partner Obligations

Contracts and service level agreements with third party service providers who have access to – or share custody of OPS information and/or information systems – must include the obligation to follow the requirements of this policy and its corresponding guidelines. This requirement must extend to any sub-contractors on whom the service providers rely to deliver services to the Ontario Government or to citizens.

Classifying Information from Other Organizations or Jurisdictions

All information received from other program areas, Ministries, organizations or jurisdictions must be safeguarded according to the classification it bears. If a different classification scheme has been used, the recipient of the information should clarify the handling requirements with the information owner or originating jurisdiction.

If information received from other organizations or jurisdictions does not bear a sensitivity classification, it must be classified and labelled in accordance with this policy and safeguarded accordingly while it is in the custody and control of the OPS.

Appropriate Recordkeeping Processes to Identify What Records to Retain, Transfer or Dispose Of

The Archives and Recordkeeping Act, 2006 states that the retention, transfer and disposition of records in any format is governed by a records schedule approved by the Archivist of Ontario. The records schedule determines how long records must be retained in the ministry, and their final disposition (i.e. transfer to the Archives of Ontario, or destroy). If transferring archival digital records, please refer to the Guideline for Transferring Archival Digital Records to the Archives.

Appropriate Disposal of Information

Paper Documents

All sensitive paper documents must be placed in the secure disposal containers provided by the Secure Document Destruction Vendor of Record. Paper documents labelled as Unclassified may be recycled.

Information on Computerized Devices & Digital Storage Media

Information on computerized devices and digital storage media must be made inaccessible using the sanitization process and hardware destruction procedures approved for use in the OPS. Please refer to the GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media and the corresponding Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media Guidelines.

ROLES AND RESPONSIBILITIES

Users

All users of information and information systems in the custody and/or under the control of the Government of Ontario must,

- Classify and safeguard information in accordance with the requirements of this policy and the associated guidelines;
- Label all information or documents they create according to the four sensitivity levels defined in this policy and its corresponding guidelines;
- Recognize the sensitivity ratings assigned to information assets created by others and safeguard those assets accordingly;
- Review Information Sensitivity Classification learning materials/courses;
- Comply with government legislation, directives, policies, operating procedures and standards when using I&IT resources.
- Report any actual or suspected information security or privacy breaches to their manager in a timely manner and notify the OPS IT Service Desk of any suspected security breach.

Program Owners

All Program Owners must,

- Ensure that all users in their program area are made aware of this policy and its corresponding guidelines;
- Complete the Information Sensitivity Classification training and oversee its completion by all direct reports;
- Ensure that all staff in their program area understand the importance of classifying, labelling and safeguarding sensitive information;
- Identify the sensitivity classification level of all program-related information and information systems and take steps to secure them accordingly;
- Ensure that the aggregate sensitivity of all record series developed for or used by their program area is documented, and that records are managed accordingly;
- Where appropriate, ensure that a Statement of Sensitivity exists for all information systems under their control;
- Respond to any reports of an information security or privacy breach.

Cyber Security Division

Cyber Security Division must,

- Maintain this policy and the corresponding guidelines;
- Provide policy interpretation and guidance as required;
- Provide tools to raise awareness about these requirements and help all users meet their obligations to implement them;

- Provide information security risk assessment services including Asset Classification Reports, Statements of Sensitivity, Threat Risk Assessments, Vulnerability Assessment/Penetration Tests, etc., as may be required to assist ministries in the implementation of this policy;
- Work with Infrastructure Technology Services, IT Clusters and relevant program managers to investigate information security breaches; and
- Work with OPS partners to ensure that appropriate security tools and services (e.g. data and email encryption, system logging, intrusion detection/prevention systems) as well as hosting and storage environments are made available to enable the appropriate safeguarding of information and information systems of all sensitivity levels.

Chief Information Officers, I&IT Clusters

- Design and build I&IT systems that address the information sensitivity classification as identified by the Program Manager, and that take into consideration the statement of sensitivity, the results of any security and/or privacy assessments and the requirements of other applicable corporate policies;
- Ensure that they and their Cluster staff operate I&IT systems in a manner that meets business requirements and is consistent with information sensitivity classifications;
- Provide, or assist with, electronic and paper-based information and document management practices as appropriate.

Infrastructure Technology Services

- Work with Cyber Security Division to ensure that appropriate security tools and services (e.g. data and email encryption, system logging, intrusion detection/prevention systems) as well as hosting and storage environments are made available to enable the appropriate safeguarding of information and information systems of all sensitivity levels.
- Work with Cyber Security Division, IT Clusters and relevant program managers to investigate information security breaches.

Information Privacy & Archives (IPA)

- Work with Cyber Security Division to ensure legislative requirements under the Freedom of Information and Protection of Privacy Act (FIPPA) and the Archives and Recordkeeping Act (ARA) are addressed in Cyber Security policies, standards and procedures.

GLOSSARY

“availability” – present and ready for authorized use.

“confidentiality” – the condition of, or the requirement for, privacy or secrecy.

“control” – not in the physical possession of information, but with a legal/contractual right or responsibility to deal with it.

“custody” – In the physical possession of the information (excluding unsolicited or accidental possession).

“digital signature” – a mathematical scheme for demonstrating the authenticity of a digital message or document, identifying the sender and proving that the message was not altered in transit.

“disclosure” – any exposure to recorded information, whether deliberate or accidental, authorized or unauthorized and includes the ability to read only, or to read and also manipulate the information.

“disposal” – the act or process of getting rid of something that is no longer required and does not need to be retained.

“disposition” – the final action taken with a record when its retention period is over

“enterprise” – an entire organization or business; may be used to refer to the Ontario government, Ontario Public Service, or a private business.

“extremely serious personal or enterprise injury” – catastrophic physical harm or even death, or ruinous financial injury, or permanent loss of reputation to an individual, the Government of Ontario, or a third party company or organization that does business with the government.

“harm” – the physical, mental or emotional damage to an individual or an organization’s reputation, assets, or the ability to serve clients that could result from a business injury.

“information” – recorded information in any form, in any medium, and at all stages of its life cycle including information created, recorded, transmitted or stored in digital form or in other intangible forms by electronic, magnetic, optical or any other means, but does not include a mechanism or system for creating, sending, receiving, storing or otherwise processing information.

“information asset” – a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognizable and manageable value, risk, content and lifecycles; e.g., a database of contacts, all the files associated with a specific project, or all the financial data for an organization.

“information custodian” – a person in whom trust is given for the safe-keeping of classified information. The person responsible for securing the information according to its sensitivity classification.

“information owner” – a person who created the information or is delegated formal responsibility for the information.

“information system” – any system or technology resource that is used by/on behalf of the Ontario Government ministries to create, enter, process, communicate, send/receive, publish/disseminate, store or dispose of information.

“injury” – a security incident or breach (e.g., unauthorized disclosure) that causes harm.

“integrity” – the condition of or requirement for assurances that information that has not been modified or deleted in an unauthorized or undetectable manner.

“ministry” – a ministry of the Government of Ontario and includes all information and information technology clusters and associated agencies.

“personal health information” – means identifying information about an individual in oral or recorded form, if the information,

- a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family,
- b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- c) is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual,
- d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
- e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- f) is the individual’s health number, or
- g) identifies an individual’s substitute decision-maker.

“personal information” – recorded information about an identifiable individual as described in the *Freedom of Information and Protection of Privacy Act*.

“privacy impact assessment” – is both a due diligence exercise and risk management tool. It is a proactive approach designed to help protect privacy by identifying and analyzing privacy-related risks early enough to be able to take appropriate action; avoiding, eliminating or minimizing negative impacts on privacy; and complying with relevant privacy legislation and assessing broader privacy implications.

“program owner” – means any program director or equivalent having authority and accountability under legislation, regulation, policy or other instrument for particular business activities and for the business records relating to those activities.

“record” - information in context, however recorded, whether in printed form, on film, by electronic means or otherwise, including:

- (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material, regardless of physical form or characteristics and any copy thereof;
- (b) any record that is capable of being produced from a machine-readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution ("document").³

"record schedule" – An Archivist of Ontario-approved document that identifies and describes the records made and received by public bodies and sets out retention periods and final dispositions for those records, the format in which the records are to be kept and which records. Records schedules consist of records series (Page 11, Corporate Policy on Recordkeeping, 2015).

"risk" – a measure of the extent to which an entity is threatened by a potential circumstance or event – typically calculated by a consideration of the adverse impacts that would arise if a circumstance/event occurs, as well as the likelihood of it occurring.

"safeguard" – a protective and precautionary measure intended to prevent a threat agent from causing harm and injury.

"sensitive information" – information, that if released without authorization, would cause harm (personal or enterprise injury, embarrassment, unfair economic advantage, etc.).

"statement of sensitivity" – an analysis of information or information system which defines the sensitivity of the information within the system and the importance of the supporting services of the system. A statement of sensitivity may also define the sensitivity requirements of supporting assets (that is, hardware and software, interfaces, personnel, supporting systems and utilities, and access control measures). A statement of sensitivity is an important component of a Threat/Risk Assessment.

"Threat/Risk Assessment" – a formalized process to determine the risks to information and information systems. Based on the sensitivity of all information and associated assets, the TRA will assess the appropriateness of the safeguards currently in place to protect the information's confidentiality, integrity, and availability. It will also offer recommendations about additional measures to mitigate risk or to increase the efficiency and effectiveness of existing safeguards, as required.

"unauthorized" – without the permission of the accountable program manager or his/her delegate.

"unclassified" – information that if accessed without authorization will cause no harm or injury.

"unauthorized disclosure" – any unapproved exposure to recorded information, whether deliberate or accidental, and includes the ability to just read, or also to read and edit the information.

³ As per the *Freedom of Information and Protection of Privacy Act*, 1990

“user” – anyone authorized to access information in the custody or under the control of the Government of Ontario.

CONTACT INFORMATION

Contact	Alex Fanourgiakis Manager, Cyber Security Policy and Standards, Cyber Security Division, Ministry Government and Consumer Services Alex.Fanourgiakis@Ontario.ca 647-776-1167
Writer	Sylvia Nikodem Security Policy Advisor, Cyber Security Policy and Standards, Cyber Security Division, Ministry Government and Consumer Services Sylvia.Nikodem@Ontario.ca 416-327-2502
Effective Date	August 28, 2018

VANESSA FAREAU, et al.
Plaintiffs

-and-

BELL CANADA, et al.
Defendants

Court File No.: CV-20-00635778-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE
Proceeding commenced at TORONTO

Proceeding under the *Class Proceeding Act, 1992*

SUPPLEMENTARY AFFIDAVIT
OF NADINE BLUM
(Affirmed May 13, 2021)

SOTOS LLP

180 Dundas Street West, Suite 1200
Toronto, ON M5G 1Z8

David Sterns (LS#36274J)

Mohsen Seddigh (LS#707441)

Tassia K. Poynter (LS#70722F)

GOLDBLATT PARTNERS LLP

20 Dundas Street West, Suite 1039
Toronto, ON M5G 2C2

Kirsten L. Mercer (LS#54077J)

Jody Brown (LS#58844D)

Lawyers for the Plaintiffs