SCHEDULE R

SECURITY REQUIREMENTS

1. The Security Obligations

In accordance with the Agreement, and at all times during the Full Term, TELUS will comply with the security requirements set out in this Schedule R (including its attachments), in the GPS Group Security Policies (subject to Section 5 of this Schedule), and in Section 19 of the main body of this Agreement, and any additional security requirements related to the Services or the Network which may be agreed to between TELUS and the GPS Group (the "**Security Obligations**").

2. [Intentionally Deleted]

3. Security of Information

TELUS acknowledges that the Services, the Network and any infrastructure owned or leased by TELUS or any GPS Entity and used to provide the Services, will carry governmental information transmissions, including GPS Confidential Information and Personal Information, and as such, the security, including the availability, integrity, confidentiality and privacy, of the information is of paramount importance to the GPS Group.

4. Adherence to GPS Group Security Standards

(a) At all times during the Full Term, without limiting the obligation of TELUS to comply with other Policies or Security Obligations, and subject to the exemptions set out in Section 5 of this Schedule, TELUS shall meet or exceed the security policies, guidelines and practice of the GPS Entities as outlined and implemented in the documents listed below in this Section 4 (the "**GPS Group Security Policies**") at no additional cost or expense to the GPS Entities:

(i) Chapter 12 - IM/IT, Core Policy and Procedures Manual, which can be found at http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm;

(ii) Chapter 12 - IM/IT, Core Policy and Procedures Manual Supplemental Manual 2007, which can be downloaded from http://www.cio.gov.bc.ca/local/cio/about/documents/cpm12.pdf

(iii) Chapter 14 – Risk Management, Core Policy and Procedures Manual, which can be found at http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/14_Risk_Mgmt.htm;

(iv) Chapter 15 – Security, Core Policy and Procedures Manual, which can be found at http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/15_Security.htm;

(v) Chapter 16 – Business Continuity Management, Core Policy and Procedures Manual, which can be found at

http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/16_Business_Continuity_Mgmt.htm;

(vi) Chapter 17 – Internal Audit, Core Policy and Procedures Manual, which can be found at http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/17_Internal_Audit.htm;

(vii) Information Security Policy Manual Ver. 2.0 - October 2010, which can be downloaded from http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf OR at http://www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page;

(viii) Recorded Information Management Manual which can be found at http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/index.html;

(ix) IM/IT Architecture and Standards which can be found at http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf OR at http://www.cio.gov.bc.ca/cio/standards/standards_manual.page;

(x) Risk Management Branch's Security Standards Guidelines;

(xi) The Province's IT Asset Disposal Standard by ensuring that the TELUS' policy and procedures for IT asset disposal meet or exceed such standard (notwithstanding that such standard only applies to provincially owned assets) and any other standards for the disposal of the assets of a GPS Entity that relate to Services and are set out in Policies and applicable Standards referred to herein;

(xii) The Province's Physical Security Technical Standard for Secure Zones – Ministry Shared Rooms and Physical Security Technical Standard for Secure Zones – WTS Network Centre by ensuring that TELUS' physical security standards meet or exceed such standard (notwithstanding that such standard is geared toward government operations) and any other similar physical security standards of a GPS Entity that relate to Services and are set out in Policies and applicable Standards referred to herein; and

(xiii) Information Incident Management Process which can be found at: http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf or at http://www.cio.gov.bc.ca/cio/information_incident/index.page.

(b) The GPS Group Security Policies may be amended from time to time at the sole discretion of the GPS Entities. Subject to the Change Process, TELUS will implement all additional security obligations resulting from any such amendments that are applicable to the Services and the Network and all any other additional security requirements requested from time to time by the GPS Group. Notwithstanding the Change Process, if amendments to the GPS Group Security

Policies as required by the GPS Entities are a reflection of the evolution of technology and security practices in the telecommunications industry during the Full Term, and such changes will be implemented by TELUS as part of the natural evolution and maintenance of the currency of the Available Services, then the financial costs of such changes will be assumed by TELUS, provided that TELUS is able to make such amendments in accordance with TELUS own security policies and timelines, acting reasonably.

5. GPS Group Security Policies Exemptions

(a) Without limiting the obligations of TELUS to comply in all other respects with the GPS Security Policies, other Policies, and the Security Obligations, the GPS Group hereby grants TELUS a limited exemption from compliance with the GPS Security Policies with respect to the following specific matters as described herein:

(i) Access Control: Policy requires the password to be changed on privileged accounts every 90 days (3 months). The GPS Group grants to TELUS an exemption to the foregoing Policy requirement to allow TELUS to change passwords every 180 days (6 months).

(ii) Access Control: Policy specifies a minimum 15 character password for privileged accounts. The GPS Group grants to TELUS an exemption to the foregoing Policy requirement for systems where the maximum password length supported is less than 15 characters. In these cases, the maximum number of characters the system supports must be used.

(iii) Account Lockout: Policy specifies a maximum 3 incorrect password attempts before invoking a minimum 15 minute account lockout. The GPS Group grants to TELUS an exemption to the foregoing Policy requirement to allow for a maximum 5 unsuccessful password attempts.

(iv) Operating hours: Policy requires restricting access hours to high value applications. The GPS Group grants to TELUS an exemption to the foregoing Policy requirement to allow provision of support without restriction.

(v) Media Handling: Policy requires all removable media to be managed to prevent unauthorized disclosure of information contained on the device. The GPS Group grants to TELUS an exemption to the foregoing Policy requirement to allow TELUS to use USB portable memory devices that are not centrally managed. The device will remain under the management of the individual TELUS staff until final disposal in a secure manner (via erasure or destruction).

(vi) Physical Access: Policy specifies colour coding access identity badges to distinguish between staff and guests. The GPS Group grants to TELUS an exemption to the foregoing Policy requirement to permit non-colour coded badges on TELUS premises. TELUS will have sufficient access controls in place to ensure all guests are identified and escorted while on TELUS premises.

6. Service Specific Security Requirements

(a) TELUS shall, in addition to the general security requirements set out in this Schedule R, comply with the service-specific security-related terms, conditions and requirements set out in the following Attachments, which are incorporated by reference into this Schedule R and shall form part of the Security Obligations:

(i) Attachment R1 – Long Distance Services Specific Security Requirements;

(ii) Attachment R2 – Conferencing Services Specific Security Requirements;

(iii) Attachment R3 – Voice Services Specific Security Requirements;

(iv) Attachment R3-IVR – Hosted IVR Services Specific Security Requirements;

(v) Attachment R5 - Data Services Specific Security Requirements; and

(vi) Attachment R9 - Cellular Services Specific Security Requirements.

7. TELUS Group Compliance

At all times during the Full Term, TELUS shall cause the TELUS Group to comply with the Security Obligations, including the GPS Group Security Policies. The foregoing obligation shall be subject to the following limited exceptions:

(a) Where a Subcontractor undertakes Work in respect of the Services, and that Subcontractor and its employees and other representatives have no access to, or ability to access, at any time during the Full Term: (i) the Network, (ii) any GPS Confidential Information, (iii) any GPS Group Intellectual Property; (iv) any Personal Information applicable to the GPS Entities; or (v) any records, information, data, network traffic, facilities, Systems, Hardware, Software or internal networks of the GPS Entities, then TELUS shall have no obligation to cause the Subcontractor to comply with the Security Obligations; or

(b) Upon a written request from TELUS to the Administrator during the Full Term, the GPS Entities may, at their sole discretion and on such terms and conditions as they deem appropriate, grant an exemption to TELUS in respect of the applicability of some or all of the GPS Group Security Policies to an individual Subcontractor. Any such exemption must be granted in writing and must be signed by the Administrator.

8. Security Communication and Compliance Monitoring

(a) At all times during the Full Term, TELUS will follow and monitor for compliance, all of the Security Obligations. If for any reason TELUS or the TELUS Group does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule R in any respect, TELUS must promptly notify the GPS Entities of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

9. Security Clearances

(a) TELUS will ensure that all members of the TELUS Group who are involved in any way in providing the Services, either directly or indirectly, who require access to information associated with the provision of the Services or access to facilities (including Sites) used to provide the Services to the GPS Group, shall comply with the security screening criteria and procedures as a condition of employment or as a condition of being retained by TELUS in sections 26 and 27 of this Schedule.

(b) The TELUS Group will have procedures in place during the Full Term to immediately revoke access to any member of the TELUS Group whose employment is terminated, or who ceases to be a member of the TELUS Group, or who is determined by TELUS or any GPS Entity, acting reasonably, to be a security concern.

10. Network and GPS Infrastructure Access

(a) TELUS will ensure that access to any infrastructure owned or leased by any GPS Entity used in respect of the Services will be limited only to members of the TELUS Group authorized under this Agreement.

(b) TELUS will ensure that management, maintenance and administrative access to the Network, whether physical or electronic, will be limited only to members of the TELUS Group authorized under this Agreement.

(c) Any part of the Network (including processing platforms or telecommunications facilities) that is shared with other customers of the TELUS Group will be partitioned in such a way to allow only members of the TELUS Group authorized under this Agreement to have the ability to access information of the GPS Group.

11. GPS Group Information Access

(a) Except as expressly permitted pursuant to the Agreement, TELUS will not, nor will TELUS authorize or permit any member of the TELUS Group or any third parties to access any information of the GPS Group without the express written approval of the GPS Group.

(b) TELUS will make arrangements consistent with the highest industry standards to maintain the security of information of the GPS Group, and to protect the information of the GPS Group against such risks as unauthorized access, collection, use, duplication, modification, disclosure or disposal.

(c) TELUS will ensure that security measures and security management practices are implemented to ensure the security, confidentiality, integrity and availability of all GPS Entity information, including GPS Confidential Information and Personal Information, while being transmitted through the Network. To the extent that any GPS Entity information is required to be in the custody of, accessed by or stored by TELUS in accordance with the terms of this Agreement, then TELUS will further ensure that security measures and security management practices are

implemented to ensure the security, confidentiality, integrity and availability of that information while in the custody of, accessed by or stored by TELUS.

(d) TELUS shall not take any action or fail to take any action that in either case results in TELUS or the TELUS Group intercepting, obtaining or otherwise gaining access to any Personal Information of a GPS Entity, or GPS End User, except as set out in section 24.1.2(a) of the main body of this Agreement.

12. Physical Access

TELUS will comply with the GPS Entities' 'secure zone' standards, including ensuring that equipment and telecommunications facilities used to provide the Services or the Network to the GPS Group are secured by electronic card access system, combination lock, or lock and key or equivalents. TELUS will maintain logs of all accesses to any of its Sites including its network centres used to provide the Services.

13. Monitoring

(a) At all times, TELUS shall comply with Industry Standards (including those relating to goods, technology, services, and management practices) to prevent, mitigate, detect, protect against and otherwise secure the Services from any harm, damage, sabotage, hacking, virus, interference, interception, unauthorized access, corruption, or fraudulent use by any person or otherwise permit any such activities. Subject to section 24.1.2 of the main body of this Agreement with respect to Personal Information and except as expressly permitted herein to the extent required to provide the Services, TELUS must not, except as compelled, authorized or permitted by Applicable Law or as otherwise expressly provided herein or authorized in writing by a GPS Entity in respect of the Services provided to such GPS Entity, conduct or otherwise engage in any act or omission intended or designated to hack, tap, divert, eavesdrop, interfere with, intercept, record, manipulate, copy, store or otherwise monitor a GPS Entity's communications or transmissions or those of any of its GPS End Users, including the acts of: (i) capturing or decoding communications packets; or (ii) intercepting, tapping, monitoring, scanning for key words, viewing, recording or listening to voice conversations or other communications.

(b) TELUS shall advise the GPS Entity of any suspected fraudulent, illegal or other use of the Services that breach this Agreement as soon as possible after becoming aware of any such use and shall take all reasonable steps to prevent such actions or events from continuing or reoccurring, including co-operating with the GPS Entity. TELUS confirms that it maintains Network security procedures and that the Network incorporates security features consistent with the procedures and network features employed by the leading telecommunications providers in Canada.

(c) Except as otherwise permitted pursuant to this Agreement, TELUS will restrict monitoring of data and voice traffic transited using the Services and the Network to authorized and security screened Personnel and External Personnel performing Network maintenance activities, and ensure that any information accessed is not stored, used or disclosed to third parties other than as may be expressly permitted under this Agreement. TELUS shall also have policies in

place that prohibit the use or disclosure of any sensitive monitored information by TELUS that are consistent with the GPS Group Security Policies.

(d) TELUS will assist and cooperate with GPS Entities' Designated Security Prime or Security Authorised Representative, and if requested, will provide monitoring required for security-related investigations.

(e) TELUS will monitor the Network access and usage to identify any anomalies or irregularities in order to identify potential irregular, fraudulent, malicious or unauthorized activity and, where such activities are identified, will immediately notify the GPS Entities. Notwithstanding the foregoing, in circumstances where a brief period of time is necessary to identify if indeed there has been irregular, fraudulent, malicious or unauthorized activity, or just a false positive alert from a monitoring system, TELUS may delay immediate notification, but only for such time as is reasonably necessary to complete such identification.

14. Security Records and Reporting

TELUS agrees that:

(a) the Administrator and each applicable GPS Entity (through the Designated Security Prime of each GPS Entity) will be given immediate notification by TELUS of any actual or suspected security breaches or violations relating to the Services, or in respect of the Network, upon TELUS becoming aware of the same;

(b) subject to Applicable Laws, TELUS will grant a GPS Entity access to any security records and monitoring logs relating to the Services or the Network to enable investigations of security incidents by that GPS Entity; and

(c) such security records are subject to Sections 19.2, 22 and 24 of the main body of this Agreement and Schedule Q.

15. Court Orders or other Lawful Requirements

(a) TELUS will provide the applicable GPS Entity with immediate notice of any court order or other lawful requirement that TELUS receives for monitoring of the Services or Network in order that the GPS Entity may seek judicial relief.

(b) Where the applicable GPS Entity obtains such judicial relief and provides a copy of the judicial order to TELUS, TELUS will immediately comply with the judicial order including, without limitation, refraining from monitoring the Services or Network or releasing recorded information as required or applicable.

16. Security Investigations

(a) Where TELUS becomes aware of any:

(i) unauthorized access, collection, use, disclosure, alteration or disposal of records or information of the GPS Entities; or

(ii) unauthorized access to facilities or equipment relating to the Services or Network which has occurred or is likely to occur (whether or not related to a failure by TELUS to comply with this Schedule or this Agreement); or

(iii) compromises or breaches relating to the Services, Network and all equipment, devices, systems, or infrastructure used by TELUS, or its Personnel, agents and Subcontractors to provide the Services,

then TELUS shall:

(iv) immediately notify the applicable Designated Security Prime of the affected GPS Entity of the particulars of that occurrence or likely occurrence;

(v) if TELUS provides such a notification other than in writing, that notification must be confirmed in writing to the GPS Entity as soon as it is reasonably possible for TELUS to do so;

(vi) in circumstances where a brief period of time is necessary to identify if indeed there is a breach or compromise, perceived or actual, or just a false positive alert from a monitoring system, TELUS may delay immediate notification, but only for such time as is reasonably necessary to complete such identification;

(vii) TELUS will investigate all compromises or breaches relating to the Services or the Network and all equipment, devices, systems, or infrastructure used while providing the Services or the Network, and will provide a report of the investigation to the GPS Entities affected as soon as it is reasonably possible to do so after the completion of the investigation, but no later than thirty (30) days after the completion of the investigation. If the investigation takes more than thirty (30) days to complete, TELUS will provide an interim report as soon as it is reasonably possible to do so, but no later than thirty (30) days after the occurrence of the compromise or breach, and every thirty (30) days after that, until the investigation is completed.

(b) The GPS Entities reserve the right to conduct their own internal security investigations or reviews. If a GPS Entity decides to conduct a review or security investigation of a matter described in this section 16 (whether or not the matter came to the attention of the GPS Entity as a result of a notification by TELUS under this Agreement), TELUS shall, on the request of the GPS Entity, participate in and cooperate with the review. In particular:

(i) TELUS shall use reasonable commercial efforts to support and assist any GPS Entity conducting a security investigation and shall at no time take any steps to prevent or hinder any such investigation;

(ii) TELUS shall provide a single, direct point of contact that may be used by any GPS Entity conducting a security investigation;

(iii) Subject to Applicable Laws, TELUS shall grant the applicable GPS Entity access to any of its monitoring and logging information related to the Services or Network for the purposes of either court-ordered or security investigations conducted by the applicable GPS Entity. At the request of the applicable GPS Entity, TELUS shall provide the monitoring and logging information as soon as possible, but no later than forty-eight (48) hours after a request, unless TELUS can clearly demonstrate that it cannot provide the logs within 48 hours due to operational issues or technology limitations, in which case the logs will be provided as soon as technically feasible. In cases where a GPS Entity security investigation is related to threat to life or limb, and where the GPS Entity notifies the TELUS Customer Service Manager (CSM), TELUS shall take immediate action and provide the logs as soon as possible;

(iv) if TELUS is conducting an investigation and is the primary holder of the chain of custody processes, TELUS shall provide copies of the monitoring and logging data;

(v) TELUS shall ensure that it maintains adequate chain of custody processes and procedures for the security investigations monitored and logged information provided in respect of the Services; and

(vi) TELUS acknowledges that the GPS Entities may have processes in place to identify, investigate and take action against inappropriate use of the Services, Network, systems, devices or infrastructure and will provide reasonable assistance to the GPS Entities in respect of such processes and, without limitation, any investigations of suspicious events.

17. Incident Response

(a) TELUS will work collaboratively with the GPS Entities to assist with GPS Entity requests for changes and emergency changes needed to mitigate any security breaches and incidents relating to the Network or the Services in accordance with Schedules N and RR.

(b) TELUS shall immediately investigate and report any security-related Incident to the GPS Entities in accordance with Schedule N.

(c) TELUS shall provide a direct point of contact that may be used by GPS Entities for security Incident response activities.

18. Security Threat And Risk Assessments

(a) TELUS shall demonstrate sound risk management practices by performing comprehensive security threat and risk assessments ("**STRA**") to demonstrate that risks have been identified and are being managed adequately:

(i) after the Effective Date as follows:

A. 1 STRA for Data Services (other than Internet Services but including Local, WAN, Fully Managed type Services);

B. 1 STRA for Internet Services (but can be linked to WAN type Services);

C. 1 STRA for Voice Services (other than Hosted IVR Services);

D. 1 STRA for Hosted IVR Services;

E. 1 STRA for Cellular Services;

F. 1 STRA for Audio Conferencing Services;

G. 1 STRA for Web Conferencing Services; and

H. 1 STRA for Long Distance Services; and

(ii) before implementation of any new Service added to this Agreement to demonstrate that risks have been identified and are being managed adequately.

(b) STRAs will be conducted in accordance with the GPS Security Policies. The GPS Group will provide TELUS with details about the STRA methodology that it uses or designates and will notify TELUS of any changes or updates to its STRA methodology.

(c) If TELUS uses a different STRA or audit methodology than the methodology used by the GPS Group, TELUS will, at no additional charge:

(i) provide the results of the STRA in an agreed upon format; and

(ii) transpose/translate the results of the STRA into the specific STRA methodology that the GPS Group uses or designates.

Additional STRA methodology translations besides the one STRA methodology designated by the GPS Group are chargeable based on time and materials rates set out in the Price Book.

(d) Any STRA performed by TELUS in respect of Services or the Network will include the assessment of risk introduced by any supporting infrastructure or systems utilized by TELUS to access, operate, maintain or manage the Services or the Network provided, as well as the associated security management practices.

(e) Any STRA performed by TELUS in respect of Services or the Network will be conducted during the planning and design phase of any new information systems, services or infrastructure, and before the initiation of Services, as applicable to the scope of the Services and infrastructure, including the Network, provided by TELUS under this Agreement.

(f) As applicable to the scope of the Services and the Network, provided by TELUS under this Agreement, STRA will be conducted for significant changes to information systems, Services or infrastructure provided (e.g. changes in

architecture, new operating system versions, major service pack updates, and changes to the type of security controls, devices or software used). STRAs for significant changes will be performed during the planning and design phase of such proposed changes and before the implementation of such changes.

(g) The results of the STRAs conducted by TELUS will be submitted to the GPS Entities for review. The GPS Group will complete the review of the STRA results, and communicate the results to TELUS no later than thirty (30) days after TELUS' submission.

(h) Deficiencies that are identified with regard to meeting compliance with the Security Obligations as set out in this schedule, will be the responsibility of TELUS for remediation in a reasonable time frame. If deficiencies identified are in addition to meeting Security Obligations, or are in regard to a specific implementation requirement from the GPS Group, then these will be remediated and addressed through joint discussion and agreement between TELUS and the GPS Group and it will be handled by the dispute resolution process described in the section 28 of the main body of this Agreement.

19. Compliance

(a) TELUS shall, during each year of the Full Term and at no additional cost, comply with the GPS Entities' annual compliance assessment process to measure compliance with the GPS Group Security Policies (the "**Annual Compliance Assessment**"). The Annual Compliance Assessment process includes the following requirements:

(i) The current Annual Compliance Assessment methodology used by the GPS Group is the iSMART Annual Compliance Assessment Questionnaire.

(ii) Every Calendar Year during the Full Term, TELUS will complete the Annual Compliance Assessment covering the Services and Network and using the then-current GPS Group methodology and will provide the results of such annual compliance check to the GPS Group no later than February 1st of the following year.

(iii) The scope of the Annual Compliance Assessment covers all services, systems and infrastructure provided by TELUS to the GPS Entities under the Agreement.

(iv) The Annual Compliance Assessment will be completed separately for each of the Service Towers, unless agreed otherwise between the parties.

(v) The Annual Compliance Assessment methodology of the GPS Group is subject to periodic reviews and change at the sole discretion of the GPS Group. No later than November 31st of every year during the Full Term, the GPS Group will communicate to TELUS the Annual Compliance Assessment methodology for the following calendar year and the

designated procedure for completion/submission of reports as defined by the GPS Group.

(b) A GPS Entity may require TELUS to periodically assess its compliance with the Security Obligations and the Privacy Obligations and provide a report of same signed by a senior TELUS executive. Additional compliance assessments beyond the Annual Compliance Assessment will be scoped as a billable Project at the professional services rates set out in the Price Book.

20. Network & Administrative Security

(a) At all times during the Full Term, TELUS shall ensure that it has the ability to revoke immediately the access of any member of the TELUS Group to the Network, the GPS Confidential Information, the Personal Information and the GPS Entities' devices, systems or internal networks.

(b) TELUS shall strictly limit access to the Network, or related devices, systems or infrastructure (including any processing platforms or telecommunications facilities used to provide the Services), to members of the TELUS Group authorized to provide the Services under this Agreement and only in cases where such access is required in order to provide the Services.

(c) TELUS shall ensure that any part of the Network, or related devices, systems or infrastructure (including any processing platforms or telecommunications facilities used to provide the Services), that are shared with other TELUS customers are partitioned in such a way to ensure that the information of each GPS Entity is isolated and secure at all times. In particular:

(i) only authorized members of the TELUS Group shall be able to access GPS Entity information in accordance with the terms of this Agreement;

(ii) GPS Entity data and traffic shall be logically isolated on the network at all times from other data and traffic of other customers or GPS Entities; and

(iii) TELUS will maintain vulnerability management practices, including proactive monitoring of vendor alert services to and ensure the Network will be updated with patches, update releases or new versions of software in a timely manner and in line with TELUS' security standards in this area. TELUS shall maintain a secure Network that mitigates all known vulnerabilities in a transparent fashion.

(d) To ensure proper protection for the GPS Confidential Information and the Personal Information, TELUS shall, at a minimum, implement the following measures:

(i) ensure that an audit trail is created when any Personal Information or GPS Confidential Information is accessed in connection with this Agreement; and

(ii) restrict remote access to the Network and TELUS Equipment to authorized members of the TELUS Group only.

21. Facility Security

(a) TELUS shall ensure that, except for TELUS Equipment that is stored at the premises of a GPS Entity and except as otherwise authorized in writing by the GPS Group, all of the TELUS Equipment and similar equipment utilized by any Subcontractors in providing the Services shall be located at a secured location that:

(i) has security measures to the highest industry standards;

(ii) has appropriate physical and environmental security controls;

(iii) ensures physical access to such locations is limited to authorized Personnel only; and

(iv) equipment and telecommunications facilities used to provide the Services are at a minimum secured by electronic card access system, combination lock, or lock and key or equivalent.

(b) TELUS shall create, maintain and follow a documented process to:

(i) protect the Network from loss, damage or any other occurrence that may result in any of portions of the Network being unavailable when required to provide the Services; and

(ii) limit access to any portion of the Network that may be used by someone to access GPS Entity information, including GPS Confidential Information, solely to those persons who are authorized under this Agreement to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons.

(c) If any GPS Entity makes available to TELUS any facilities or equipment of the GPS Entity for the use of TELUS or the TELUS Group in providing the Services, Subject to the Change Process, TELUS will comply with any Policies of such GPS Entity on acceptable use, protection of, and access to, such facilities or equipment.

22. Integrity Of Information

TELUS shall create, maintain and follow a documented process for maintaining the integrity of GPS Entity information, including GPS Confidential Information, while possessed or accessed by TELUS. In particular, TELUS shall ensure that all such information shall remain as complete as when it was acquired or accessed by TELUS and shall not be altered in any material respect.

23. Equipment Security

(a) TELUS shall ensure that adequate controls are implemented with respect to the TELUS Equipment and the Network in order to ensure that they are appropriately secured which shall include, at a minimum, the following measures:

(i) appropriate log-in procedures such as password security and limits on unsuccessful attempts to log-in;

(ii) the changing of default passwords and the prohibition on use of blank passwords;

(iii) the disabling of unneeded ports, protocols and services;

(iv) appropriate destruction and scrubbing of all memory or storage devices that are discarded or reused and which could potentially contain GPS Confidential Information (including any configuration data) or any Personal Information; and

(v) the performance of all remote management in a secure manner, using encrypted communication channels and adequate access controls.

24. Destruction Of Information

At such time as required under this Agreement, or at such earlier time as a GPS Entity may require, and unless prohibited from doing so by Applicable Laws, TELUS shall destroy or otherwise dispose of all Agreement Records, Personal Information and GPS Confidential Information; provided, however, that TELUS must notify the GPS Entity of any intended destruction or disposal at least 30 days prior to commencing the destruction or disposal and, unless the GPS Entity indicates in writing that delivery is not necessary.

25. Reporting

(a) TELUS will at no additional cost generate the following security reports every six months and provide such reports to the GPS Entities upon request from a Designated Security Prime or Security Authorised Representative:

(i) vulnerability scan reports of the infrastructure providing the Services, including all network equipment providing the Services;

(ii) Patch status reports for the infrastructure providing the services.

(b) A GPS Designated Security Prime or Security Authorised Representative may request a copy of these reports at any time within the 6 month cycle, provided that TELUS will only generate these reports on a 6 month cycle.

(c) TELUS will retain control of the format and overall content of the reports, but will maintain standards in alignment with industry standard best practise reporting for security.

26. Security Screening Requirements

(a) TELUS shall employ the following personnel security screening requirements, which are at the Effective Date consistent with TELUS internal policy and shall be subject to the Change Process, to determine whether or not Personnel or External Personnel (for the purposes of this section 26, each such individual a "**Services Worker**") constitutes an unreasonable security risk:

(i) Verification of name, date of birth and address. TELUS will verify the name, date of birth and current address of a Services Worker by viewing at least one piece of "primary identification" of the Services Worker and at least one piece of "secondary identification" of the Services Worker,* as described in the table below. TELUS will obtain or create, as applicable, records of all such verifications and retain a copy of those records. For a Services Worker from another province or jurisdiction, reasonably equivalent identification documents are acceptable.

Primary Identification	Secondary Identification
Issued by ICBC: • B.C. driver's licence or learner's licence (must have photo) • B.C. Identification (BCID) card	• School ID card (student card) • Bank card (only if holder's name is on card) • Credit card (only if holder's name is on card) • Passport • Foreign birth certificate (a baptismal certificate is not acceptable)
Issued by provincial or territorial government: • Canadian birth certificate **Issued by Government of Canada:** • Canadian Citizenship Card • Permanent Resident Card • Canadian Record of Landing/Canadian Immigration Identification Record	• Canadian or U.S. driver's licence • Naturalization certificate • Canadian Forces identification • Police identification • Foreign Affairs Canada or consular identification • Vehicle registration (only if owner's signature is shown) • Picture employee ID card • Firearms Acquisition Certificate • Social Insurance Card (only if has signature strip) • B.C. CareCard • Native Status Card • Parole Certificate ID • Correctional Service Conditional Release Card

*It is not necessary that each piece of identification viewed by TELUS contains the name, date of birth and current address of the Services Worker. It is sufficient that, in combination, the identification viewed contains that information.

(ii) Verification of education and professional qualifications. TELUS will verify, by reasonable means, any relevant education and professional

qualifications of a Services Worker, obtain or create, as applicable, records of all such verifications, and retain a copy of those records.

(iii) Verification of employment history and reference checks. TELUS will verify, by reasonable means, any relevant employment history of a Services Worker, which will generally consist of TELUS requesting that a Services Worker provide employment references and TELUS contacting those references. If a Services Worker has no relevant employment history, TELUS will seek to verify the character or other relevant personal characteristics of the Services Worker by requesting the Services Worker to provide one or more personal references and contacting those references. TELUS will obtain or create, as applicable, records of all such verifications and retain a copy of those records.

(iv) Security interview. A GPS Entity may request that TELUS permit and assist the GPS Entity to conduct a security-focused interview with a Services Worker if the GPS Entity identifies a reasonable security concern. TELUS will review the request and determine (in its sole discretion acting reasonably) whether to permit and facilitate any such interview.

(v) Criminal history check. TELUS will arrange for and retain documented results of a criminal history check for all Services Workers directly providing support under this Agreement, including employees in all positions that may, in the course of their duties, have access to communications facilities or information repositories containing government information. Notwithstanding the foregoing, TELUS' employees as of the Effective Date are considered exempt and are not required to have a current criminal history check. TELUS will arrange for and retain documented results of a criminal history checks on a Services Worker obtained through the Services Worker's local policing agency

27. Personnel Security

(a) TELUS will implement screening procedures and perform background and security checks on all the Personnel and External Personnel who have access to GPS Confidential Information and Personal Information in accordance with the terms of this Agreement and will have appropriate procedures in place at all time during the Full Term to prevent any disclosure of GPS Confidential Information and Personal Information when such Personnel or External Personnel's employment or contracts are terminated. TELUS shall provide sufficient training to the Personnel and External Personnel on the Security Obligations and the Privacy Obligations to ensure compliance.

(b) TELUS will not permit a Services Worker who is an employee or volunteer of the TELUS Group to have access to sensitive GPS Confidential Information unless the Services Worker has first entered into a confidentiality agreement with TELUS to keep GPS Confidential Information confidential.

(c) TELUS will only permit a Services Worker who is an employee or a volunteer of the TELUS Group to have access to GPS Confidential Information or otherwise

be involved in providing the Services if, after having subjected the Services Worker to the personnel security screening requirements set out in this Schedule R and any additional requirements TELUS may consider appropriate, TELUS is satisfied that the Services Worker does not constitute an unreasonable security risk. TELUS will create, obtain and retain records documenting TELUS' compliance with the security screening requirements set out in this Schedule R.

28. GPS Infrastructure Acceptable Use

Infrastructure owned or leased by any GPS Entity is to be used by TELUS only to provide Services to the GPS Group. The use of unauthorized attachments of cables, modems, wireless, optical transmission components or other communication equipment on any portion of the infrastructure owned or leased by the GPS Group is prohibited. TELUS agrees to have policies and procedures that will prohibit such use and attachments. The GPS Group will communicate to TELUS any such requirements or policies respective to the use of such GPS Entity owned infrastructure.

29. Adherence to GPS Group Security Safeguards

TELUS and other members of the TELUS Group will implement mutually agreed security safeguards respecting the Services and the Network as may be requested by the GPS Group during the Full Term of this Agreement subject to the Change Process.

30. Material Breach

A breach of this Schedule by TELUS will be considered to be a material breach of this Agreement where such breach:

(a) is a result of any failure by the TELUS Group to comply with its obligations under this Schedule R or the Security Obligations;

(b) has resulted in unauthorized access, collection, use, exposure or disclosure of GPS Entity records or information (including GPS Confidential Information or any Personal Information of any GPS Entity or any GPS End User); and

(c) results in any GPS Entity or GPS End User suffering material harm.

31. Security Representatives

(a) TELUS and each GPS Entity will designate its own primary point of contact for all security related issues between TELUS and the GPS Entity (each a "Designated Security Prime"). Each Designated Security Prime will execute an appropriate non-disclosure agreement as required under this Agreement. Each Designated Security Prime will be vetted through appropriate background checks and will have appropriate professional experience for the performance of such duties. The Designated Security Prime of a GPS Entity can assign the role of Security Authorized Representative.

(b) A GPS Entity may assign authority on its behalf to any individual to conduct activities such as audits or investigations on behalf of such GPS Entity (a "Security Authorized Representative"). Each Security Authorized Representative

will execute an appropriate non-disclosure agreement as required under this Agreement. Each Security Authorized Representative will be vetted through appropriate background checks and will have appropriate professional experience for the performance of such duties.

Attachment R1

Long Distance Services Specific Security Requirements

In addition to TELUS' other obligations under Schedule R, and without limitation, TELUS will comply and will cause the TELUS Group to comply with the following security-related terms, conditions and requirements in connection with the provision of any Long Distance Services under this Agreement.

1. TELUS will, upon request of a GPS Entity, provide telephone Call Detail Records (CDR) with respect to Long Distance Services provided to such GPS Entity to assist in security investigations under section 16 of Schedule R.

2. TELUS will comply with the following requirements:

    2.1 TELUS will ensure that it has the ability to provide CDR for all long-distance, toll-free or calling card calls provided as part of the Long Distance services.

    2.2 CDR will contain at a minimum the following types of information: (a) date of call; (b) time of call; (c) source telephone number; (d) destination telephone number; and (e) and length of call.

    2.3 In addition to its other obligations, TELUS will comply with the GPS Group Security Policies regarding the log data retention, storage and access to CDR with respect to the Long Distance Services. TELUS will ensure that adequate security controls, processes, monitoring and access controls are implemented to ensure that such CDR in the custody of TELUS will not be modified, tampered, or deleted trough unauthorized actions, whether malicious or accidental.

    2.4 To support security investigations conducted under section 16 of Schedule R, TELUS will:

        2.4.1 make best efforts to provide electronic access (read only) for the GPS Entities' investigators to the CDR with respect to the Long Distance Services directly via an on-line facility or to archived CDR via an adequate interface; or

        2.4.2 if TELUS is unable to provide electronic access to CDR as required herein, provide at a minimum CDR with respect to the Long Distance Services in a CSV or equivalent electronic file format.

    2.5 TELUS will, upon request of a GPS Entity, provide summary reports of such CDR, including reports based on specific numbers, dates and other call details, within two Business Days from the time the GPS Entity makes the request.

    2.6 For cases where GPS Entity indicates that the request is related to an emergency life or limb situation, TELUS will provide the CDR in the time frames outlined in section 16 of Schedule R.

2.7 TELUS will comply with the Province's applicable data retention periods as set out in the applicable GPS Group Security Policies. For clarity, as of the Effective Date the GPS Group Security Policies require a total period of two years from the creation of such record, provided, however, that if electronic access to such record is provided by TELUS in accordance with this Attachment R1, such period will be structured as follows:

2.7.1 such record will be available on-line for a minimum of six months from the time of creation (provided that a one year period on-line is preferred); and

2.7.2 such record will be archived for the balance of the required two year retention period and will be provided to the GPS Designated Security Primes upon request.

Attachment R2

Conferencing Services Specific Security Requirements

In addition to TELUS' other obligations under Schedule R, and without limitation, TELUS will comply and will cause the TELUS Group to comply with the following security-related terms, conditions and requirements in connection with the provision of any Web and Audio Conferencing Services under this Agreement.

1. Audio Conferencing Specific Security Requirements

In connection with the provision of any Audio Conferencing Services that form part of the Conferencing Services, TELUS will comply with the following privacy and security requirements:

(a) Audio Conferencing Services will be in compliance with FOIPPA such that all (primary and back-up) servers and bridges will be located in Canada.

(b) Audio Conferencing Services will be accessible only by a secure passcode.

(c) TELUS will ensure that Audio Conferencing Services call detail records (CDR) are created and will be provided on-line via the TELUS Active Reporting portal.

(d) TELUS will ensure that reporting data can be exported to CSV or other electronic format via the TELUS Active Reporting portal.

(e) TELUS will provide administrative level access to the TELUS Active Reporting portal to authorized GPS Entity security investigations staff to support investigations.

(f) The CDR for the Audio Conferencing Services will contain at a minimum the following types of information:

(i) date of conference call;

(ii) time of conference call start and stop;

(iii) calling from number of all conference participants when available;

(iv) dialled Number of each conference participant;

(v) conference minutes total;

(vi) conference type;

(vii) conference ID;

(viii) start time, Stop time of individual conference participant; and

(ix) individual length of conference participation for each conferencing participant.

(g) TELUS will comply with the Province's applicable data retention periods as set out in the applicable GPS Group Security Policies. For clarity, as of the Effective Date the GPS Group Security Policies require TELUS to retain the records for a total period of two years from the creation of such records.

(h) TELUS will ensure that adequate security controls, processes, monitoring and access controls are implemented to ensure that such CDR in the custody of TELUS will not be modified, tampered with, or deleted through unauthorized actions, whether malicious or accidental.

(i) In connection with the provision of any Reservation-less Conferencing Services, TELUS will comply with the following security requirements:

(i) TELUS will provide each Host with a permanent dial-in telephone number and a pass code that is a minimum of four characters in length; and

(ii) TELUS will always require a pass code to be entered by the Host to begin a reservation-less Conference.

2. Web Conferencing Specific Security Requirements

In connection with the provision of any Web Conferencing Services, TELUS will comply with the following privacy and security requirements:

Records and Reporting

(a) TELUS shall provide all standard available reports for web conferencing services that are provided by the software vendors of the Web Conferencing Services. For clarity, TELUS will not provide additional reports or security records, including SNMP, Netflow, Syslog or other system generated security logging from these service platforms.

(b) TELUS will make such reports available online as made available by the software vendors.

(c) TELUS will comply with the Province's applicable data retention periods as set out in the applicable GPS Group Security Policies. For clarity, as of the Effective Date the GPS Group Security Policies require TELUS to retain the records for a total period of two years from the creation of such records.

(d) TELUS will ensure that adequate security controls, processes, monitoring and access controls are implemented to ensure that such CDR in the custody of TELUS will not be modified, tampered with, or deleted through unauthorized actions, whether malicious or accidental.

Incidents, Investigations and Response times

(e) TELUS' ability to comply with the incident, investigation and response times in Schedule R is subject to the ability of the software vendors to comply. TELUS will make commercially reasonable efforts to ensure that the response from application vendors is within a reasonable time frames.

Passcodes

(f) TELUS will ensure that Web Conferencing Services are accessed via unique username and pass codes.

(g) TELUS will provide the initial unique password; however GPS End Users are responsible for the management and protection of passwords after the initial setup

Attachment R3

Attachment R3-C

Attachment R5

Attachment R9

Cellular Services Specific Security Requirements

In addition to TELUS' other obligations under Schedule R, and without limitation, TELUS will comply and will cause the TELUS Group to comply with the following security-related terms, conditions and requirements in connection with the provision of any Cellular Services under this Agreement.

1. Cellular Call Detail Records

1.1 TELUS shall ensure that it has the ability to provide Cellular CDR to the GPS Entities for all calls.

1.2 TELUS will ensure that the Cellular CDR will contain at a minimum the following types of information: (a) date of call; (b) time of call; (c) source telephone number; (d) destination telephone number; and (e) and length of call.

1.3 In addition to its other obligations, TELUS will comply with the GPS Entity security and data retention Policies regarding the log data retention, storage and access to Cellular CDR. TELUS will ensure that adequate security controls, processes, monitoring and access controls are implemented to ensure that Cellular CDR in the custody of TELUS will not be modified, tampered, or deleted trough unauthorized actions, whether malicious or accidental.

1.4 To support security investigations conducted under section 16 of Schedule R, TELUS will:

1.4.1 make best efforts to provide electronic access (read only) for the GPS Entities' investigators to the CDR with respect to the Cellular Services directly via an on-line facility or to archived CDR via an adequate interface; or

1.4.2 if TELUS is unable to provide electronic access to CDR in accordance with section 1.4.1 above, provide at a minimum CDR with respect to the Cellular Services in a CSV or equivalent electronic file format.

1.5 TELUS will, upon request of a GPS Entity, provide summary reports of such Cellular CDR, including reports based on specific numbers, dates and other call details, within two Business Days from the time the GPS Entity makes the request.

1.6 For cases where GPS Entity indicates that the request is related to an emergency life or limb situation, TELUS shall take immediate actions and will provide the CDR as soon as possible.

1.7 TELUS will comply with the Province's applicable data retention periods as set out in the applicable GPS Group Security Policies. For clarity, as of the Effective Date the GPS Group Security Policies require that the total period retention of a CDR will be two years, from the creation of such record, provided, however, that

if electronic access to such is provided by TELUS in accordance with this Attachment R9, such period will be structured as follows:

1.7.1 such record will be available on-line for at a minimum of six months from the time of creation (provided that a one year period on-line is preferred); and

1.7.2 such record will be archived for the balance of the required two year retention period.

2. Cellular Services

2.1 TELUS will ensure that:

2.1.1 any Cellular Service will be secure and encrypted per applicable 3GPP standards;

2.1.2 appropriate security measures will be implemented to protect and preserve the integrity, confidentiality and availability of the GPS Entities' data being transmitted using any wireless infrastructure provided; and

2.1.3 any new cellular service or wireless technologies will at a minimum meet the security level of current services.

2.2 If TELUS proposes to use any new wireless technologies to provide the Cellular Services, TELUS will provide full details of security of the proposed solution to the GPS Group.