SCHEDULE HH – POLICIES

1. General Policies

Subject to section 5 of Schedule R (Security Requirements), set out below is a list of policies of the GPS Entities that apply to all GPS Entities:

1.1 "Core Policy and Procedures Manual", all applicable chapters, and especially chapter 12 and chapter 12 Supplemental (as may be accessed from the Web site of the Office of the Chief Information Officer at http://www.cio.gov.bc.ca/cio/leg_graphic.page or http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm; and Chapter 12 http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

1.2 Data retention requirements in accordance with the Government's Operational Records Classification System (ORCS): Operational Records Classification System (ORCS) - Information Technology Services Section (as may be accessed from a Web site at http://www.gov.bc.ca/citz/iao/records_mgmt/arcs_orcs/ORCS/e_reference_library/ITS/index.html"FOIPP Act Policy and Procedures Manual" of the Province (as may be accessed from http://www.cio.gov.bc.ca/cio/priv_leg/foippa/foippa_guide.page);

1.3 "Standards of Conduct" of the Province;

1.4 the GPS Group Security Policies; and

1.5 any other related policies and any amendments, replacements or supplements to any of the policies described above in this Section 1 as may be requested from to time by the Administrator (subject to the Change Process).

2. GPS Entity-Specific Policies

2.1 Within 6 months after the Effective Date (the "**GPS Policy Review Period**"), TELUS will review the policies set out in section 2.3, which are specific to particular GPS Entities (other than the Province), and, with respect to each GPS Entity named below, identify and notify in writing such GPS Entity of: (a) any compliance exceptions to the policies of such GPS Entity that TELUS reasonably requires and would like to be granted by such GPS Entity; or (b) any changes to this Agreement that TELUS reasonably requires for TELUS to comply with the policies of such GPS Entity (e.g. an additional Fee). Any such notice provided by TELUS to a GPS Entity will set out TELUS' rationale for reasonably requiring each policy exemption or change to this Agreement requested. Notwithstanding the foregoing, TELUS will only be entitled to request an exception to any of the policies set out in section 2.3 or a change to this Agreement for TELUS to comply with any of such policies to the extent such policies are inconsistent with or more burdensome than the Province policies set out in section 1 or TELUS has not

agreed to comply with such policies under another agreement between TELUS and the applicable GPS Entity in connection with the provision of services similar to the Services. Upon TELUS requesting within the GPS Policy Review Period an exception to a policy of a GPS Entity set out in section 2.3 or a change to this Agreement for TELUS to comply with a policy of a GPS Entity set out in section 2.3, such GPS Entity and TELUS will enter into discussions with respect to such requested exception or change and if such GPS Entity and TELUS cannot agree on how to address such request to the satisfaction of both such parties within a further 30 days, the matter will be resolved in accordance with the Dispute Resolution Process. TELUS and the Administrator will enter into an amendment to this Agreement or Change Order to the extent required to document any resolution with respect to a requested change or policy exception under this section 2.1 agreed to by a GPS Entity and TELUS (whether through the Dispute Resolution Process or otherwise), provided that such change or policy exception does not affect any of the other GPS Entities.

2.2 The GPS Entities will co-operate reasonably with TELUS during the GPS Policy Review Period, including making available their Designated Security Prime and required subject matter experts to the extent reasonably required to assist with interpretation of the policies listed in section 2.3.

2.3 After the GPS Policy Review Period, TELUS will comply with the following policies specific to particular GPS Entities except any policies or portions thereof with respect to which TELUS has requested a change to this Agreement or an exception in accordance with section 2.1.

2.3.1 In connection with the performance of Services for British Columbia Hydro and Power Authority, the following policies of British Columbia Hydro and Power Authority:

2.3.1.1 IMM Document Control Process (Ref. # 0B.103.01);

2.3.1.2 Information Management Manual Description (Ref. # 0G.100.01);

2.3.1.3 Short Document Template Cover (Ref. #0G.101.03);

2.3.1.4 IMM Process Definition Template Cover (Ref. # 0G.102.03);

2.3.1.5 IMM Form, Template or Checklist Cover Sheet (Ref. # 0G.103.02);

2.3.1.6 IMM Policy Document Template Cover (Ref. # 0G.104.03);

2.3.1.7 IMM Standards Document Template Cover (Ref. # 0G.105.03);

2.3.1.8 IMM Document Review Record Cover Sheet (Ref. # 0G.107.01);

2.3.1.9 IMM Document Review Log Cover Sheet (Ref. # 0G.108.01);

2.3.1.10 Long Document Template Cover (Ref. # 0G.109.03);

2.3.1.11 Data Management Policy (Ref. # 1A.002.03);

2.3.1.12 Electronic Data Loss Prevention Policy (Ref. # 1A.040.03);

2.3.1.13 Information Life Cycle Management and Storage Policies (Ref. # 1A.100.01);

2.3.1.14 Data Reference Definitions Standards (Ref. # 1D.001.02);

2.3.1.15 Data Model Data Naming Standards (Ref. # 1D.003.03);

2.3.1.16 Data Modeling Standard (Ref. # 1D004.03);

2.3.1.17 Date Standards (Ref. # 1D.010.04);

2.3.1.18 Data Backup and Recovery Guidelines (Ref. # 1D.040.05);

2.3.1.19 Internet Content Policy (Ref. # 2A.022.03);

2.3.1.20 Acceptable Use Policy (Ref. # 2A.020.09);

2.3.1.21 Medium Distance Wireless LAN Technologies Policy (Ref. # 2A.040.02);

2.3.1.22 Cellular Phone, Blackberry and Wireless Device Use Policy (Ref. # 2A.101.02);

2.3.1.23 Horizontal LAN Cabling Standards (Ref. # 2D.004.04);

2.3.1.24 Intranet Standards (Ref. # 2D.005.03);

2.3.1.25 Dial Access Standards (Ref. # 2D.040.04);

2.3.1.26 Data Network Protocol Standards (Ref. # 2D.002.05);

2.3.1.27 LAN and WAN Site Additions and Administration Guidelines (Ref. # 2D.010.03);

2.3.1.28 Home Wireless LAN Setup Guidelines (Ref. # 2D.020.03);

2.3.1.29 Corporate Network Operating System Standard (Ref. # 2D.050.04);

2.3.1.30 Wireless LAN Standard (Ref. # 2D.200.01);

2.3.1.31 Unmanaged LAN Switch Standard (**Ref. # 2D.230.01**);

2.3.1.32 WAN Acceleration Standard (Ref. # 2D.460.01);

2.3.1.33 Home Wireless LAN Security Installation Guide Supplemental (Ref. # 2G.100.02);

2.3.1.34 Desktop Environment Management Policy (Ref. # 3A.001.11);

2.3.1.35 Information Technology Hardware and Software Acquisition Policy (Ref. # 3A.011.09);

2.3.1.36 Virtualize First Policy (Ref. # 3A.101.02);

2.3.1.37 Upgrade, Redeployment and Disposal of Computer Assets Procedure (Ref. # 3B.004.10);

2.3.1.38 Business as Usual Hardware Acquisition Process (Ref. # 3B.012.03);

2.3.1.39 Hardware Refresh Procedure (Ref. # 3B.013.04);

2.3.1.40 Controlling the Threat of Malicious Code Procedure (Ref. # 3B.030.05);

2.3.1.41 Social Engineering Mitigation Procedure (Ref. # 3B.031.01);

2.3.1.42 Standards and Approved Products for Hardware and Software (Ref. # 3D.001.65);

2.3.1.43 Software Security Patching Procedure (Ref. # 3D.004.03);

2.3.1.44 Relational Database Software Selection Guidelines (Ref. # 3D.008.03);

2.3.1.45 Server Product Standards (Ref. # 3D.010.06);

2.3.1.46 Database Software Standard (Ref. # 3D.011.09);

2.3.1.47 Printer, Plotter and MFD Standards (Ref. # 3D.020.22);

2.3.1.48 Internal Contacts for IT Vendor Inquires (Ref. # 3E.001.08);

2.3.1.49 Application Integration Policy (Ref. # 4A.030.03);

2.3.1.50 Information System Design Security Review Procedure (Ref. # 4B.032.03);

2.3.1.51 Application Certification Guidelines (Ref. # 4B.040.03);

2.3.1.52 Application Integration Assessment Process (Ref. # 4B.100.01);

2.3.1.53 Interface TP Techniques Analysis Matrix Cover Sheet (Ref. # 4G.100.01);

2.3.1.54 EAI Interface Implementation Effort Estimation Template Cover Sheet (Ref. # 4G.101.01);

2.3.1.55 Packaged Application General Upgrade Procedure (Ref. # 5B.003.03);

2.3.1.56 IT Security Design Checklist Procedure (Ref. # 5B.060.01);

2.3.1.57 Packaged Application Customization Preference Ordering Guidelines (Ref. # 5D.100.01);

2.3.1.58 User Interface Design Standards (Ref. # 5D.101.01);

2.3.1.59 Information Management Principles Compliance Policy (Ref. # 6A.003.05);

2.3.1.60 Cyber Threat Alert Response Policy (Ref. 6A.004.03);

2.3.1.61 Computing Access Policy (Ref. # 6A.012.04);

2.3.1.62 Business Continuity Planning Policy (Ref. # 6A.020.04);

2.3.1.63 Background Check Policy for IT Security Sensitive Positions (Ref. # 6A.030.07);

2.3.1.64 Compliance Management Policy **(Ref. # 6A.080.06)**;

2.3.1.65 IT Asset Change Management Policy (Ref. # 6A.081.07);

2.3.1.66 Privacy Impact Assessment Policy (Ref. # 6A.100.03);

2.3.1.67 Remote Access Policy (**Ref. # 6A.101.02**);

2.3.1.68 Network Attachment Policy (Ref. # 6A.102.01);

2.3.1.69 E-Mail Practice, Virus Protection and Scanning Procedure (Ref. # 6B.015.06);

2.3.1.70 IT Inventory Update and Reporting Guidelines (Ref. # 6B.050.04);

2.3.1.71 Applying the Enterprise IT Architecture Guidelines (Ref. # 6B.004.05);

2.3.1.72 Securing Sensitive Information on Client Devices and LANs Procedure (Ref. # 6B.009.05);

2.3.1.73 Computing Access Authorization Procedure (Ref. # 6B.012.04);

2.3.1.74 Internet Access Guidelines (Ref. # 6B.014.03);

2.3.1.75 Business Continuity Planning Guidelines for Information Systems (Ref. # 6B.021.03);

2.3.1.76 IT Capital Planning Procedure (Ref. # 6B.030.03);

2.3.1.77 Background Check Process for Security Sensitive Positions (Ref. # 6B.036.06);

2.3.1.78 Guidelines for Preventing Accidental Information Disclosure (Ref. # 6B.042.02);

2.3.1.79 IT QA Action Tracker Request Procedure (Ref. # 6B.100.01);

2.3.1.80 IMM Jurisdictional Review Process (Ref. #6B.102.01);

2.3.1.81 Information Technology Procurement Process (Ref. #6B.103.02);

2.3.1.82 IT Asset Change Management Process (Ref. #6B.104.03);

2.3.1.83 Third Party Data Access Request Process (Ref. #6B.108.02);

2.3.1.84 Establish and Manage Standards Process Definition (Ref. # 6B.109.01);

2.3.1.85 Plan and Prioritize Portfolio Process Definition (Ref. # 6B.110.01);

2.3.1.86 IMM IT QA Review Process (Ref. # 6B.112.01);

2.3.1.87 Realize Program or Project Benefits Process Definition (Ref. # 6B.113.01);

2.3.1.88 Manage IT Service Provider Process Definition (Ref. # 6B.114.02);

2.3.1.89 Manage IT Asset Portfolio Process Definition (Ref. # 6B.115.02);

2.3.1.90 Develop and Measure Performance Metrics Process Definition (Ref. # 6B.116.01);

2.3.1.91 Develop IT Operating Budget Process Definition (Ref. # 6B.117.01);

2.3.1.92 Goal Technology Architecture Process (Ref. # 6B.118.01);

2.3.1.93 User Centered Design (UCD) Process (Ref. # 6B.119.01);

2.3.1.94 Security Architecture Model (Ref. # 6C.010.03);

2.3.1.95 User ID and Password Standard (Ref. # 6D.010.10);

2.3.1.96 Remote Access Standards (Ref. # 6D.020.04);

2.3.1.97 BC Hydro Portfolio Management System User's Guide (Ref. # 6D.100.01);

2.3.1.98 IMM IT Performance Metrics Collection and Reporting Guideline (Ref. # 6D.101.01);

2.3.1.99 IT Definition and Compliance Standard (Ref. # 6D.102.01);

2.3.1.100 IT Development Standard Process Definition and Tailoring Guidelines (Ref. # 6D.103.03);

2.3.1.101 IMM Document Template Guidelines (Ref. # 6D.104.01);

2.3.1.102 IT Project Management Guidelines (**Ref. # 6B.005.09**);

2.3.1.103 IT Investment Principles (Ref. # 6D.106.01);

2.3.1.104 Purchasing Mechanism Application Guideline (Ref. # 6D.107.01);

2.3.1.105 IT Products and Services Procurement Guidelines (Ref. # 6D.108.02);

2.3.1.106 IT Commissioning Guide (Ref. # 6D.109.01);

2.3.1.107 Information Management Organization and Committees (Ref. # 6E.010.07);

2.3.1.108 IT QA Review Checklist Cover Sheet (Ref. # 6F.022.02);

2.3.1.109 Asset Strategy and Plan Template Cover (Ref. # 6G.100.01);

2.3.1.110 Detailed EAR Business Case Template Cover (Ref. # 6G.101.02);

2.3.1.111 IT Performance Metrics Dashboard Template Cover (Ref. # 6G.103.01);

2.3.1.112 Change Request Template Cover (Ref. # 6G.104.01);

2.3.1.113 Project Charter Cover Sheet (Ref. # 6G.106.02);

2.3.1.114 Simplified Business Case Template Cover Sheet (Ref. # 6G.107.01);

2.3.1.115 Project Effectiveness Report Template Cover Sheet (Ref. # 6G.108.02);

2.3.1.116 Information Management Metrics Definition Template Cover Sheet (Ref. # 6G.109.02);

2.3.1.117 Third Party Data Access Request Approval Form Cover Sheet (Ref. # 6G.110.02);

2.3.1.118 Simplified Hazard Identification Matrix Cover (Ref. # 6G.111.01);

2.3.1.119 Requirements Signoff Form Cover Sheet (Ref. # 6G.120.01);

2.3.1.120 System Design Signoff Form Cover Sheet (Ref. # 6G.121.01);

2.3.1.121 Develop or Customization Signoff Form Cover (Ref. # 6G.122.01);

2.3.1.122 User Acceptance Signoff Form Cover (Ref. # 6G.123.01);

2.3.1.123 Training Signoff Form Cover (Ref. # 6G.124.01);

2.3.1.124 Implement Signoff Form Cover (Ref. # 6G.125.01);

2.3.1.125 Warranty Signoff Form Cover (Ref. # 6G.126.01);

2.3.1.126 Project Completion – Acceptance Report Cover (Ref. # 6G.127.01);

2.3.1.127 IT DSP Tailoring / Gating Template Full Cover Sheet (Ref. # 6G.128.02);

2.3.1.128 IT DSP Tailoring / Gating Template Full Cover Sheet (Ref. # **6G.128.01**);

2.3.1.129 IT DSP IT Project Complexity Assessment Tool Cover Sheet (Ref. # 6G.132.01);

2.3.1.130 IT Commissioning RFP Toolkit Cover Sheet (Ref. # 6G.133.01);

2.3.1.131 IT Commissioning Compliance Report Template Cover Sheet (Ref. # 6G.134.01);

2.3.1.132 IT Commissioning Scoping Report Template Cover Sheet (Ref. # 6G.135.01);

2.3.1.133 IT Commissioning Confirm Technical Architecture Template Cover Sheet (Ref. # 6G.136.01);

2.3.1.134 IT Commissioning Deliverable Review Template Cover Sheet (Ref. # 6G.137.01);

2.3.1.135 IT Commissioning Activities RACI Checklist Cover Sheet (Ref. # 6G.138.01);

2.3.1.136 Organization of Information Security Policy (Ref. # 7A.201.01);

2.3.1.137 Physical and Environmental Security of Information Policy (Ref. # 7A.204.01);

2.3.1.138 IT Communications and Operations Management Policy (Ref. # 7A.205.01);

2.3.1.139 Access Control Policy (Ref. # 7A.206.01);

2.3.1.140 Information Systems Acquisition Development and Maintenance Policy (Ref. # 7A.207.01);

2.3.1.141 Information Security Incident Management Policy (Ref. # 7A.208.01);

2.3.1.142 Business Continuity Management Policy (Ref. # 7A.209.01);

2.3.1.143 Information Security Compliance Policy (Ref. # 7A.210.01);

2.3.1.144 Information Security Policy (Ref. # 7A.100.02);

2.3.1.145 Disclosure, Storage and Access to Personal Information from Outside Canada Policy (Ref. # 7A.102.01);

2.3.1.146 Asset Management Policy (Ref. #7A.202.01);

2.3.1.147 Human Resources Security Policy (Ref. # 7A.203.01);

2.3.1.148 Missing, Lost or Stolen IT Asset or Data Notification Process (Ref. # 7B.101.02);

2.3.1.149 Information Security Governance Process Definition (Ref. # 7B.100.01);

2.3.1.150 Security Logging Standard (Ref. # 7D.102.01);

2.3.1.151 Personal Digital Assistant Security Standards (Ref. # 7D.100.01);

2.3.1.152 IT Security Design Checklist Form Cover (Ref. # 7G.100.02);

2.3.1.153 Consent to Collection and Release of Personal Information Form Cover (Ref. # 7G.101.01).

2.3.2 In connection with the performance of Services for Insurance Corporation of British Columbia, the following policy of Insurance Corporation of British Columbia:

2.3.2.1 Code of Ethics; and

2.3.3 In connection with the performance of Services for Workers Compensation Board of British Columbia, the following policies of Workers Compensation Board of British Columbia (WorkSafe BC):

2.3.3.1 Information Security Policy;

2.3.3.2 Asset Management Policy;

2.3.3.3 Access Control Policy;

2.3.3.4 Communications and Operations Management Policy;

2.3.3.5 Physical and Environmental Security Policy;

2.3.3.6 Systems Acquisition Development and Maintenance Policy;

2.3.3.7 Information Security Awareness and Compliance Policy;

2.3.3.8 Business Continuity Management Policy;

2.3.3.9 Information Security Incident Management Policy;

2.3.3.10 Information Security Compliance Policy;

2.3.3.11 Electronic Communications Policy;

2.3.3.12 Harassment Policy;

2.3.3.13 Scent Safety in the Workplace (HEA 1-9);

2.3.3.14 Standards of Conduct; and

2.3.3.15 Privacy Statement of WorkSafe BC.

2.4 For clarity, the policies of the Province listed in section 1 will apply in connection with the performance of Services for all GPS Entities during the GPS Policy Review Period and thereafter during the Full Term.