Government Contact Centre Services (GCCS) Stream 2: Contact Centre as a Service (CCaaS)

Statement of Work Template

Table of Contents

Index of Tables

1 PROJECT MANAGEMENT

(1) The requirements in this section apply to any Work for Service Readiness, Security and Privacy Readiness, Value Added Services, Subscription Service Subscription Service Configuration and Subscription Service Integration in accordance with Service Orders issued for Professional Services..

1.1 Work Project

(2) When and as requested by Canada, the Contractor must conduct and complete portions of the Work as a Work Project.

(3) The Contractor must begin the Work identified by Canada as a Work Project within 10 FGWDs of the request by Canada.

1.1.1 Work Project Meetings

(4) The Contractor must facilitate a weekly meeting for each Work Project (Work Project Meeting) that includes a presentation to review the Work Project Status Report.

(5) The Contractor must facilitate a weekly meeting to review all Work Projects that includes a presentation to review the Project Management Office (PMO) Status Report.

1.1.2 Work Project Reporting

(6) The Contractor must provide the reports for Work Projects in Table 1.

Table 1. Work Project Reports

Report Name	Work Project Status Report
Frequency	2 FGWDs prior to each Work Project Status Meeting
Purpose	The report must present the status of a Work Project.
Description	The report must include: a) minutes from the previous Work Project Review Meeting; b) action items; c) view of Project Schedule milestones; d) current and upcoming Work tasks; e) project issues including assessment of impacts and current escalation status; f) summary of Work Project risks; and g) summary with description of the Project Change Requests.
Report Name	Project Management Office (PMO) Status Report
Frequency	2 FGWDs prior to each PMO Meeting
Purpose	The report must present an overall summary of all Work Projects.
Description	The report must include: a) minutes from the previous PMO Meeting;

	b) action items; c) summary of top 5 issues; and d) view of Master Project Schedule milestones.

1.2 Project Change Requests

(7) The Contractor must create and maintain a log of Project Change Requests for each Work Project and master log for all Work Projects where the format of the log is developed in consultation with Canada and approved by Canada.

(8) The Contractor must review each Project Change Request in consultation with Canada and assess the impacts.

(9) The Contractor must update the Project Schedule if a Project Change Request affects any task or timeline in the Work Project.

(10) Canada is not required to issue a Project Change Request for new Work Projects. The re-allocation of Work between existing Work Projects or between existing Work Projects and new Work Projects will be done in consultation with the Contractor.

1.3 Project Risk Register

(11) The Contractor must create and maintain a Project Risk Register for each Work Project and a master register that summarizes the risks for all Work Projects where the format of the register is developed in consultation with Canada and approved by Canada...

1.4 Project Schedule

(12) The Contractor must create and maintain a Project Schedule for each Work Project and a master schedule that summarizes the Project Schedules for all Work Projects where the format of the schedule is developed in consultation with Canada and approved by Canada.

(13) .A Project Schedule must:

a) not create dependencies on Canada's review and acceptance of Work, unless approved by Canada;

b) limit dependencies to the maximum extent possible;

c) schedule tasks in parallel to the maximum extent possible;

d) provide for deliverables to be submitted progressively (i.e. not all at once);

e) be produced and maintained in Microsoft Project;

f) identify the phases, gates, tasks, deliverables and milestones of the Work including:

g) identify any Project Change Requests that cause changes to the completion date of any major milestone, with numbers assigned that correlate with the numbers assigned to them in the Work Project Status Report.

(14) The Contractor must set a baseline for all task start and end dates in a Project Schedule based on the date of acceptance of the Project Schedule by Canada.

(15) The Contractor must not change the baseline of a Project Schedule for the duration of the Work Project unless approved by Canada. If a change to the Project Schedule is approved by Canada, the Contractor must set a new baseline schedule in a new version of the Project Plan that clearly states that the baseline has been revised.

(16) The Contractor must ensure that resource assignments for a Project Schedule take into consideration the availability and non-availability of each resource (e.g. holidays, training and vacation), such that there is no impact to the completion of Work in the Work Project.

1.5 Project Resource Plan

(17) The Contractor must create and maintain a Project Resource Plan for each Work Project that includes:

a) roles and responsibilities of all resources (primary and backup Key Resources, other resources to the Manager level) to complete the Work for the Work Project including:

i) name and title of the resource;

ii) description of the qualifications of the resource to complete the Work; and

iii) work level allocation (dedicated, part time);

b) a Responsible, Accountable, Consulted, and Informed (RACI) chart to identify the Work by deliverable and Work activities to be completed by each resource, Canada and Client stakeholders to the manager level;

c) a description of the management escalation process (org chart with names and contact information for all resources on the Work Project).

(18) The Contractor must create and maintain a master Project Resource Plan that summarizes the Project Resource Plans for all Work Projects.

2 DOCUMENTATION

(19) The Contractor must define the content and format of documents for Work Deliverables in:

a) in consultation with Canada and subject to Canada's acceptance;

b) English, and in French when requested by Canada;

c) the native format (e.g. Word, Excel, Visio) and in PDF in a format. Where the diagrams are embedded within another document format (e.g. Word), the diagrams must be in a metafile format (not editable) to reduce the size of the documents;

(20) The Contractor must provide all diagrams used for a Work Deliverable as native Visio diagrams to Canada within 5 FGWDs of a request from Canada.

(21) The Contractor must provide user guides, training materials and OEM documentation in both English and French.

(22) The Contractor must ensure that all documentation is kept current and up-to-date at all times.

(23) The Contractor must not make any changes (format, content provided) to an approved Work Deliverable without following the Request Fulfillment processes.

(24) The Contractor must provide an updated Work Deliverable (text and diagrams) to Canada within 20 FGWDs of a request by Canada that reflects all changes to the document in associated Service Requests since the last version of the document.

3 MEETINGS

(25) Meetings must be conducted during business hours (8 am to 5 pm ET) on FGWDs.unless otherwise approved by Canada.

(26) The Contractor must provide agendas for all meetings prior to the meeting (excluding daily meetings) unless otherwise approved by Canada.

(27) Except where Canada specifies otherwise, for each meeting attended by the Contractor, the Contractor is responsible for:

a) coordinating with Canada;

b) coordinating any subcontractor participation (if necessary);

c) providing the minutes, schedules, lists, tests, design analysis and any other pre- and post-review data as appropriate;

d) ensuring that qualified Contractor personnel with knowledge of the issues to be discussed attend the meeting; and

e) ensuring the Contractor personnel representatives have sufficient authority to make expeditious decisions on behalf of the Contractor.

(28) The Contractor must prepare minutes for each meeting during the meeting and review with Canada at the end of the meeting where format for minutes is developed in consultation with Canada and approved by Canada.

4 SECURITY AND PRIVACY READINESS

(29) The Work in this subsection must be completed by the Contractor and accepted by Canada for the Security and Privacy Readiness deliverable at no additional cost to Canada.

4.1 Cloud Guardrail Assessment

(30) The Contractor must complete the Cloud Guardrail Assessment within 30 calendar days following the issuance of the Contract that includes Canadas time to review and assess evidence provided by the Contractor that the cloud guardrails specified at https://github.com/canada-ca/cloud-guardrails have been implemented for the Subscription Service.

(31) Where Canada exceeds 2 FGWDs to assess evidence and provide feedback, Canada will solely determine if the Contractor will be provided with additional time (calendar days) to complete the Cloud Guardrail Assessment.

4.2 Security Assessment

(32) The Contractor must complete a First Party Security Assessment OR a Third Party Security Assessment, as selected by the Contractor, in accordance with the Annex A Security Controls (separate attachment).

4.2.1 First Party Security Assessment

(33) The Contractor must provide Canada with a ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements certification and a ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services and a SOC 2 Type II report completed within the last 12 months of the Contract date.

4.2.2 Third Party Security Assessment

(34) The Contractor must complete a security assessment with an independent third party assurer, qualified under AICPA or CPA Canada and/or an ISO certification regime that conforms to ISO/IEC 17020 quality management system standards, at no additional cost to Canada that will prepare a Security Assessment Report that includes:

a) the legal business name of the Contractor;

b) current date and/or status of certifications and/or SOC 2 Type II report;

c) evidence to demonstrate compliance of the Service with Annex A-5 Security Requirements and other security requirements in the Contract;

d) name and address of the third party assurer that performed the security assessment; and

e) evidence that the third party assurer is qualified under AICPA or CPA Canada, and/or ISO certification regime that conforms to ISO/IEC 17020 quality management system standard.

4.3 Plan of Actions and Milestones

(35) The Contractor must provide a Plan of Actions and Milestones for Canada's approval within 20 FGWDS of a request from Canada that:

a) documents the remedial actions planned by the Contractor to correct security deficiencies identified during the Cloud Guardrail Assessment and Security Assessment and in any subsequent SOC2 Type II report or ISO re-certification; and

b) includes a Project Schedule to complete the remedial actions; and

(36) The Contractor must update the Plan of Actions and Milestones based on the results from security assessments, security impact analyses, and security monitoring activities conducted by the Contractor.

(37) The Contractor must implement the remedial actions identified in the Plan of Actions and Milestones in accordance with the Project Schedule for the initial approved version and any subsequent versions.

4.4 System Security Plan

(38) The Contractor must provide a System Security Plan (SSP) that documents the security controls in place, or planned for meeting, for the security requirements in the contract that:

a) Is consistent with the Contractor's enterprise architecture;
b) explicitly defines the authorization boundary for the Service;
c) describes relationships with or connections to other External Information Systems;
d) provides an overview of the Security Control Requirements for the Service;
e) describes the rationale for security controls including the tailoring and supplementation decisions; and
f) includes a component diagram that clearly shows the Services architecture.

4.5 Operations Security Procedures

(39) The Contractor must provide a Operations Security Procedures (OSP) that documents the following for each connection to a Service:

a) system components;
b) the interface characteristics;
c) security requirements;
d) nature of the information communicated;
e) secure configuration, installation, and operation of the Service;
f) effective use and maintenance of security functions;
g) known Security Vulnerabilities regarding configuration and use of administrative (i.e. privileged) security functions;
h) user-accessible security functions and how to effectively use those security functions;
i) methods for user interaction, which enables individuals to use the CCaaS service in a more secure manner; and
j) user responsibilities for maintaining the security of the CCaaS service and system components..

4.6 Service Incident Response Plan

(40) The Contractor must provide a Security Incident Response Plan that includes:

a) how the Contractor plans to identify, report, and escalate Security Incidents;
b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery;
c) a description of the structure and organization of the Security Incident response capability;
d) a high-level approach for how the Security Incident response capability fits into the Contractor's overall organization;
e) a definition of reportable Security Incidents;
f) a definition of metrics for measuring the Security Incident response capability; and
g) a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.

4.7 Service Contingency Plan

(41) The Contractor must provide a Service Contingency Plan that describes:

a) essential missions and business functions including supporting critical CCaaS system components and associated contingency requirements;
b) a detailed plan and documented processes for restoring Service operations;

c) back up strategies for datacentre facilities, network facilities, operational support systems and data, and key Service components;
d) recovery objectives, restoration priorities, and metrics as per Service Level Agreements (SLAs);
e) contingency roles, responsibilities, and assigned individuals with contact information;
f) process for full Service restoration without deterioration of the security safeguards originally planned and implemented;
g) how essential missions and business functions are maintained despite a Service disruption, compromise, or failure;
h) process(es) for testing the Service Contingency Plan;
i) detailed communications plans with Canada, Canada's Clients and the Contractor's suppliers and sub-contractors;
j) detailed plan and processes for transferring operational, management and administration functionality to a backup operations centre; and
k) steps the Contractor will take if any of its key subcontractors go out of business or are identified by Canada as being subject to security concerns

(42) The Contractor must implement Service Contingency Plan (all processes, procedures, roles, responsibilities etc.) following its acceptance by Canada and prior to completion of Service Readiness.

4.8 Privacy Management Plan

(43) The Contractor must provide a Privacy Management Plan to Canada that includes:
a) the roles and responsibilities of the Contractor's Privacy resources and how they interface with Canada and Contractor's suppliers;
b) a description of how the Contractor plans to develop and maintain overall privacy awareness on an ongoing basis through various channels (intranet, posters etc.);
c) a description of the Contractor's privacy protection strategies detailing exactly how the Personal Information will be treated over its life cycle;
d) a description of how the Contractor intends to ensure that its staff is trained on privacy and privacy;
e) a description of how the Personal Information will be collected, used, retained, and disclosed only for the purposes of the Work specified in the Contract;
f) a description of how the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;
g) processes for the development and testing of Services without using Canada production data (i.e. real information related to Users);
h) processes to identify, document, review, report, respond, and escalate privacy related Incidents;
i) processes for managing, accessing, collecting, using, disclosing, receiving, creating or disposing of personal information;
j) processes for limiting the retention of personal information and ensuring adherence to the retention requirements of Canada, including backup and archiving of data;
k) role-based access controls to restrict/limit access to operational and administrative information required by authorized Contractor personnel including logging all instances where personnel have had access to operational information;
l) processes to ensure incorporation of specific retention and disposal requirements as determined by Canada's Privacy Impact Assessments (PIA's); and
m) processes to ensure the logging and data capture settings of the information protection and network monitoring devices are appropriately defined to limit the collection of personal information;
n) process for dealing with requests for access to Records under the Access to Information Act and requests for access to Personal Information under the Privacy Act (Access Requests).
o) the privacy breach protocol, and details on how any privacy breaches will be handled;

p) any new measures the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification; and

q) how the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification..

4.9 Privacy Impact Assessment

(44) The Contractor must assist Canada in creating the privacy impact assessment for the Subscription Service in accordance with the TBS Directive on privacy impact assessment (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308).

(45) In particular, with respect to any information that Canada identifies as Personal Information during the Contract Period, the Contractor must provide the following information within 20 FGWDs of a request by the Contracting Authority:

a) business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;

b) a list of the Personal Information used by the Contractor in connection with the Work and the purpose of how each Personal Information item is used by the Contractor in connection with the Work;

c) how the Personal Information is shared and with whom;

d) a list of all locations where hard copies of Personal Information are stored;

e) a list of all locations where Personal Information in machine-readable format is stored (e.g., the location where any server housing a database including any Personal Information is located), including back-ups;

f) a list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by the Contract;

g) any privacy-specific security requirements or recommendations that need to be addressed;

h) a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

i) results of consultations (if any) from a privacy impact assessment review by the Office of the Privacy Commissioner of Canada (OPCC) with signoff by the OPCC.

j) The Contractor must implement recommendations from the privacy impact assessment based on a schedule approved by Canada at no cost to Canada.

k) If changes to Services are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by Canada, the Contractor must provide Canada with sufficient detail on the changes to support an update to the privacy impact assessment, and obtain approval from the Contracting Authority for the anticipated change.

l) The Contractor must provide a privacy awareness communications kit to Contractor resources involved in Services that provides an overview on the use of Personal Information.

5 SERVICE OPERATIONS

(46) The Work in this subsection is applicable to the ongoing operation, administration, management and maintenance of the CCaaS, with the objective of proactively diagnosing and repairing problems before these become service affecting and is included with the Subscription Service unless otherwise indicted in the SOW as requiring a Work Request Notice (WRN).

5.1 Service Desk

(47) The Contractor must provide a Service Desk that performs the following functions:

a) acting as the primary point of contact for Incidents reported by Canada 24 hours per day, 7 days per week, 365 days per year;
b) answering and continuing the subsequent Level 1 and Level 2 dialogue using the official language of Canada (French, English) requested by the caller;
c) interacting with Canada's representatives as designated by Canada's Service Desk;
d) providing a unique and dedicated toll-free telephone number (e.g., 1-800 number) for Canada's authorized representatives to access the Service Desk; and
e) providing a single email address for Canada's authorized representatives to access the Service Desk.

5.2 Operational Service Management

When requested by Canada in a Work Request Notice (WRN), the Contractor must provide 1 dedicated Engineer to provide 24 hours, 7 days per week operations support for:

a) providing general guidance/bestpractice adherence for the configuration and operation of the platform;
b) planned back log activities;
c) performing move, add, change, delete (MACD) functions;
    d) users, stations, workgroups, roles, ACDs, account codes, skills, schedules etc
i) performing configuration enhancements and modification;
j) adding or modifying call flows;
k) coordinating requirement gathering discussions;
l) coordinating formal work order delivery and project execution;
m) project related change control activity;
n) participating in production migration activity and operational handoff;
o) updating operational documentation;
p) management of incident tickets:
    i) troubleshooting and incident triage;
    ii) collection of logs and additional supporting information;
    iii) communication with point of contact for the ticket;
    iv) escalation of issues to higher tier support;
    v) coordination to transition high priority incidents to the Care team;
    vi) participation in calls for P1 and P2 incidents;
    vii) ensure delivery of root cause analysis for all P1 and P2 incidents;
    viii) coordination with Care team to ensure root cause analysis for P3/P4 incidents are provided when requested by Customer;
q) perform daily health checks;
r) real time resolution of issues discovered during health checks;

s) adhoc and historical reporting;

5.3 Service Operations Meetings

(48) The Contractor must facilitate and conduct the Service Review meetings summarized in Table 2Table 2.

Table 2. Service Review Meetings

Meeting Name	Service Management Review Meeting
Frequency	Monthly, or as requested by Canada
Purpose	Review of Incidents, Change Requests, Service Requests, Problems, Service Level Targets and Billing/Invoicing.
Description	The meeting must include a review of: a) issues log from previous meeting; b) action items log from previous meeting; c) Post-Service Request Reports from the previous month; d) Post-Change Request Reports from the previous month; e) Post-Incident Reports from the previous month; f) Service Level Targets and failures from the previous month; g) Service Requests scheduled for the coming month; h) Change Requests scheduled for the coming month; i) issues that have or may affect Service performance; and j) root cause analysis of open Incident Tickets.
Meeting Name	Security Review Meeting
Frequency	Within 1 FGWD of a request by Canada
Purpose	Review of Security Incidents
Description	The meeting must include a review of (for each Security Incident): a) date/time and duration of Security Incident; b) description including whether attack appears to have been successful; c) scope (Service Portal; single or multiple Clients, etc.); d) estimated injury/impact level; e) list of known and suspected Applications affected; f) actions taken; g) apparent source/origin of attack(s); and h) status of mitigations.

5.4 IT Service Management

(49) The Contractor must provide IT Service Management for Services, as described in the following subsections, 24 hours per day, 7 days per week and 365 days per year.

5.4.1 Change Management

(50) The Contractor must create a Change Request for any change that may disrupt Services.

(51) The Contractor must create 1 or more Change Request Tickets for a Change Request.

(52) The Contractor must create an Emergency Change Request for each mitigation measure required to contain a Security Incident.

(53) The Contractor must complete Change Request activity, excluding Emergency Change Requests, in maintenance windows. This includes the outage time to complete the Change Request and any outage time required for back-out of the Change Request. Any outage that extends beyond the maintenance window will be treated as the Service being unavailable and this outage period must be taken into account in the calculation of Service Level Target Service Availability (SLT-SA) and Service Level Target Maximum Time to Restore Service (SLT-MTRS). In such a case, the Contractor must initiate an Incident Ticket and record the time beyond the approved maintenance window as outage time for the Service.

(54) If the execution of a Change Request causes an unplanned impact or outage to a Service, or it is determined that it will exceed the maintenance window approved by Canada, the Contractor must contact Canada immediately. The Contractor must provide a detailed explanation of the impacts and the plan to restore the Service or complete the Change Request as quickly as possible. The Contractor must also initiate an Incident Ticket for any outage not identified in the Change Request.

(55) Any outage to a Service that occurs as a result of an Emergency Change Request initiated by the Contractor will be treated as the Service being unavailable.

(56) The Contractor must enter information in the Change Request Ticket log for a failed Change Request explaining the failure, what the current status is for the environment that was subject to the Change Request and what partial changes were implemented.

(57) The Contractor must provide a Post-Change Request Report to Canada within 5 FGWDs of a failed Change Request.

5.4.2 Request Fulfillment

(58) The Contractor must use Change Management for all changes required for a Service Request.

(59) The Contractor must create 1 or more Service Request Tickets for each Service Request submitted by Canada.

(60) The Contractor must update a Service Request Ticket following a change in Work associated with the Service Request.

(61) The Contractor must provide a Post-Service Request Report to Canada following a failed Service Request.

5.4.3 Release Management

(62) The Contractor must use Change Management for all changes required for a Service Release.

(63) The Contractor must not use Services in production to test a Service Release prior to any changes.

(64) The Contractor must provide a Post-Service Release report to Canada following a failed Service Release that includes a Service Release that:

a) had to be backed out;

b) that caused disruption to the Services, or

c) did not achieve the Contractor's objective and therefore may need to be repeated at a later date.

5.4.4 Event and Incident Management

(65) The Contractor must proactively monitor Services for Incidents 7 days per week, 24 hours per day, 365 days per year.

(66) The Contractor must co-operatively work with Canada, Clients and any other third parties identified by Canada to resolve Incidents.

(67) The Contractor must open an Incident Ticket after detecting an Incident or receiving a notice from Canada reporting an Incident.

(68) The Contractor must update the Incident Ticket log following a change in status for the Incident.

(69) The Contractor must assign the highest priority to Incidents for Applications specified by Canada.

(70) The Contractor must provide Canada with an operational escalation matrix and a management escalation matrix for Incidents that:

a) defines the primary contact for each level of escalation;

b) defines the alternates (of equal authority) for each level of escalation; and

c) contains clear instructions for contacting the primary and alternate escalation authority.

(71) The Contractor must categorize and assign Incidents with a priority level

(72) The Contractor must notify Canada of Incidents, with priority levels specified by Canada,.

(73) The Contractor must provide an estimated time for resolution within the Incident Ticket.

(74) The Contractor must resolve Incidents by taking appropriate action to repair and restore Services as quickly as possible in accordance with the SLT-SA associated with the affected Services.

(75) The Contractor must document in the Incident Ticket activity log all:

a) management and technical escalations for Incidents;

b) interactions with third parties;

c) investigation, troubleshooting and analysis details, resolution activities and communications for Incidents

(76) The Contractor must track and report the outage time of each Incident in the associated Incident Tickets.

(77) The outage time for an Incident must start at the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada, whichever occurs first.

(78) The outage time for an Incident ends at the time that the affected Services are fully restored in relation to that Incident.

(79) The Contractor must not alter the outage time for an Incident Ticket once the Incident Ticket has been closed.

(80) If an Incident Ticket is closed and a subsequent Incident occurs within 24 hours for the same Incident, the Contractor must re-open the original Incident or open a new Incident with a cross reference to the previous Incident, and calculate the outage time for the new Incident using the combined outage time of both Incidents, and record this time in the adjusted outage time field of the Incident Ticket.

(81) The Contractor must identify and document the causal factors (root causes) of all Incidents.

5.4.4.1 Security Incidents

(82) The Contractor must report all suspected or actual Incidents for Security Breaches.

(83) The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious emails) to contain a Security Breach, protect against cyber threats or address vulnerabilities.

(84) The Contractor must provide results of logs and audit records research associated with a Security Breach, based upon criteria specified by Canada, within 72 hours of a request by Canada.

(85) The Contractor must implement an audit and investigation process for Security Breaches that allows only specific, pre-authorized representatives of Canada to request and receive discrete access and information for the purposes of conducting security investigations.

(86) The Contractor must ensure the use of proper forensic procedures and safeguards for handling Security Breaches that includes:

a) the maintenance of a chain of custody for both the audit information, and

b) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.

(87) During a Security Incident, the Contractor must reduce the standard response time according to the priority of the Security Incident as specified by Canada..

5.4.5 Configuration Management

(88) The Contractor must perform Configuration Management that includes the configuration of the Services to meet the on-going operational requirements of the Services in accordance with Service Orders for Professional Services.

(89) The Contractor must develop, document, and maintain the current baseline configuration of the Services with traceability back to previous versions.

(90) The Contractor must ensure that only authorized Configuration Items are released and/or implemented for the Services.

(91) The Contractor must log each Configuration Item addition, removal or modification where each log entry in a configuration log file.

(92) The Contractor must maintain daily back-ups of the configuration data and store the most recent copies of the daily backups at an off-site location.

(93) The Subscription Service must allow a master tenant configuration whereby this configuration can be inherited and different business rules can be applied by each of the sub-tenants specified by Canada.

5.5 Security and Privacy

5.5.1 Ongoing Security Assessment

(94) The Contractor must provide a), and b) and c), on an annual basis:

a) a SOC2 Type 2 report;

b) evidence that demonstrates current certification for ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and

c) evidence that demonstrates current certification for ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

5.5.2 Service Contingency Plan

(95) The Contractor must ensure that the Service Contingency Plan is:

a) coordinated with organizational elements responsible for related plans including incident handling teams;

b) communicated and distributed to organizational elements involved with executing the plan; and

c) protected from unauthorized disclosure and modification.

(96) The Contractor must notify Canada immediately upon determining that a disaster or other emergency situation has occurred that affects Services. The notification must include the following information: a brief description, date/time, estimated restore time, and impacted SDPs.

(97) The Contractor must test Service Contingency Plan (all processes, procedures, roles, responsibilities etc.) annually as documented in the approved plan, and provide the test results to Canada within 20 FGWDs of completing the testing.

(98) The Contractor must restore Service functions as part of Service Contingency Plan testing. The restoration exercise must not be performed using production Services unless otherwise approved by Canada.

(99) The Contractor must correct any problems to Services identified during the testing of Service Contingency Plan within 60 FGWDs after completion of the testing.

(100) The Contractor must provide to Canada within 40 FGWDs of a Service Request, evidence not more than 12 months old (e.g., test results, evaluations, and audits, etc.) that Service Contingency Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Service Contingency requirements for Services.

5.5.3 Privacy Management Plan

(101) The Contractor must review the Privacy Management Plan annually and provide a report to Canada within 20 FGWDs of completing the review that summarizes the results of the review and proposed changes. The Contractor must update the Privacy Management Plan within 20 FGWDs of Canada's acceptance of the report.

(102) The Contractor must provide to Canada within 40 FGWDs of a request, evidence not more than 24 months old (e.g., test results, evaluations, and audits) that the Privacy Management Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Canada's privacy management requirements.

(103) The Contractor must produce a Vulnerability Mitigation Report after completion of remediation activities completed for a Vulnerability Mitigation Plan that includes:

a) a description of the corrective measures implemented; and

b) proof that associated system documentation has been updated to reflect the changes.

(104) The Contractor must mitigate all security deficiencies found in accordance with Canada's security requirements at no additional cost to Canada as a result of vulnerability testing by the Contractor and Canada..

5.6 Reports and Documents

(105) It is Canada's intention to use existing reports provided by the Contractor where possible as determined by Canada. The exact reports will be determined during consultation with Canada before the completion of Service Readiness.

(106) The Contractor must provide reports in English using the ET time zone.

(107) Information in reports representing numbers and dates must be downloadable as numbers and dates, and not formatted as text.

(108) The Contractor must provide all annual reports within 30 FGWDs of the end of the previous 12 months, based on the anniversary of the Contract.

(109) The Contractor must provide all weekly reports within 2 FGWDs of the end of the previous week where the end of a week is 11:59 pm Friday.

(110) The Contractor must provide all monthly reports within 5 FGWDs of the end of the previous month where the end of a month is 11:59 pm on the last FGWD of the month.

(111) The Contractor must provide Canada with all reports provided to other clients of the Contractor for Services using Canada Data.

(112) The Contractor must provide the Service Operations reports summarized in Table 3 according to frequency, purpose, and description.

Table 3. Service Operations Reports

Report Name	Service Management Summary Report
Frequency	Scheduled, Monthly
Purpose	The report must present a summary of the Contractor's performance in delivering the services and meeting Service Level Targets (SLTs).
Description	The report must include: a) total number of Incidents and the total number of SLT exceptions for the monthly period; b) list of all Incidents for the monthly period organized by type, priority, and SLT, identifying Incident Ticket numbers and escalation levels invoked; c) list of SLT exceptions for the monthly period identifying the SLT for each exception and the amount by which the SLT was missed (applies to all types of SLT exceptions whether or not there is an associated Incident Ticket); d) description of the recommendations, corrective actions and timeframes to implement any required changes to resolve chronic Problems or service degradation and/or prevent future SLT exceptions; e) description of Incidents and issues related to the Contractor's services such as the Service Portal and its associated systems, tools and applications (e.g., CMDB, reporting, etc.), including the corrective actions and timeframes to resolve them; f) Service Requests completed/pending; g) Change Requests completed/pending
Report Name	Service Request and Change Request Report
Frequency	Scheduled, Monthly
Purpose	The report must present a detailed summary of all Service Requests planned or completed during the reporting period.
	The report must include: a) Service Requests closed for the weekly period b) Service Requests pending execution c) Change Requests closed for the weekly period, including the following: d) Change Requests pending execution, including the following:
Report Name	Post-Incident Report
Frequency	On-Demand, Within 2 FGWDs of Canada's request
Purpose	This report must provide Canada with an in-depth understanding of any Incident that Canada considers to have had a significant impact on its business. The report must clarify exactly what occurred during the Incident, including the Contractor's actions, as

	well as the Contractor's plans to address any potential recurrence.
Report Name	Post-Change Request Report
Frequency	On-Demand. The FGWD immediately following the execution of any Emergency Change Request and/or within 5 FGWDs of a failed Change Request or Service Release
Purpose	The report must provide Canada with an in-depth understanding of a failed Change Request, or an Emergency Change Request.
Report Name	Post-Service Request Report
Frequency	On-Demand, The FGWD immediately following the execution of any Emergency Service Request and/or within 5 FGWDs of a failed Service Request
Purpose	The report must provide Canada with an in-depth understanding of a failed Service Request, or an Emergency Service Request.
Report Name	Service Release Summary Report
Frequency	Scheduled, Monthly
Purpose	Summary of Service Release Activity
Description	The report must include, for each Service Release in the preceding month: a) time and date of the Service Release; b) purpose of the Service Release; c) description of Service Release activities; d) Enterprise Contact Centre Services components affected; and e) lessons learned (if Service Release failed).
Report Name	Service Ticket Report
Frequency	Real time, as required.
Purpose	A User-definable report that must provide access to Incident Tickets, Problem Tickets, Change Request Tickets and Service Request Tickets based on ticket type selected by Canada and any ticket field over a time period selected by the User..
Description	The report generator must provide: a) ability to search, sort and view tickets; b) ability to download ticket query results using a file naming convention specified by Canada and COTS file format; c) ability to view individual tickets (all fields) in a hierarchical tree fashion where information within a ticket can be viewed in a successive "drill-down" manner (i.e., related tickets) by selecting hyperlinks;

	d) cumulative report detailing for each ticket in the query results: the ticket number, date, priority, associated tickets (where applicable), impacted Enterprise Contact Centre Services, outage time, detailed description of ticket; e) direct access to the CIs from the CMDB involved by selecting a hyperlink in the ticket; and f) ability to generate open or closed ticket summary information, displayed in graphical and tabular format, by year, month, day and hour intervals for number of tickets, and number of tickets by priority level.
Report Name	Privacy Summary Report
Purpose	Personal information that is collected, used, disclosed, retained or disposed of as part of Services
Frequency	Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December)
Description	The report must include the following information: a) a description of any new measures taken by the Contractor to protect the Personal Information (e.g. new software or access controls being used by the Contractor); b) a description of any changes made to the software, the access controls and the operating procedures, which may have privacy implications; c) a list of any corrections made to Personal Information at the request of Canada on behalf of an individual (including the name of the individual, the date of the request, and the correction made); d) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; e) a list with details of any privacy breaches; and a complete copy (attached annex to the report, in a file format specified by Canada) of all the Personal Information stored electronically by the Contractor.
Report Name	Personal Information Report
Purpose	This report must provide a summary of activities for Personal Information
Frequency	Quarterly
Description	The report must include: a) description of any new measures taken by the Contractor to protect the Personal Information (eg. new software or access controls being used by the Contractor); b) description of any changes made to the software, the access controls and the operating procedures, which may have privacy implications; c) list of any corrections made to Personal Information at the request of Canada on behalf of an individual (including the name of the individual, the date of the request, and the correction made); d) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; and

	details of any privacy breaches of Personal Information.

5.7 Service Level Targets

(113) The Contractor must monitor, measure, calculate, and report on SLTs 7 days per week, 24 hours per day, 365 days per year, unless otherwise indicated for a specific SLT.

5.7.1 Outage Time

(114) Outage time for a Service begins from the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada, whichever occurs first. The outage time used in the calculations ends when the affected Service is fully restored for the Incident.

(115) The Contractor's lack of proper security clearance (for itself or its personnel) does not excuse it from its obligation to restore the affected Service within the SLT.

(116) In cases where Canada attempts to report an Incident for an outage but the Contractor's Service Desk does not answer the call, the start time for the outage begins at the time Canada placed the call to the Service Desk.

(117) The following events may, with Canada's approval, be excluded from the calculation of outage time for a Service during a review of the Incidents associated with the outage:

a) failure related to a Security Incident where Canada has approved mitigation actions that impact the availability of CCaaS;
b) failure of another Service;
c) scheduled downtime;
d) failure of a Canada Service, including data received from the Canada Service;
e) suspension of Incident Ticket;
f) a Canada Service does not provide sufficient capacity.

5.7.2 Service Level Target for Service Availability

The Service Level Target Service Availability (SLT-SA) for the Subscription Service must be greater than or equal to 99.900%.

(118) The period of measure for SLT-SA is a calendar month (7/24); therefore the total number of minutes in the measurement period will vary based on the number of calendar days in the month.

(119) The Contractor must calculate SLT-SA as follows: ((measurement period – sum of the outage times) / measurement period) x 100.

(120) The outage time for Incidents where a Service does not function in accordance with the Service Design must be included in the calculation of the SLT-SA for that Service.

(121) The outage time for any of the Incidents defined in CCaaS Annexes must be included in the calculation of the SLT-SA for the Service.

(122) The outage time for any of the following Incidents must be included in the calculation of the SLT-SA for Subscription Service:

a) 1 or more Interaction Priority Queues are unable to process Communication Channels interactions as implemented;
a) Real-Time or Historical Reporting is not available for use by Canada;
b) 2 or more Subscription Service Users are unable to register a change of Status; and
c) 1 or more Supervisors are unable to access Subscription Service via their Web browser.

5.7.3 Service Level Target for Service Desk Response

(123) The Service Level Target for Service Desk Response (SLT-SDR) is that the Contractor's Service Desk must answer 80.0% of all telephone calls placed by Canada within 20 seconds. The period of measure for SLT-SDR is the calendar month.

(124) The SLT-SDR must be calculated as follows:

(125) ((number of calls answered within 20.0 seconds + number of calls abandoned within 20.0 seconds) / (total number of calls answered + total number of abandoned calls)) x 100

(126) The calculation of time to answer a call by the Service Desk begins when a caller starts waiting in queue for a Contractor's Service Desk agent and ends when the Contractor's

(127) Service Desk agent, a live person, answers the caller. Although the Contractor may use voice scripts and menu options acceptable to Canada, the calculation of time to answer a call excludes any time spent by callers listening to and making menu selections in the Contractor's Interactive Voice Response system prior to waiting in queue for the Contractor's Service Desk agent. An abandoned call to the Service Desk is a call that is connected to the Contractor's telephone system but that the Calling Party terminates before a Service Desk agent answers the call.

5.8 Analytics

(128) Contact Centre data (including but not limited to outbound calling, workforce management, service request, incident, release, change, audit data, agent data, CCaaS performance data, IVR utilization, queue data, call data) must be provided to Canada in a format defined by the Contractor in consultation with Canada and subject to Canada's acceptance, as and when required, at no cost to Canada.

(129) Data to be provided at the level sufficient to support invoicing and audit requirements upon Canada request.

(130) Data to be provided at the level sufficient to support internal chargeback requirements upon Canada request.

5.9 Equivalency Arrangements

5.9.1 Product Roadmaps

(131) Canada acknowledges that each Party benefits from open communication. Included in the fees paid to the Contractor, the Contractor shall provide Canada with subject matter expertise support to assist in assessment of product release material including online demo support, user interface impacts, training needs analysis and technical support. This will allow Canada to communicate functional capability enhancements to Government users.

(132) Release material must be provided unfiltered to Canada.

(133) On an annual basis (September 30) and upon Canada request, the Contractor must provide the IP Owner's most current roadmap of anticipated product enhancements/upgrades and anticipated delivery dates. The roadmap shall include functional capabilities in as much detail as requested by Canada. Potential pricing must be identified.

5.9.2 Forums

(134) The IP Owner shall provide Canada with access to the user community such as online message boards, newsgroups, chat rooms, support (technical and troubleshooting), Wikis, blogs and/or other interactive forums that can be accessed and contributed to by certain registered users of Canada. The level of access granted to these communities, as well as toll free telephone support, will be at an equivalent service level as if Canada had contracted directly with the IP Owner.

5.9.3 Support

(135) In the event of an underlying system issue with the service provided by the IP Owner, at the discretion of Canada, the Contractor will include Canada in all interactions with the IP Owner including, but not limited to, meetings, records of decision, and correspondence relating to opening of ticket(s), root cause analysis, resolution/rollback plan and status updates against the plan.

(136) The Contractor shall ensure that IP Owner is bound, and will abide, by the terms for the functional capability outlined in this statement of work. For greater clarity, the level of support provided by the Contractor to the Contractor shall be no less than the level of support provided by the Contractor to Canada.

6 SUBSCRIPTION SERVICE

To be completed for each Requirement.

7 VOICE SERVICES

To be completed for each Requirement.

8 WORK DELIVERABLES

To be completed for each Requirement.

9 TRAINING

To be completed for each Requirement.

10 PROFESSIONAL SERVICES

To be completed for each Requirement