General Requirements, Security Requirements, Manpower Requirements and Technical Requirements

1. General Requirements

1.1 All Add-on Government Public Cloud Services (GPCS) offered shall include but not be limited to the following set-up measures:

1.1.1 Be a secure and reliable 24 x 7 (24 hours a day and 7 days a week) non-stop service.

1.1.2 Built-in with the resilience that the switch-over operation be performed in an automatic manner and be transparent to the Government.

1.1.3 Built-in with the business continuity capability and be resided in a minimum of two different geographic sites to avoid service outage during disaster situations.

1.1.4 Provide usage management capability where service usage can be monitored, controlled and/or reported.

1.2 All Add-on GPCS offered shall include but not be limited to the following implementation measures:

1.2.1 Be designed for business use and be interoperable and compatible with the existing hardware, software, networking devices mentioned in the Specifications document by the respective user Government bureau/department.

1.2.2 Comply with the Government Interoperability Framework.

(Detailed description of the Government Interoperability Framework can be found at the Government web site – https://www.digitalpolicy.gov.hk/en/our_work/data_governance/policies_standards/interoperability_framework/index.html).

1.2.3 Built-in with the capability that no user data loss or loss of user data access after service disruption.

1.2.4 Provide the capability for handling Government's orders with minimal or no Contractor's human interaction.

1.2.5 Support rapid and elastic service provisioning and de-provisioning, such that the service being provisioned or de-provisioned often appear to be unlimited and can be purchased in any quantity at any time.

1.2.6 Provide dedicated support resources to the Government in relation to the provisioning of the Add-on GPCS.

1.2.7 Provide an exit plan to the Government within one month after the implementation of

the Add-on GPCS.

1.2.8 Report any critical incident to the Government within four hours after it has occurred.

1.2.9 Complete any non-critical incident or provide reasonable explanations within five working days after it has occurred.

1.2.10 Provide a solution or work-around in response to a helpdesk enquiry within 24 hours after it has been raised by the Government.

1.3 On request by B/Ds and where applicable, the Add-on GPCS offered shall include but not be limited to the following additional implementation measures:

1.3.1 Support the Hong Kong Supplementary Character Set (HKSCS) published by the Government.

(Detailed description of HKSCS can be found at HKSCS: https://www.digitalpolicy.gov.hk/en/our_work/data_governance/policies_standards/ccli/hkscs/)

1.3.2 Support the ISO 10646 standard and the HKSCS coded in the ISO 10646 standard.

(Detailed description of ISO 10646 and HKSCS can be found at ISO 10646: https://www.digitalpolicy.gov.hk/en/our_work/data_governance/policies_standards/ccli/iso_10646/)

1.3.3 Support provisioning of practically scalable storage, network bandwidth, computing power and memory.

1.3.4 Provide documented procedures, Application Programming Interfaces (APIs) or other electronic means for the Goverrnment Representatives to export or extract their corresponding user data any time.

1.3.5 Have the capability for the Government Representatives to perform the corresponding user data migration, and data destruction upon expiry, completion or termination of the Contract, or requested by the Government.

2 Security Requirements

2.1 All Add-on GPCS offered shall include but not be limited to the following set-up measures:

2.1.1 Store all user data processed by the Add-on GPCS in data centres accredited with one or more International standards in information security management like ISO/IEC 27001, or audited with the Statement on Standards for Attestation Engagements

(SSAE) No. 16 or equivalent, where applicable.

2.1.2 Enable password protection on per user, user group or role basis to protect the access to the Add-on GPCS with one or more of the following measures to be implemented:

- Anti-password guessing mechanism
- Configurable timeout period
- Password aging

2.1.3 Have the anti-virus service enforced to protect the Government against virus, worms, Trojan horses, spyware and malicious code, etc., wherever applicable.

2.1.4 Ensure the anti-virus service to be run with the most appropriate or up-to-date list of virus signatures.

2.2 All Add-on GPCS offered shall include but not be limited to the following implementation measures:

2.2.1 Comply with the Baseline IT Security Policy (S17). The following guidelines shall also be followed as appropriate:

- Baseline IT Security Policy (S17)
- IT Security Guidelines (G3)
- Practice Guide for Security Risk Assessment & Audit (ISPG-SM01)
- Practice Guide for Information Security Incident Handling (ISPG-SM02)
- Practice Guide for Mobile Security (ISPG-SM03)
- Practice Guide for Cloud Computing Security (ISPG-SM04)

These policies and guidelines are accessible through the following URL: (https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/information_cyber_security/government/)

2.3 On request by B/Ds and where applicable, the Add-on GPCS offered shall include but not be limited to the following additional implementation measures:

2.3.1 Be processed under an end-to-end encryption environment and/or as required by the Specification on IT security.

2.4 The Contractor shall include but not be limited to the following implementation measures:

2.4.1 Not disclose any data or information relating to Add-on GPCS to any external parties and not use those data or information for other purposes.

2.4.2 Report any vulnerability, its resolution and/or any workaround to the Government, if a security vulnerability is reported on the Add-on GPCS.

2.4.3 Resolve the vulnerability as soon as technically feasible, without any charges to the Government.

2.4.4 Acquire at its own cost to engage a third party to perform annual security risk assessment and audit exercise once every year after the contract award on all Add-on GPCS offered, to ensure its compliance with the prevailing government security standards.

2.4.5 Submit an annual reports on security risk assessment and audit exercises to the Government for review and record

2.4.6 Obtain the Government's prior approval to use other equivalent documents or reports or certifications as an alternative to proving its compliance with the prevailing government security standard, if the Contractor chooses not to engage a third party to perform the annual security risk assessment and audit exercise as specified in 2.4.5.

General Requirements, Security Requirements, Manpower Requirements and Technical Requirements

3 Manpower Requirements

3.1 The Contractor shall deploy a team of professional staff conforming to the requirements stipulated in Section 3.2 to carry out the contractual obligations. The staff shall be full-time employees of the Contractor and shall only be engaged in one function. The qualification and experience of the staff member will be counted up to the application date for inclusion in the List of GPCS Providers. The minimum number of staff members to be deployed under each Service Category is as follows.

i) Service Category (A) Productivity Apps

Function*	*Minimum No. of Staff Members Required*	*Staff Category**
Service Manager	1	Category 2
Service Specialist	1	Category 1

ii) Service Category (B) Business Apps

Function*	*Minimum No. of Staff Members Required*	*Staff Category**
Service Manager	1	Category 2
Service Specialist	1	Category 1

iii) Service Category (C) Cloud IT Services

Function*	*Minimum No. of Staff Members Required*	*Staff Category**
Service Manager	1	Category 2
Service Specialist	1	Category 1

iv) Service Category (D) Social Media Apps

Function*	*Minimum No. of Staff Members Required*	*Staff Category**
Service Manager	1	Category 2

Service Specialist	1	Category 1

*: Requirements for each staff category and their functions are provided in Section 3.2 below.

3.2 The qualifications of each staff category are defined below:

Staff Category	**Qualifications**	**Function**
Category 1	At least **six** years of IT experience including at least **two** years of experience in the relevant function	Service Specialist
Category 2	At least **ten** years of IT experience including at least **three** years of experience in the relevant function	Service Manager

Notes:

a) Only full-time involvement in IT job positions like project manager, technical support manager, service manager, product manager, systems analyst, system consultant, system specialist, product consultant, service consultant, service specialist or equivalent is counted as IT experience. The following cases are not counted as IT experience:

- Time spent on full-time undergraduate or full-time postgraduate programmes;
- Time spent on sandwich training in full-time undergraduate or full-time postgraduate programmes;
- Sales or marketing of IT related products and services; and
- Teaching of IT related subjects.

b) Only the full-time involvement in the following duties and responsibilities is counted as the past experience in the relevant function:

Service Manager	■ Adequate resources are planned and managed leading to the deployment of the required services ■ Correct decision is made in resolving technical issues arising from users when they use the services ■ Good quality control and quality assurance are performed on the deployed services
Service Specialist	■ Detailed user requirements are analyzed and interpreted, and details of the required services are recommended to users ■ Comprehensive system testing and user acceptance are prepared and conducted on the deployed services ■ Appropriate technical advice are provided to users on using the deployed services

General Requirements, Security Requirements, Manpower Requirements and Technical Requirements

4 Technical Requirements

The following summarizes the mandatory requirements as stipulated under Section 3 of Appendix A for ease of reference by respondents.

4.1 For Service Category (A) Productivity Apps – Office Tools and Suites, the following requirements shall be satisfied:

- Provide web-based office suite which includes functions for word processing, spreadsheet calculation and creating presentations over the Internet
- Provide functions for viewing, sharing and editing of files directly via web browsers on PCs or mobile devices
- Provide online storage and access control for the stored files
- Provide service availability for the month : >=99.5%
- Provide storage size: at least 1GB per user

4.2 For Service Category (A) Productivity Apps – Document and Content Management, the following requirements shall be satisfied:

- Provide online storage for sharing documents and contents
- Provide content management functions such as version control, access control, retention policy and generation of audit report on the stored documents
- Provide functions for administration and management of user accounts
- Allow sharing, managing and searching for information and resources with restricted permission control
- Provide service availability for the month : >=99.5%
- Provide storage size: at least 1GB per user

4.3 For Service Category (A) Productivity Apps – Collaboration, Meetings, Conferencing, the following requirements shall be satisfied:

- Provide audio and visual transmission of meeting activities over the Internet
- Provide web conferencing to deliver presentation, share documents and whiteboards with meeting attendees
- Provide instant messaging or text chat functionalities between attendees
- Provide service availability for the month : >=99.5%
- Support at least 10 attendees per meeting/conference

4.4 For Service Category (B) Business Apps – E-mail, the following requirements shall be satisfied:

- Provide e-mail, calendar, contacts and task management with the most current anti-virus and anti-spam protection over the Internet
- Provide functions for users to create and maintain contact information
- Provide functions for user account management (e.g. rules for filtering and forwarding)
- Support for Post Office Protocol (POP) client connectivity for use with other e-mail clients
- Provide service availability for the month : >=99.5%

- Provide storage size for e-mails: at least 15GB per e-mail box

4.5 For Service Category (C) Cloud IT Services – Backup and Restore, the following requirements shall be satisfied:

- Provide backup and restore of data over the Internet
- Provide scalable and reliable data backup storage infrastructure
- Provide configurable schedule backup functionality
- Support various backup modes including full backup and incremental/differential backup
- Support data backup in compressed mode
- Provide encryption of backup data to ensure data security
- Provide integrity checking of backup data to ensure data integrity
- Support backup of common database (e.g. MS SQL Server, Oracle, MySQL), e-mail, document servers (e.g. MS Exchange, Lotus Domino/Notes) or file systems (e.g. Windows, Linux)
- Provide backup report in e-mail, web site or other electronic means to notify users of the status of backup including details of any backup failure and errors detected
- Provide statistics reports or other electronic means on the performance and usage
- Provide multiple versions of backup
- Provide service availability for the month : 99.5%
- Provide storage size: at least 1TB per user
- Provide Bandwidth: at least 50Mbps

4.6 For Service Category (D) Social Media Services – Photo Hosting/Sharing, the following requirements shall be satisfied:

- Provide functionality for the Government to share photos with the public over the Internet
- Provide option for Government users to control the privacy of photos
- Provide functionality for Government users to manage the photos
- Allow Government users to group photos into different albums
- Provide service availability for the month : >=99.5%
- Provide storage size: at least 20GB
- Support photo size: at least 15MB

4.7 For Service Category (D) Social Media Services – Video Hosting/Sharing, the following requirements shall be satisfied:

- Provide functionality for the Government to share videos with the public over the Internet
- Provide option for Government users to control the privacy of videos
- Provide functionality for Government users to manage the videos
- Allow Government users to define set of searching keywords for the videos
- Support at least 2 of the following video file formats: Third Generation Partnership Project file format (3GPP), Audio Video Interleave (AVI), Flash Video (FLV), Matroska (MKV), QuickTime multimedia file format (MOV), MPEG-4 Part 14 (MP4), Moving Picture Experts Group (MPEG), Windows

Media Video (WMV) ■ Provide service availability for the month : >=99.5% ■ Provide storage size: at least 20GB ■ Support video size: at least 1GB

- End of Appendix C -