Bell Acceptable Use Policy for G-Cloud 15 Framework (RM1557.15)

Creation Date: 20/01/2026

Contents

Applicability

This document is provided for the purposes permitted under the Crown Commercial Service G-Cloud 15 Framework (RM1557.15).

This document applies only to the extent that, and insofar as, its terms are consistent with and permitted by the RM1557.15 Framework agreement, the CCS General Terms, the Joint Schedules and the applicable Call-Off Contract.

In the event of any conflict or inconsistency, the RM1557.15 Framework agreement and the applicable Call-Off Contract shall prevail, and any conflicting provision of this document shall be disapplied.

1. Purpose

The purpose of these policies is to outline the responsibilities and acceptable use of Bell's IT assets and provide clarity on the required and expected behaviours by Bell to protect the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Scope

This policy applies to all Bell employees, agents, contractors, consultants, business partners or any other third party (referred to in this document as 'users') who have access to IT assets (all information systems, hardware, software and channels of communication) and to all information and data relating to Bell, it's personnel and other organisations with whom it deals. It covers the appropriate and legal use of these technologies and resources that are made available to users.

1.2 Intended Audience

This policy is intended for all Users with access to Bell information and assets. Where visitors and other third parties are on-site at a Bell location, the Bell host must ensure that their visitor is aware of anything pertinent to their visit and that they comply with the policy requirements.

2. General Principles

2.1 Acceptable Use

The user will:

- Use information, systems, and equipment in line with Information Security Management Policies.
- Be responsible for the security of their passwords and accounts in line with the Password Management Policy.
- Only use IT assets or have access to data or information needed to perform their role.
- Only share content with relevant personnel using approved and secure mechanisms, including transferring data outside of Bell.
- Ensure all information that is created, used, and disposed of, is in line with business needs and is compliant with Information Classification and Handling Policy.
- Protect confidentiality if the message or document is confidential and/or contains sensitive information.
- Consider the confidential or sensitive nature of any discussion when using a device, landline, or instant messaging tool outside of the Bell network. This will include anything that should not be discussed in an open domain or would be in breach of a Non-Disclosure Agreement.
- Be careful not to be overhear or overlooked in public areas when conducting Bell business.
- Use authentication software to verify who they are on any Bell device or to access the Bell network. This may require installing an authenticator app on a personal device.
- Keep data storage to a minimum, deleting/archiving obsolete files or emails on a regular basis in line with the Data Retention Schedule or when they are no longer useful.
- Immediately report any breach of this Information Security User Policy to their line manager or HR and comply with official procedures when a breach of the policy is suspected or reported.
- Maintain all Company equipment in appropriate condition in line with the Acceptable Use Policy.

2.2 Personal Use

The user will:

- Exercise reasonable judgement regarding personal use of business devices.
- Understand that they are personally accountable for what they do online and with Bell technology.
- Limit personal communication so that is does not interfere with the performance of official business duties, infringe on the law or on other company policies.
- Ensure that stored personal information is appropriate i.e., legal, appropriate, and compliant with this policy.
- Ensure activities do not damage the reputation of Bell and its personnel including accessing, storing, transmitting, or distributing links or material that:
    - Could embarrass or compromise Bell in any way

- Violates copyright laws or breach terms of licencing agreements
- Could constitute as bullying or harassment
- Is considered indecent or obscene, including images and literature

2.3 Unacceptable Use

The user will not:

- Use IT assets for on-line gambling while using Bell accounts and/or systems during company business, without prior permission from the Human Resources Director, excluding the National Lottery Syndicate and Fantasy Football.
- Broadcast unsolicited personal views on social, political, or other non-business-related matters.
- Solicit to buy or sell goods or services unrelated to Bell.
- Provide unauthorised views or commitments that could appear to be on behalf of Bell.
- Use our company email, username and password as their login to any external sites or software that is not related to Bell business use.
- Attempt to compromise or gain unauthorised access to Bell IT systems or data or prevent legitimate access to it.
- Use any type of applications and/or devices to circumvent management or security controls.
- Perform any unauthorised change to Bell information or assets.

2.4 Use of Email

The user will:

- Comply with Bell expectations for written communications, with regards to style, content, appropriate language and presentation of a message.
- Acknowledge that offers or contracts transmitted via e-mail are as legally binding to Bell as those sent on paper. All legally binding agreements must be approved by Legal or HR and use appropriate tools (within Bell this is DocuSign).
- Exercise caution when forwarding any internal Bell emails to an outside network.
- Only use customer email accounts to share Bell data classified as public.
- Only ask for access to other users email for a limited time to extract business related information.
- Not impersonate another user or create / send material designed to mislead people about the originator or who authorised it.
- Not send chain mail or engage in mass transmission of unsolicited emails (SPAM).
- Be aware of and do not respond to content that is phishing for any personal details.
- Report any suspicious emails to the Service Desk.
- Not create any external email forwarding, if required raise a service desk request.

2.5 Use of Internet and Social Media

The user will:

- Only access appropriate content using Bell technology.
- Not use personal social media account for work purposes other then for promoting Bell offerings with appropriate authority.
- Avoid giving information which could inadvertently provide unauthorised access to personal or sensitive data and consider any Artificial Intelligence tool before submitting corporate information in line with our IT18 – Artificial Intelligence Policy.
- Be aware that any information submitted to social media sites should be regarded as published information.
- Only post from a Bell email address to newsgroups if it contains a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bell, unless posting is for business duties.
- Not participate in personal communication with company credentials e.g. chat rooms, “blogging”.
- Not create and/or operate a personal web site in company time or with company credentials.

2.6 Use of Software, Devices and Networks

The user will:

- Only use systems, applications, software and devices which are approved when undertaking business, therefore not loading software from unapproved sources. Please refer to IT09 – Operations Security Policy.
- Request all software, for internal use, via a ticket in ServiceNow. This will enable it to be purchased, packaged and managed by the Internal IT department.
- Not knowingly or carelessly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Not deliberately or recklessly introduce malware or viruses.
- Not introduce IoT devices to the network without approval from Internal IT.
- Not connect unauthorised devices to the company network, including USBs.
- Ensure no AI processes corporate data without approval from Internal IT.
- Not access Bell data using an un-managed device.
- Ensure sensitive company and personal identifiable information is not stored or transferred without password protecting documentation.
- Not store Bell data on any un-managed device or unauthorised cloud solution.
- Ensure unauthorised personnel are not allowed access to a Bell device.
- Ensure all devices are locked when leaving a device to prevent unauthorised usage.
- Be responsible for all Bell devices assigned to them, keeping them safe and secure. This means, protecting Bell devices while travelling, carrying laptops as hand luggage and never leaving a device in sight within a parked vehicle.

- Not use applications to misrepresent your actual location, or to present them as being in another country. Applications and/or devices must not be used to bypass company security controls, locations restrictions, or audit requirements.
- Ensure all Bell hardware must be maintained in its original condition and must not be altered in any way, including the addition of personal stickers or markings.
- Immediately report any loss or damage of equipment to their line manager and Service Desk. If damage to devices occurs repeatedly, charges may be incurred.
- Return any Bell devices to the line manager or local office when leaving the company, with the line manager completing all necessary exit procedures with the leavers.
- Assist IT in ensuring installed software is appropriately maintained and updated when required.

2.7 Monitoring

Where permitted, Bell reserves the right to inspect, review, store or retrieve data to respond to requests for information or monitor employee's use of the IT assets for the purposes of:

- Investigation, detection and prevention of infringement of the law, this policy or other Bell policies.
- Investigation of alleged misconduct by employees.

Failure to comply with any procedure in Bell's Acceptable Use Policy may result in action being taken against the user under the Disciplinary Procedure, up to and including termination, depending on the circumstances.

3. Password Management

Passwords should be known only to the person responsible for the account and is the first line of defence for Bell IT systems. If an account or password is suspected to have been compromised, it should be immediately reported as a security incident with the Service Desk and the password changed.

All Bell users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Yous password must:

- Have a minimum length of 12 characters
- Contain characters from three of the following four categories:
    - English uppercase characters (from A through Z)
    - English lowercase characters (from a through z)
    - Base 10 digits (from 0 to 9)
    - Non-alphanumeric characters (for example: !, $, ~, or %)
- Be changed every 90 days

Mobile Devices / BYOD

Password management is just as important when securing mobile devices and users as outlined above should adhere to the following conditions.

Your passcode must:

- Be protected by a 6-digit passcode on a phone or personal device.
- Be alphanumeric, accepting all numbers or all letters or a combination.

Keeping your password safe

Here is a list of “don’ts”:

- Don’t reveal a password to ANYONE.
- Don’t write down a password or store them where they are open to theft.
- Don’t store a password in a computer system without encryption.
- Don’t sent it in an email or message.
- Don’t use part of your username within the password.
- Don’t use the “Remember Password” feature of applications (e.g. Internet Explorer, Firefox).
- Don’t use the same password to access different Bell systems.
- Don’t use the same password for systems inside and outside work.

4. Clear Desk and Clear Screen

- Users must safeguard sensitive information from unauthorised access, loss or damage.
- Users must secure their workspace whenever absent from their desk. Secure workspaces by:
    - Cleaning desktops and work areas
    - Locking documents (classified as Commercial and above) in a drawer when not in use. They must not be left unattended on desks, meeting rooms or printers.
    - Retrieving documents from printers.
    - Disposing of documentation as per the Information Classification and Handling Policy.
    - Locking the workstation, mobile device or other media when it is unattended to activate password protections.
    - Locking the laptop or other devices in a drawer at the end of the working day if leaving devices in the office.
    - Erasing restricted and/or confidential information on a whiteboard.
    - Closing or locking filing cabinets that contain confidential information when not in use or unattended.
    - Storing keys for access in a dedicated key safe and not left in or on an unattended desk. Keys for pedestals must be the responsibility of the key owner to keep safe.
- Users must ensure their screen is not visible to unauthorised personnel when accessing information classified Commercial and above.

Regular and ongoing Clear Desk, Clear Screen spot checks will be undertaken to ensure continued compliance with this policy.

5. Remote and Mobile Working

Remote working allows users to work as home, on the road or in a satellite location for all or part of the working week where users will be bound by the terms of this policy, ensuring care and compliance at all times.

- All users agree to the proper use, care, maintenance and safekeeping of information assets and allocated devices.
- Users are aware of the additional risk associated with remote working (including the likelihood of theft of equipment or accidental unauthorised exposure of confidential or sensitive information).
- Users working arrangements are compliant with legal and regulatory requirements (e.g. Health and Safety laws and Data Privacy regulations).
- Any cases for working in a different country from your contracted location must be agreed with Human Resources and your line manager.
- Users will be responsible for ensuring that all IT remote working kit is packaged securely ready for collection or is dropped off and handed over to an agreed member of IT when returning IT assets.

Any user found to have violated tis policy may be subject to disciplinary action, up to and including termination of employment.

The user will:

- Take all reasonable care to assess the risks in their given environment they are remote working to prevent the theft or loss of portable devices.
- Not leave the device unattended for any reason unless the session is “locked”, and it is in a safe working place.
- As far as possible ensure they are not observed and information such as passwords are not compromised.
- Ensure that data on a device is kept to a minimum and all company data is saved within Bell approved applications.
- Take all precautions necessary (e.g. store documents in correct file locations) to secure confidential or sensitive data especially if remotely working from public locations.
- Validate that only secured Wireless (Wi-Fi) connections are utilised. If you are unsure of the connection is secure, always use the VPN so the connection is protected.

5.1 Mobile Devices

Bell offers access to Microsoft 365 suite on company mobile and BYOD devices.

The user will:

- Allow the installation of Intune and Multi Factor Authentication (MFA) to connect directly to the Bell network. Intune Company Portal can be downloaded from the Appstore, company devices may already have this pre-installed.
- Never store confidential or sensitive information, such as financial reports or personal data.
- Only install software from approved sources on company phones (additional apps can be requested through the ServiceNow portal).
- Be personally liable for all in Appstore purchases.
- Be responsible for ensuring your device is compliant to the latest operating systems. Access may be revoked if you are no longer on a supported operating system.
- Not take devices, which contain cameras or methods of communications that are not permitted in an ADISA secure processing area.

Bell shall reserve the right to undertake monitoring of telephone or data usage by users on company phones.

Corporate Mobile Data Usage

- Your mobile phone is primarily to be used for work purposes – do not connect to personal devices.
- You must nor use corporate data from your phone as a tether, as per the Hybrid Working Policy HR19, if you don't have adequate broadband then you need to go into your link office or provide your own solution.

Device Disconnection

- The company reserves the right to disconnect devices or disable services without notification.
- The device will be remotely wiped and rest to factory settings if:
    - The device is lost
    - The user enters the wrong passcode after 10 failed attempts
    - The user of a company phone terminates his or her employment
    - IT detects a data or policy breach, a virus, or similar threat to the security of the company's data and technology infrastructure
    - The device becomes rooted (Android) or jailbroken (iOS) either intentionally or unintentionally
- Lost or stolen devices must be reported to Bell immediately or within 24 hours. Additionally, if it is a personal device, users are responsible for notifying their own mobile carrier upon loss of a device.

Travel Abroad

- Users should confirm mobile use abroad is reasonable and necessary to avoid incurring significant costs and that is has been authorised by the line manager.
- The user must log a request using the ServiceNow portal before travelling, both to optimise costs and provide the appropriate bundle that may be required for use as well as ensure we can support you while abroad.

5.2 Bring Your Own Device (BYOD)

The use of a personally owned device in connection with Bell business is a privilege granted to device owners. BYOD devices adhere to the same policies outlined above for both mobile device and remote working, unless clearly stated. It is the responsibility or the Bell user to ensure their personal device meets the required minimum-security standards below.

The user will:

- Assume full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Consider insuring the device and advise the insurer that the device will be used for work purposes at home and office locations.
- Advise Service Desk if you decide to sell, recycle, give away or change your device.
- Always be expected to use their personal devices in an ethical manner whilst using it for business purposes and therefore adhere to the company's Acceptable Use Policy.
- Be personally liable for all costs associated with the device unless agreed with Line Manager beforehand.
- Ensure that their BYOD devices are protected with active anti-virus software and current operating systems.
- Acknowledge that while IT will take every precaution to prevent the user's personal data from being lost in the event it must enact a remote wipe of a device, it is the user's responsibility to have additional precautions for personal data, such as ensuring data is backed up and that you secure and encrypt your phone appropriately using the facilities on the device.
- Not reconfigure a remote worker's equipment for split-tunnelling or dual homing, this is not permitted at any time.
- Ensure that their devices meet these specifications and comply with our policies.

What Bell can see or do on your device:

- View model, serial number and operating system
- Identify your device by name
- Reset lost of stolen device to factory settings
- View information collected by corporate apps and networks

What Bell cannot see or do on your device:

- View browsing history
- See your personal emails, documents, contacts or calendar
- Access your passwords
- View, edit, or delete your photos
- See the location of the device

Bell reserves the right to request access to inspect or delete company data held on a personally owned device to the extent permitted by law and for legitimate business purposes. It may also revoke Bring Your Own Device privileges without notice.

5.3 Bell IT Responsibilities

IT is responsible for ensuring that remote working, mobile and BYOD devices all adhere to company policies.

- Devices must be configured with a secure password that comply with the Bell Password Management Policy.
- Company laptops only connect to Bell network and services through an encrypted connection, either via Microsoft 365 native encryption or via a secure VPN client if not on the Bell network.
- All company and end user devices must be encrypted and will require two factor authentication to set up the device.
- Company owned laptops must be protected by a firewall and anti-virus software that is current and up to date, including patching with the latest manufacturers' updates.
- Organisations or individuals who wish to implement non-standard Remote Access solutions to the Bell production network must obtain prior approval from the IT Department.
- Non-standard hardware configurations for company devices must be approved by the IT Department.
- These policies will be enforced by the IT Department using Device Management software.

6. General Obligations

Users having access to the Bell Information for Bell's customer information, are responsible for:

- Complying with this policy and any associated policies.
- Maintaining vigilance and reporting security-related incidents and possible breaches of this policy to the IT Service Desk and notifying their manager in cases involving personal data, in accordance with Bell's Data Protection Policy.
- Reading and familiarising themselves with this policy and related standards, procedures and guidance that are appropriate to their roles.

Data Processing Agreement

This document is provided for the purposes permitted under the Crown Commercial Service G-Cloud 15 framework (RM1557.15).

This document applies **only to the extent that, and insofar as, its terms are consistent with and permitted by** the RM1557.15 framework agreement, the CCS General Terms, the Joint Schedules and the applicable Call-Off Contract.

In the event of any conflict or inconsistency, the RM1557.15 framework agreement and the applicable Call-Off Contract shall **prevail**, and any conflicting provision of this document shall be **disapplied**.

Document Date:
Classification: PUBLIC

CONTENTS

CLAUSE

ANNEX

This agreement is dated [DATE]

PARTIES

(1) [FULL COMPANY NAME] incorporated and registered in England and Wales with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] **(Customer)**

(2) Bell Microsystems Limited incorporated and registered in England and Wales with company number 03102360 whose registered office is at Bay House Compass Road, Cosham, Portsmouth, Hampshire, England, PO6 4RS **(Provider)**

BACKGROUND

(A) The Customer and the Provider entered into [SERVICE PROVIDER AGREEMENT] (**Master Agreement**) on [INSERT DATE] that may require the Provider to process Personal Data on behalf of the Customer.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors and the General Data Protection Regulation (*(EU) 2016/679)*.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the Customer authorises to give the Provider written personal data processing instructions as identified in ANNEX A and from whom the Provider agrees solely to accept such instructions.

Business Purposes: the services to be provided by the Provider to the Customer as described in the Master Agreement and any other purpose specifically identified in ANNEX A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given in the Data Protection Legislation.

Controller: has the meaning given in section 6, DPA 2018.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications;

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given in Clause 12.

Term: this Agreement's term as defined in Clause 10.

UK GDPR: has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.

1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4 A reference to writing or written excludes fax but not email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail.

2. Personal data types and processing purposes

2.1 The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions from Authorised Persons. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Provider must comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) requires the Provider to process or disclose the Personal Data to a third-party, the Provider must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

3.5 The Provider must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Provider's performance of the Master Agreement or this Agreement.

4. Provider's employees

4.1 The Provider will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

5. Security

5.1 The Provider must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX B.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 The Provider will without undue delay and in any event within forty-eight (48) hours notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic or EU law.

6.5 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Provider caused such, including all costs of notice and any remedy as set out in Clause 6.5.

7. Transfers of personal data

7.1 The Provider (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK or, the EEA without obtaining the Customer's prior written consent.

8. Subcontractors

8.1 The Provider may only authorise a third-party (subcontractor) to process the Personal Data if:

(a) the Customer is provided with an opportunity to object to the appointment of each subcontractor within (20) working days after the Provider supplies the Customer with full details in writing regarding such subcontractor;

(b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's

written request, provides the Customer with copies of the relevant excerpts from such contracts;

(c) the Provider maintains control over all of the Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.2 Those subcontractors approved as at the commencement of this Agreement are as set out in ANNEX A. The Provider must list all approved subcontractors in Annex A and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.3 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider which contains terms substantially the same as those set out in this Agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.4 The Parties agree that the Provider will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

9. Complaints, data subject requests and third-party rights

9.1 The Provider must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2 The Provider must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider must notify the Customer within (5) days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic or EU law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) the Provider retains any of the Personal Data related to the Master Agreement in its possession or control (**Term**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, the Customer may terminate any part of the Master Agreement involving the processing of the Personal Data effective immediately on written notice to the Provider without further liability or obligation of the Customer.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within (30) days, either party may terminate the Master Agreement on written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Provider will certify in writing to the Customer that it has deleted or destroyed the Personal Data within (30) days after it completes the deletion or destruction.

12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Agreement and the Data Protection Legislation and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Annexes to this Agreement [FREQUENCY] to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least (60) days' notice, during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Personal Data.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach has occurred or is occurring, or the Provider is in material breach of any of its obligations under this Agreement or any of the Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, the Provider will:

(a) promptly, conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit; AND

(c) provide the Customer with a copy of the written audit report;

13.4 [FREQUENCY], the Provider will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

13.5 On the Customer's written request, the Provider will make all of the relevant audit reports available to the Customer for review. The Customer will treat such audit reports as the Provider's confidential information under the Master Agreement.

13.6 The Provider will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider's management.

14. Warranties

14.1 The Provider warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.

15.2 Any limitation of liability set forth in the Master Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

16. Notice

16.1 Any notice given to a party under or in connection with this Agreement shall be in writing and shall be:

(a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

(b) sent by email to the following addresses (or an address substituted in writing by the party to be served):

(i) For the Customer: [CUSTOMER DATA PRIVACY CONTACT]

(ii) For the Provider: [PROVIDER DATA PRIVACY CONTACT]

16.2 Any notice shall be deemed to have been received:

(a) if delivered by hand, at the time the notice is left at the proper address; or

(b) if sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting; or

(c) if sent by email, at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume.

16.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This Agreement has been entered into on the date stated at the beginning of it.

Signed by [NAME OF DIRECTOR]	
for and on behalf of [NAME OF **Customer**]	Director
Signed by [NAME OF DIRECTOR]	
for and on behalf of [NAME OF **Provider**]	Director

ANNEX A Personal Data processing purposes and details

Subject matter of processing: [Short description, for example name of the service or description of the master agreement]

Duration of Processing: [Periods for which the services are being provided]

Nature of Processing: [Description of the type of processing such as data collection, storage, sharing and so on]

Business Purposes: [Description of the processing purpose(s) – for example processing for HR purposes, recruitment, direct marketing and so on]

Personal Data Categories: [Set out types of personal data such as names, contact details, pay details, images and so on]

Data Subject Types: [Set out categories of data subjects such as employees, customers, students and so on]

Authorised Persons: [Insert details of employees/others authorised to give written instructions]

Approved Subcontractors:

- [List all approved subcontractors.]

ANNEX B Security measures

Provider to insert description of its technical and organisational data security measures such as:

- Physical access controls.
- System access controls.
- Data access controls.
- Transmission controls.
- Input controls.
- Data backups.
- Data segregation.

SHARED RESPONSIBILITIES AGREEMENT FOR CROWN COMMERCIAL SERVICE G-CLOUD 15 FRAMEWORK (RM1557.15)

Document Date: 20/01/2026
Classification: PUBLIC

1. APPLICATION OF THIS AGREEMENT

1.1 The following terms and conditions shall apply only to a Contract under which cloud computing services ("Services") is sold by Bell to the Client under the Crown Commercial Service G-Cloud 15 framework (RM1557.15), including but not limited to software as a service, platform as a service, infrastructure as a service and desktop as a service.

1.2 This document is provided for the purposes permitted under the Crown Commercial Service G-Cloud 15 Framework (RM1557.15).

1.3 This document applies only to the extent that, and insofar as, its terms are consistent with and permitted by the RM1557.15 framework Agreement, the CCS General Terms, the Joint Schedules and the applicable Call-Off Contract.

1.4 In the event of any conflict or inconsistency, the RM1557.15 Framework agreement and the applicable Call-Off Contract shall prevail, and any conflicting provision of this document shall be disapplied.

2. DEFINITIONS

The following words and phrases used in this Appendix 3 shall have the meanings assigned to them below:-

"**Authorised Users**"	means individuals who have been provided with Access Codes by the Subscriber;
"Call-Off Contract"	A contract agreed between Bell and the Subscriber under the Crown Commercial Service G-Cloud 15 framework (RM1557.15).
"Subscriber Data"	the data input to the Online Service by the Authorised Users, or by Bell on the Subscriber's behalf for the purpose of using the Online Service or facilitating the Subscriber's use of the Online Service;
"**Documentation**"	means the operating manuals, user instruction manuals, technical literature, user specifications and other documentation relating to the Online Service made available to the Subscriber by Bell online;
"**Subscription Term**"	means the period for which Subscriber shall have access to the Online Service as set out in the Call-Off Contract;
"Software"	the online software applications provided as part of the Online Service;

"**Subscriber**"	means the Client or the Client Customer identified as the buyer of the Online Service in the Call-Off Contract;
"**Service Level Agreement ("SLA")**"	means the terms and conditions governing the performance of the Online Service as specified in the Call-Off Contract and agreed by the Parties;
"Support Online Service Policy"	Means Bell's policy for providing support in relation to the Online Service as made available on its website from time to time;
"User Subscriptions"	Means the user subscriptions purchased by the Client pursuant to Paragraph 6.1 which entitle Authorised Users to access and use the Services and the Documentation in accordance with this Contract;
"Virus"	any thing or device (including any software, code, file or program) the purpose of which is to: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

3. RIGHT TO ACCESS AND USE THE SERVICE

3.1 In consideration of the payment of the fees set out in the agreed Call-Off Contract, Bell shall grant the Client the right for the Subscriber to use the Online Service for the Licence Term on the terms and conditions set out in Paragraphs 4 to 12 (inclusive below).

4. USER SUBSCRIPTIONS

4.1 In relation to the Authorised Users, the Subscriber undertakes that:

4.1.1 the maximum number of Authorised Users that it authorises to access and use the Online Service and the Documentation shall not exceed the number of User Subscriptions it has purchased from time to time;

4.1.2 it will not allow or suffer any User Subscription to be used by more than one individual Authorised User unless it has been reassigned in its

entirety to another individual Authorised User, in which case the prior Authorised User shall no longer have any right to access or use the Online Service and/or Documentation;

4.1.3 each Authorised User shall keep a secure password for his use of the Online Service and Documentation, that such password shall be regularly and frequently changed consistent with Bell's published security policy and that each Authorised User shall keep his password confidential;

4.1.4 it shall maintain a written, up to date list of current Authorised Users and provide such list to Bell within five (5) Working Days of Bell's written request at any reasonable time or times;

4.1.5 it shall permit Bell or Bell's designated auditor to audit the Online Service in order to establish the name and password of each Authorised User and the Subscriber's data processing facilities to audit compliance with this Contract. Each such audit may be conducted no more than once per quarter, at Bell's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Subscriber's normal conduct of business;

4.1.6 if any of the audits referred to in Paragraph 5.2.5 reveal that any password has been provided to any individual who is not an Authorised User, then without prejudice to Bell's other rights, the Subscriber shall promptly disable such passwords and Bell shall not issue any new passwords to any such individual; and

4.2 The Subscriber shall not access, store, distribute or transmit any Viruses, or any material during the course of its use of the Online Service that:

4.2.1 is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

4.2.2 facilitates illegal activity;

4.2.3 depicts sexually explicit images;

4.2.4 promotes unlawful violence;

4.2.5 is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or,

4.2.6 is otherwise illegal or causes damage or injury to any person or property; and,

4.3 Bell reserves the right, without liability or prejudice to its other rights to the Subscriber, to disable the Subscriber's access to any material that breaches the provisions of this Paragraph 4.

4.4 The Subscriber shall not:

4.4.1 except as may be agreed under the Call-Off Contract and all applicable terms, or allowed by any Applicable Laws which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under this Contract:

4.4.2 attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software and/or Documentation (as applicable) in any form or media or by any means; or

4.4.3 attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; or

4.4.4 access all or any part of the Online Service and Documentation in order to build a product or service which competes with the Online Service; or

4.4.5 use the Online Service and/or Documentation to provide services to third parties; or

4.4.6 subject to Paragraph 5.7, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Online Service and/or Documentation available to any third party except the Authorised Users, or

4.4.7 attempt to obtain, or assist third parties in obtaining, access to the Online Service and/or Documentation, other than as provided under this Paragraph 5; or

4.4.8 introduce or permit the introduction of, any Virus into Bell or the Subnetwork and information systems.

4.5 The Subscriber shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Online Service and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify Bell.

4.6 The rights under this Paragraph 4 are granted to the Subscriber only, and shall not be considered granted to any subsidiary or holding company of the Subscriber but this shall not prohibit the scope of the term Authorised User

such that an individual may qualify as an Authorised User even if an employee, agent or contractor of a subsidiary or holding company of the Subscriber.

5. ADDITIONAL USER SUBSCRIPTIONS

5.1 If at any time the Subscriber requires additional User Subscriptions for the Online Service it shall notify Bell accordingly and Bell shall provide a Quotation setting out the additional Charges payable for the requested User Subscriptions.

5.2 Subject to payment of the applicable Charges, Bell shall grant access to the Online Service and the Documentation to such additional Authorised Users in accordance with the provisions of this Contract.

6. ONLINE SERVICE

6.1 Bell shall use commercially reasonable endeavours to make the Online Service available 24 hours a day, seven (7) days a week, except for:

6.1.1 planned maintenance performed as and when notified to the Subscriber; and

6.1.2 urgent unscheduled maintenance.

6.2 Bell shall use commercially reasonable endeavours to perform maintenance at times likely to cause the least disruption to its end users unless an emergency.

6.3 Bell will, as part of the Online Service, provide the Subscriber with Bell's standard Subscriber support services in accordance with Bell's Support Online Service Policy in effect at the time that the Online Service are provided. Enhanced support services may be purchased separately at Bell's published rates.

6.4 If, at any time whilst using the Online Service, the Subscriber exceeds the usage set out in Bell's acceptable use policy (if applicable), any additional use charges incurred shall be paid to Bell at the then current excess use rates.

7. SUBSCRIBER DATA

7.1 The Subscriber shall own all right, title and interest in and to all of the Subscriber Data that is not personal data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of all such Subscriber Data.

7.2 Bell shall follow its archiving procedures for Subscriber Data as set out in its back up policy as may be amended by Bell in its sole discretion from time to time. In the event of any loss or damage to Subscriber Data, the Subscriber's remedy shall be for Bell to use reasonable commercial endeavours to restore

the lost or damaged Subscriber Data from the latest back-up of such Subscriber Data maintained by Bell in accordance with the its back up policy. Bell shall not be responsible for any loss, destruction, alteration or disclosure of Subscriber Data caused by any third party except those third parties sub-contracted by Bell to perform services related to Subscriber Data maintenance and back-up.

7.3 Bell shall, in providing the Online Service, comply with its Privacy and Security Policy as such document may be amended from time to time by Bell in its sole discretion.

7.4 All Parties will comply with Clause 12.1, this Paragraph 7 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Laws.

7.5 All parties acknowledge that:

7.5.1 if Bell processes any personal data on the Subscriber's behalf when doing so, the Subscriber is the controller and Bell is the processor for the purposes of the Data Protection Laws; and,

7.5.2 the Subscriber shall be responsible for entering into a data processing agreement with Bell on such terms as the Subscriber may agree with Bell and in the absence of such an agreement prior to the Subscriber's use of the Online Service, the terms of Bell's policy on the processing and use of personal data shall apply unless and until such an agreement is in effect.

7.6 Without prejudice to the generality of Paragraph 7.4, the Subscriber will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to Bell for the duration and purposes of this Contract so that Bell may lawfully use, process and transfer the personal data in accordance with this Contract on the Subscriber's behalf.

8. THIRD PARTY PROVIDERS

8.1 The Subscriber acknowledges that the Online Service may enable or assist it to access the website content of, correspond with, and purchase products and services from, third parties via third-party websites and that it does so solely at its own risk. Bell makes no representation, warranty or commitment and shall have no liability or obligation whatsoever in relation to the content or use of, or correspondence with, any such third-party website, or any transactions completed, and any contract entered into by the Subscriber, with any such third party. Any contract entered into and any transaction completed via any third-party website is between the Subscriber and the relevant third party, and not

Bell. Bell recommends that the Subscriber refers to the third party's website terms and conditions and privacy policy prior to using the relevant third-party website. Bell does not endorse or approve any third-party website nor the content of any of the third-party website made available via the Online Service.

9. THIRD PARTY VENDOR'S OBLIGATIONS

9.1 Bell undertakes that the Online Service will be provided substantially in accordance with the Documentation and with reasonable skill and care.

9.2 The undertaking at Paragraph 10.1 shall not apply to the extent of any non-conformance which is caused by use of the Online Service contrary to the Documentation or Bell's instructions, or modification or alteration of the Online Service by any party other than Bell or Bell's duly authorised contractors or agents. If the Online Service does not conform with this undertaking, Bell will, at its expense, use all reasonable commercial endeavours to correct any such non-conformance promptly, or provide the Subscriber with an alternative means of accomplishing the desired performance. Such correction or substitution constitutes the Client's sole and exclusive remedy for any breach of the undertaking set out in Paragraph 10.1.

9.3 Bell:

9.3.1 does not warrant that:

(1) the Subscriber's use of the Online Service will be uninterrupted or error-free;

(2) the Online Service, Documentation and/or the information obtained by the Subscriber through the Online Service will meet the Subscriber's requirements; or,

(3) the Software or the Online Service will be free from Viruses.

9.3.2 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Subscriber acknowledges that the Online Service and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

9.4 Bell warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this Contract.

10. CLIENT'S RESPONSIBILITIES

10.1 The Subscriber acknowledges that it is responsible for the following, at its own cost and expense:

10.1.1 responding to any reasonable requests from Bell in order to provide the Online Service;

10.1.2 carrying out all its responsibilities set out in this Contract t in a timely and efficient manner;

10.1.3 ensuring that the Authorised Users use the Online Service and the Documentation in accordance with the terms and conditions of this Contract;

10.1.4 any Authorised User's breach of this Contract;

10.1.5 obtaining and maintaining all licences, consents, and permissions necessary for the Authorised Users to access and use the Online Service but not those required by Bell to supply the Online Service in the jurisdictions in which it markets and promotes the Online Service;

10.1.6 ensuring that its network and systems comply with the relevant specifications provided by Bell from time to time; and

10.1.7 to the extent permitted by law and except as otherwise expressly provided in this Contract, procuring, maintaining and securing its network connections and telecommunications links from its systems to Bell’s data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Subscriber's network connections or telecommunications links or caused by the internet.

11. INTELLECTUAL PROPRIETARY RIGHTS

11.1 The Subscriber acknowledges and agrees that Bell and/or its licensors own all Intellectual Property Rights in the Online Service and the Documentation, subject to any conflicting terms within the Crown Commercial Service G-Cloud 15 Framework (RM1557.15). Except as expressly stated herein, this Contract does not grant the Subscriber any rights to, under or in, any patents, copyright, database right, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licences in respect of the Online Service or the Documentation.

11.2 Bell confirms that it has all the rights in relation to the Online Service and the Documentation that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this Contract.

12. TERM AND TERMINATION

12.1 On termination of this Contract for any reason:

12.1.1 the Subscriber shall immediately cease all use of the Online Service and/or the Documentation; and,

12.1.2 Bell shall permanently delete all of the Subscriber Data in its possession, unless Bell receives, no later than ten (10) Working Days after the effective date of the termination of this Contract, a written request for the delivery to the Subscriber of the then most recent back-up of the Subscriber Data. Bell shall use reasonable commercial endeavours to deliver the back-up to the Subscriber within thirty (30) days of its receipt of such a written request, provided that the Subscriber has, at that time, paid all Charges outstanding at and resulting from termination (whether or not due at the date of termination). The Subscriber shall pay all reasonable expenses incurred by Bell in returning or disposing of Subscriber Data.