MANAGED CLOUD DATA PROTECTION SERVICE TERMS

These Managed Cloud Data Protection Service Terms ("**Terms**") contain the terms governing the provision of the **Managed Cloud Data Protection Services** by Interactive Pty. Limited ABN: 17 088 952 023 of 461 Williamstown Road, Port Melbourne VIC 3207 ("**Interactive**") to the customer named in the CMS SOW that applies to these Terms ("**Customer**"). The Master Services Agreement applies to these Terms and the CMS SOW.

1 Services

1.1 Interactive will provision the Services and required licenses for and on behalf of the Customer.

1.2 If the CMS SOW states that Interactive provides Managed Cloud Data Protection Services for Microsoft 365, the following applies:

(a) The Managed Cloud Data Protection Services for Microsoft 365 enable data protection, backup and restore services comprising:

i. **Exchange Online**, including:

A. mailbox level data protection;

B. item level restore (in place or to PST);

C. individual mailbox restore (In place or to PST); and

For the avoidance of doubt, mass mailbox restore is not supported and/or scoped.

ii. **Teams**, including:

A. channel level data protection; and

B. item level restore (in place or to file).

iii. **OneDrive for Business**, including;

A. User level data protection; and

B. item level restore (in place or to file).

iv. **Azure Active Directory** (also known as AAD), including:

A. Object level data protection; and

B. item level restore (in place).

v. **SharePoint Online**, including:

A. site level data protection; and

B. item level restore (in place or to file).

vi. Provision of licensing for Microsoft 365 data protection as per the metering policy set out below:

A. A maximum of 50GB of Tenant Backup Storage is included in each User Subscription but calculated at the tenant level such that the total capacity will be calculated as Users X 50GB.

B. All protected mailboxes with a valid Microsoft 365 for Exchange Online license are counted as part of Subscription Usage. The parties will determine which mailboxes and mailbox types are to be protected during onboarding;

C. A OneDrive User with OneDrive Quota (OneDrive storage is allocated) and valid Microsoft 365 OneDrive license is counted as part of Subscription Usage. The parties will determine which OneDrive for Business accounts are to be protected during onboarding;

D. SharePoint and Teams are not metered by User but by Backup Storage consumed. The parties will determine which SharePoint and Teams Sites are to be protected during onboarding;

vii. Interactive will aim to protect each Microsoft 365 object every 24 hours, excluding when new Protected Data is added to the Platform. New Protected Data and initial data protection operations for added Protected Data are limited by Microsoft online services throttling.

1.3 If the CMS SOW states that Interactive provides Managed Cloud Data Protection Services for File and Object Workloads, the following applies:

(a) The Managed Cloud Data Protection Services for File and Object workloads enable data protection, backup and restore services comprising:

i. Azure Object Storage Accounts located within Australia, subject to the requirements of the Third Party Software Vendor;

ii. Amazon S3 Object Storage Accounts located within Australia; subject to the requirements of the Third Party Software Vendor;

(b) Provision of licencing for File and Object data protection in accordance with the metering policy set out below;

A. License usage is measured by consumption, based on front end used capacity, in 1TB increments;

(c) Interactive will aim to protect each object every 24 hours, excluding when new Protected Data is added to the Platform. New Protected Data and initial data protection operations for added Protected Data are limited by Third Party Software Vendor online services throttling.

1.4 If the CMS SOW states that Interactive provides Managed Cloud Data Protection Services for Microsoft Dynamics 365, the following applies:

(a) The Managed Cloud Data Protection Services for Microsoft Dynamics 365 enable data protection, backup and restore services comprising:

i. **Dynamics,** including:

A. Customized tables; and

B. System tables set out below;

Display Name	**Logical Name**
Account	account
Appointment	appointment
Article	kbarticle
Article Template	kbarticletemplate
Attachment	activitymimeattachment
Bookable Resource	bookableresource
Bookable Resource Booking Header	bookableresourcebookingheader
Bookable Resource Category	bookableresourcecategory
Bookable Resource Category Assn	bookableresourcecategoryassn
Bookable Resource Characteristic	bookableresourcecharacteristic
Bookable Resource Group	bookableresourcegroup
Booking Status	bookingstatus
Business Unit	businessunit
Campaign	campaign
Campaign Activity	campaignactivity
Campaign Response	campaignresponse
Case	incident
Case Resolution	incidentresolution
Category	category
Channel Property	channelproperty
Channel Property Group	Channelpropertygroup

Characteristic	Characteristic
Competitor	competitor
Connection	connection
Contact	contact
Contract	contract
Contract Line	contractdetail
Contract Template	contracttemplate
Currency	transactioncurrency
Discount	discount
Discount List	discounttype
Document Location	Sharepointdocumentlocation
Email	email
Email Server Profile	emailserverprofile
Email Signature	emailsignature
Email Template	template
Entitlement	entitlement
Entitlement Template	Entitlementtemplate
Expired Process	expiredprocess
Fax	fax
Feedback	feedback
Follow	postfollow
Goal	goal
Goal Metric	metric
Invoice	invoice
Invoice Line	invoicedetail
Knowledge Article	knowledgearticle
Knowledge Article Incident	knowledgearticleincident
Knowledge Article Views	knowledgearticleviews
Lead	lead
Lead To Opportunity Sales Process	leadtoopportunitysalesprocess
Letter	letter
Mailbox	mailbox
Mail Merge Template	mailmergetemplate

Marketing List	list
New Process	newprocess
Note	annotation
Opportunity	opportunity
Opportunity Close	opportunityclose
Opportunity Line	opportunityproduct
Opportunity Relationship	customeropportunityrole
Opportunity Sales Process	opportunitysalesprocess
Order	salesorder
Order Close	orderclose
Order Line	salesorderdetail
Organization	organization
Phone Call	phonecall
Phone To Case Process	phonetocaseprocess
Position	position
Post	post
Price List	pricelevel
Price List Item	productpricelevel
Product	product
Product Association	productassociation
Product Relationship	productsubstitute
Publisher	publisher
Queue	queue
Queue Item	queueitem
Quote	quote
Quote Close	quoteclose
Quote Line	quotedetail
Rating Model	ratingmodel
Rating Value	ratingvalue
Rollup Query	goalrollupquery
Sales Attachment	salesliteratureitem
Sales Literature	salesliterature
Service	service

Service Activity	serviceappointment
SharePoint Site	sharepointsite
Site	site
Subject	subject
Task	task
Team template	teamtemplate
Territory	territory
Theme	theme
Unit	uom
Unit Group	uomschedule
User	systemuser

(b) Provision of licencing for Microsoft Dynamics 365 data protection in accordance with the metering policy set out below;

A. There is no maximum storage utilization limit for each User Subscription, however Interactive reserves the right to pass on any additional monthly fees if the Third Party Software Vendor imposes a storage limitation or charges Interactive for the Tenant Backup Storage.

B. All Users with a valid Microsoft Dynamics 365 License are counted as part of Subscription Usage. The parties will agree the number of Users which are protected during onboarding.

(c) Interactive will aim to protect each Microsoft Dynamics 365 object every 24 hours, excluding when new Protected Data is added to the Platform. New Protected Data and initial data protection operations for added Protected Data are limited by Microsoft online services throttling.

1.5 If the CMS SOW states that Interactive provides Managed Cloud Data Protection Services for the Customers Infrastructure as a Service ("**IaaS**") environment the following applies:

(a) Interactive will provide the Customer with data protection, backup and restore services IaaS:

i. Where the Customer has Virtual Machines ("**VM**") on either Azure Amazon Web Services("**AWS**"), VMWare or Hyper-V Interactive will perform snapshot backup with copy to Object Storage.

ii. Provisioning of licensing for VM data protection.

(b) Interactive will charge the Customer monthly, based on peak usage per month, per VM per workload.

1.6 If the CMS SOW states that Interactive will provide Managed Cloud Data Protection Services for the Customers Platform as a Service (**"PaaS**") environment the following applies:

(a) Interactive will provide the Customer with data protection, backup and restore services for PaaS:

i. Interactive will perform full database export with backup to Object Storage where the Customer has either of the following databases:

A. Azure PaaS; Azure SQL; or

B. Azure SQL Managed Instance Interactive will perform full database export with backup to Object Storage.

ii. Interactive will perform full database snapshots where the Customer has either of the following databases:

A. AWS PaaS Databases; or

B. AWS Relational Database Service ("**RDS**").

iii. Provisioning of licensing for PaaS data protection

(b) Interactive will charge the Customer monthly, based on peak usage per month, per PaaS per Workload.

1.7 The following features apply to the Services:

(a) Service setup and activation subject to the payment of the relevant Implementation Fee;

(b) License management and review;

(c) 24x7 Service Desk for the Managed Service via call or email;

(d) Platform health monitoring and management;

(e) Daily license usage and backup reporting;

(f) Incident triage;

(g) Change and configuration management; and

(h) Third-Party Software Vendor management and escalation.

2 Term of Services

2.1 Interactive will provide the Services for the Individual Term. The Individual Term commences on the Service Start Date.

2.2 Not less than 30 days before the end of the Individual Term or a current Further Term, either party may serve written notice on the other party stating it will not renew the Services. The Services renew for successive terms of 12 months (each successive term being a "**Further Term**"), at the end of the Individual Term and each Further Term if no such notice is served.

3 Pricing Terms

3.1 The Customer will be charged a management fee for any management services provided by Interactive and a licensing fee for any licenses provided by Interactive.

3.2 The Customer shall pay the Service Fee for each Service that is set out in the CMS SOW.

3.3 Notwithstanding clause 3.2, the Customer shall pay the monthly Managed Cloud Data Protection Fee for the Services listed in the CMS SOW from the date each license is provisioned. Licensing usage is measured daily, with the peak usage for each type of license counted to the next whole month.

3.4 Interactive may adjust the Managed Cloud Data Protection Fee for the Services detailed in the CMS SOW (for the avoidance of doubt, this change applies to both initial and additional Services) by giving no less than 30 days' notice to the Customer.

3.5 From the time each User or Protected Object is configured for protection until the User or Protected Object is no longer configured for protection, the Customer must pay Interactive the Managed Cloud Data Protection Fee that applies to the User or Protected Object.

3.6 If the Customer's usage exceeds the amounts set out in the CMS SOW, then the Customer will be required to pay additional Managed Cloud Data Protection Fees for the excess usage, which will be added to the following month's invoice. The excess usage will be charged at the per unit price set out in the CMS SOW, multiplied by the quantity of the excess usage.

3.7 The Implementation Fee for the Services is payable by the Customer on the following milestones:

(a) 50% on the date of the CMS SOW.

(b) 50% on the Service Start Date.

3.8 With respect to any the Third-Party Software detailed in the CMS SOW, if the relevant Third-Party Software Vendor:

(a) increases its license fees or introduces new license fees for their products that directly relate to the Services being provided to the Customer, Interactive may increase the Service Fees upon 30 days' written notice from Interactive to the Customer; or

(b) issues a billing correction to Interactive that directly relates to the Services, Interactive may issue an additional invoice to the Customer in respect of the billing correction, which may include retrospective Service Fees payable.

4 Project Delivery

4.1 Each party will assign a Project Manager and confirm an expected Project start date.

4.2 If the Customer is delaying the Project, Interactive may send the Customer a notice requiring it to rectify the delay within five (5) Business Days. If the Customer fails to or is unable to rectify the delay, Interactive may complete the remaining activities that are not dependent on the Customer and issue a notice confirming the Service Start Date (for the avoidance of doubt in these circumstances the provision of this notice will not require any Acceptance Tests to have occurred).

DUE DILIGENCE

4.3 The parties shall conduct the Due Diligence Stage to confirm the accuracy of the information the Customer has provided to Interactive and identify any possible issues or impact upon the Project.

4.4 If any issues are identified by Interactive which affect the Solution, the parties may agree to change the Solution in accordance with the Change Management Process (clause 5) or the Assumptions (clause 11).

BUILD STAGE

4.5 During the Build Stage, Interactive will liaise with the Customer to develop a detailed design, Project plan and Project schedule and complete the Solution design.

4.6 Interactive will perform the Build Stage in accordance with the Project plan.

ACCEPTANCE TESTING

4.7 Interactive will complete Acceptance Testing, after the Build Stage.

4.8 On completion of the Acceptance Testing, Interactive will notify the Customer of the date Acceptance Testing has concluded ("Acceptance Testing Conclusion Date").

4.9 The Customer shall approve Acceptance Testing no later than five (5) Business Days after the Acceptance Test Conclusion Date.

4.10 If the Customer identifies any defects caused by Interactive that prevent the Customer from using the tested Services, the Customer may provide Interactive with notice in writing rejecting the Acceptance Tests and detailing the reasons why. If the Customer delivers that notice:

(a) the parties shall work together to identify and correct the error that caused the Acceptance Tests to fail; and

(b) after the cause of error is corrected, Interactive will notify the Customer of a new Acceptance Test Conclusion Date and, in that event, clause 4.9 will apply again.

4.11 If the Customer, acting reasonably, delivers more than two notices rejecting the results of the Acceptance Tests, either party may refer the matter for resolution in accordance with the dispute resolution provisions in the Master Services Agreement.

4.12 If the Customer fails to approve Acceptance Testing or deliver a notice rejecting the Acceptance Tests within five (5) Business Days after the Acceptance Test Conclusion Date, then Acceptance Testing will be deemed approved by the Customer. After the Customer has approved Acceptance Testing or is deemed to have approved Acceptance Testing, Interactive will provide the Customer with a notice informing it of the Service Start Date.

SUPPORT

4.13 From the Service Start Date, Interactive will provide support to the Customer for the Services in accordance with these Service Terms.

4.14 Interactive will provide the Customer with semi-administrative login (username and password) for accessing the Platform on the Acceptance Testing Conclusion Date.

4.15 Data will not be considered protected until all Protected Data has been ingested into the Platform. If Protected Data is added or migrated to the Platform, Recovery Point Objectives pause until of all Protected Data is ingested to the Platform.

5 Change Management

Prior to the Service Start Date

5.1 Before the Service Start Date, if either party requests any change to the CMS SOW, that party shall submit to the other party a Project Change Request ("**PCR**").

5.2 The party submitting the PCR shall describe the change, the rationale for the change and the effect the change will have on the Services and relevant fees in the PCR.

5.3 Each party's Project Manager shall review the proposed change and may then either approve it, submit it for further investigation or reject it.

5.4 If parties agree to the PCR, they shall sign the PCR and, from the date it is signed, the CMS SOW will be amended according to the changes described in the PCR. If the PCR is not agreed to, the CMS SOW will continue to apply unchanged.

After the Service Start Date

5.5 The Customer may request to move, add, change or delete resources under Interactive's management by making a Service Request after the Service Start Date.

5.6 The Customer must make a Service Request as follows:

(a) Phone: 1300 669 670 (in Australia) or +61 2 9200 2679 (internationally); or

(b) Email: cmssupport@interactive.com.au; or

(c) By contacting the Account Executive or Service Delivery Manager assigned to the Customer.

5.7 The Customer is liable for all moves, adds, changes and deletions of Protected Objects or Users that are made by it, or by someone purporting to act on behalf of the Customer.

5.8 The Customer will not be charged for Simple Service Requests. The Customer will only be charged for Complex Service Requests.

6 Service Desk & National Operations Centre (NOC)

6.1 Interactive will provide 24-hour Service Desk and National Operations Centre (NOC) coverage to handle Customer queries and monitor the systems, software and communications that make up the Services.

7 Monitoring Services

7.1 Interactive will provide monitoring and remediation for all managed objects in the Platform, Alerts that affect performance, recoverability or availability will be notified to the Customer and remediation will be on a proactive basis.

7.2 Alert definitions are defined in the Solution design.

8 Transition Out and Data Retention

8.1 If the Services are terminated for any reason, the parties shall consult and agree on the terms and responsibilities involved in transitioning out of the Services to the Customer, or a third party appointed by the Customer. If the Services are validly terminated by the Customer in accordance with the Agreement, Interactive will promptly comply with all reasonable requests and directions of the Customer to facilitate the transitioning out of the Services and Protected Data so as to cause minimal interruption to ongoing services.

8.2 The Customer shall pay Interactive on a time and materials basis (with labour charged at the Standard Charge Out Rate), all reasonable costs and charges incurred by Interactive in relation to the transitioning out of the Services.

8.3 If, before the relevant CMS SOW or Services are terminated, the Customer makes a request to Interactive in writing for a backup or copy of the Protected Data, Interactive will provide the backup or copy at the Customer's expense (based on the Standard Charge Out Rate) and will not delete the Protected Data until it has provided the backup or copy. The Customer acknowledges the Managed Cloud Data Protection Fees are required to be paid during this period.

8.4 Interactive or the Third-Party Software Vendor may delete the Customer's Protected Data stored on the Platform upon termination. The Customer shall ensure it obtains a copy of its Protected Data before the Services are terminated. Notwithstanding any other clause in the Agreement, Interactive or the Vendor is not liable to the Customer for, and the Customer irrevocably releases Interactive and the Vendor from any loss or liability incurred by the Customer in connection with deletion of the Customer's Protected Data in accordance with this clause.

8.5 The Services configuration and Protected Data are not portable to another partner or third-party service provider of the same Platform.

9 Customer Acknowledgments

9.1 The Customer agrees as follows:

(a) The Customer is solely responsible for Customer Data, retention policies and any other policy settings, schedules, and configurable parameters applied to Protected Data, including implementing its own specific retention policies.

(b) Where Protected Data, retention policies and any other policy settings, schedules, and configurable parameters are applied by Interactive this will be communicated to the Customer for reference.

(c) The Customer and its authorised Users will keep access credentials confidential, and the Customer remains responsible for the acts and omissions of its authorised Users and any activity that occurs under its customer account(s) using the access credentials.

(d) The Customer is responsible for the security of its Protected Data if the Customer disables any encryption or other security feature within the Platform.

(e) The Customer is responsible for maintaining its own internet and data connections, and components of the Solution that are accessed or used through internet connections and may be subject to the Customers' internet service providers fees and downtime.

9.2 The Customer acknowledges that Customer Data may not be available for recovery if any of the following apply:

(a) Configuration, as defined in documentation, does not cover Customer Data.

(b) The Customer's initial backup and replication is not properly completed.

(c) The Customer deletes Protected Data and does not restore it after deletion pursuant to the Customer's Protected Data retention policies.

(d) The Customer selects incorrect or inappropriate retention policies within the Platform.

(e) The Customer's IT environment is unable to secure a connection with the service or network.

(f) The Customer fails to follow technical requirements and any documentation provided to it by Interactive or the Third-Party Software Vendor about using the Platform, including installing updates, or failing to periodically test the Customer's backups and or ensure that Customer Data is protected and not otherwise corrupted.

9.3 Interactive is not liable to the Customer for, and the Customer irrevocably releases Interactive from all claims arising out of, or in relation to, loss or liability suffered by the Customer as a result of one or more of the following:

(a) The Customer making changes to the Customer's applications or environment that can negatively affect the Service.

(b) The Customer making changes to the Service or configuration.

10 Customer Data and Protected Data

10.1 All Protected Data will be held in the Platform.

10.2 All Protected Data is retained while the Services are active subject to the agreed retention policy. If the Services are not active clause 8.4 applies. A minimum subscription level is required to maintain the Protected data retention.

10.3 Interactive are not required to back-up Customer Data, unless otherwise agreed in writing between the parties. The Customer remains solely responsible for protecting its own Customer Data.

10.4 The Customer is solely responsible and liable for its conduct, Customer Data and Protected Data related to the Platform. The Customer indemnifies and holds harmless Interactive against any and all loss, cost, damage, liability and expenses arising out of, or resulting from or in connection with, the Customer's breach of the Agreement.

10.5 If Interactive causes loss of or damage to the Customer's Protected Data stored on the Platform, Interactive will assist to restore the Protected Data to the last available restoration point, however Interactive is not otherwise liable to the Customer for any loss of or damage to Protected Data.

10.6 The Customer authorises Interactive to provision Services on the Customer's behalf, control and administer the Customer's account (including to modify or terminate access) and access the Protected Data.

11 Assumptions

11.1 The relevant assumptions specified below apply to data protection:

(a) For Microsoft 365 and Microsoft Dynamics 365 Workloads:

i. the minimum number of licenses that will be supported is 50;

ii. the Customer will protect all Customer Data unless agreed otherwise agreed in writing; and

iii. the Customer must have an Azure tenancy, with Azure Active Directory as the identity provider for all Workloads;

(b) For Microsoft Dynamics 365 only the Customer will protect all entries and tables unless agreed otherwise agreed in writing;

(c) Multi Factor Authentication ("**MFA**") will be enabled via Azure Active Directory Security Assertion Mark Up Language ("**SAML**") by the Customer.

11.2 The following assumptions apply to data protection for IaaS and PaaS Workloads:

(a) the minimum number of licenses that will be supported across both IaaS and PaaS is 10.

11.3 Interactive relies on the information provided to it by the Customer to be able to perform the Services as required by this Agreement. If any assumptions made by Interactive or set out in the CMS SOW, or these Terms are proven inappropriate, including because the information provided by the Customer was incorrect or inadequate, or if technical requirements are proven to be beyond the capabilities of the Solution, Interactive will negotiate with the Customer with respect to one or more of the following:

(a) altering the Solution, which may require a change in accordance with the Change Management Process;

(b) adjusting the Project Schedule in relation to any changes required to the Solution; and

(c) adjusting either or both of the Implementation Fees and the monthly Service Fees as a result of the alterations to the Project.

11.4 The Customer will whitelist and allow network access to certain URLs, nominated by Interactive, to allow Interactive to run the Service. Interactive will provide the Customer with information explaining the purpose and security of these URLs on request.

11.5 Any Customer Data held in another application or third-party service provider which is not part of the Agreement, intended for use as data protection or disaster recovery or archive, does not fall under the scope of Managed Cloud Data Protection Services detailed in the Agreement. The Customer shall ensure that it obtains a copy of its data before the previous application or third-party service provider services are terminated.

12 Exclusions

12.1 The following items are Out of Scope and are not included in the Services provided by Interactive unless specifically detailed in the CMS SOW, but are available by agreement between the parties and will be charged in accordance with the Standard Charge Out Rate:

(a) anything not listed as being in-scope as part of the Services;

(b) Microsoft Active Directory configuration;

(c) agent deployment to an unprotected Workload;

(d) Disaster Recovery;

(e) support for desktop, laptop, handheld device & smart phone;

(f) infrastructure, storage, networks at the customer (or other third party) location, unless otherwise managed by Interactive;

(g) providing the Customer with relevant information for auditors, regulatory bodies, or insurers;

(h) alternative storage locations for the Customer Data;

(i) configuration of the Customer's tenancy to allow connectivity to the Platform, excluding initial setup;

(j) rectifying or mitigating issues within the Customer's environment, if the issue is caused or contributed to by the Customer (for example, servers not being supported by the Third-Party Vendor) and Interactive has previously provided recommendations to the Customer to rectify or mitigate the issue, which the Customer has not implemented;

(k) migration of any existing backups or backup data to the new Solution; and

(l) management of any existing backup data from a third party or application

(m) test or development or sandbox instance of Microsoft Dynamics 365.

12.2 The following items are Out of Scope and not included in relation to Microsoft 365 workloads:

(a) Microsoft 365 Public Folders;

(b) full SharePoint site recovery;

(c) management of any existing backup data; and

(d) migration of any existing backups or backup data to the new Solution.

12.3 The following items are Out of Scope and not included in relation to IaaS & PaaS workloads:

(a) Protection for any NAS devices.

(b) Protection for any appliance-based devices, unless explicitly stated in the CMS SOW.

(c) Migration of any existing backups or backup data to the new Solution.

(d) Management of any existing backup data.

(e) Security, configuration, monitoring and availability of on Customer provided storage or compute.

12.4 The CMS SOW may specify additional exclusions that apply.

13 Interactive Responsibilities

13.1 Interactive will;

(a) configure the Managed Cloud Data Protection Services as specified in the Solution design;

(b) provide an 'as built' document for the implemented Solution;

(c) provide the relevant Workload licenses to enable data protection, including procurement, billing, and overages;

(d) provide and review reports on backup health;

(e) configure the relevant alerting and notifications for successful backup jobs, failed or incomplete backup jobs, audit trail and Subscription Usage;

(f) configure the Platform security as specified in the Solution design, including Azure based Single Sign On ("**SSO**") with Multi factor Authentication ("**MFA**");

(g) perform service checks, monitoring and report on the service status and protectively address issues;

(h) assist to perform data protection and restoration activities under the Incident management process;

(i) complete Customer initiated configuration change requests under the Change Management Process;

(j) monitor and manage the availability, security, and the capacity of the Platform;

(k) notify the Customer of maintenance activities where appropriate; and

(l) provide support to the Customer for issues related to the Platform and or Service.

14 Customer Responsibilities

14.1 The Customer will;

(a) provide appropriate Platform connectivity, including Microsoft 365 and Azure Tenancy Global Administrator credentials as a service account, with an Exchange Online mailbox;

(b) take ultimate responsibility for the Backup Plans and Content;

(c) take responsibility for Policies and Compliance;

(d) inform Interactive of any changes, or planned changes to the protected Services, such as the addition or removal of Users and/or a migration of a significant data size (>500GB). Increase of data size may impact backup performance and Recovery Point Objective;

(e) provide Interactive Microsoft 365 administrative login credentials (username and password) for accessing the Platform; and

(f) provide roles, Users and Azure Active Directory groups for Role Based Access Control, as detailed in the Solution design.

(g) Oversee the security, configuration, monitoring, capacity, maintenance, and availability of any necessary storage, network or compute used by the Platform, unless these responsibilities are assigned to Interactive through a separate Addendum or Statement of Work.

(h) If provided with self-service access:

i. the Customer assumes responsibility for all actions taken under their own login/access;

ii. any changes made by the Customer using their login/access, which require Interactive remediation, will be charged at current Standard Charge Out Rates.

15 General

15.1 Interactive reserves the right to discontinue the Managed Cloud Data Protection Services at any time. In those circumstances, if Interactive is unable to transition to a replacement service offering with similar functionality to the discontinued Platform, Interactive will give the Customer as much notice as is practicable and provide the Customer with reasonable time to export a copy of the Protected Data from the Platform to an alternate service and third-party service provider of the Customer's choice.

15.2 The Customer acknowledges that Interactive may vary these Terms at any time by posting an updated version at www.interactive.com.au/terms-and-conditions/or such other URL as may be used by Interactive. It is the Customer's responsibility to monitor the relevant URL for updates, and to comply with these Terms as updated. The updates to these Terms will apply from the version date. By continuing to use the Services after that date, the Customer is deemed to have agreed to the updated Terms.

16 Definitions

16.1 The following definitions apply to these Terms:

Agreement means these Terms, the CMS SOW, and the Master Services Agreement.

Acceptance Testing or **Acceptance Test** means Interactive's testing of the software or hardware on a complete integrated system to evaluate the Platform's compliance with the Customer's requirements specified during or prior to the Due Diligence Stage.

Acceptance Testing Conclusion Date means the date that Interactive concludes Acceptance Testing and considers the Services ready for use.

Backup Plans and Content means the content that is configured to be protected, including the schedule, the retention and the data.

Backup Storage means a supplementary, segregated copy of data selected for protection by Interactive's Managed Cloud Data Protection Service that can be recovered in the event of primary data failure.

Build Stage consists of implementing the Solution; tracking progress against the Project plans; conducting system tests; and providing system access to the Customer to perform migration and Acceptance Testing.

Change Management Process means the process described in clause 4.

CMS SOW means the statement of work for cloud and managed services entered into between Interactive and the Customer named in that statement of work.

Commencement Date means the date set out in the CMS SOW.

Complex Service Request means a Service Request that is not a Simple Service Request.

Customer Data means the Customer information that is stored on Customer controlled systems.

Due Diligence Stage comprises the Customer providing Interactive with access to its systems and supporting documentation.

Exchange Online refers to a suite of cloud-based email services provided by Microsoft.

IaaS refers to Infrastructure as a Service and specifically relates to Virtual Machines hosted on Azure, AWS or on premise VMWare and HyperV.

Incident means an unplanned interruption to the standard operation of the Platform.

Individual Term means, for the Services, the individual term set out in the CMS SOW, commencing on the Service Start Date, as extended in accordance with these Terms.

Implementation Fee means the Service Fee for the onboarding of each Service, as set out in the CMS SOW.

Managed Cloud Data Protection means the solution providing data protection service described in these Terms.

Managed Cloud Data Protection Fee means the Service Fee payable for Managed Services and the fee for the licenses acquired under the terms of these Terms.

Master Services Agreement means the Master Services Agreement referred to in the CMS SOW.

Microsoft 365 means a suite of cloud-based services provided by Microsoft.

Object Storage is commonly used in cloud storage services and large-scale data repositories, where the ability to store and manage unstructured data is essential. Supported object storage solutions include Amazon S3, Microsoft Azure Blob Storage, Metallic Recovery Reserve and Google Cloud Storage.

OneDrive for Business refers to a suite of cloud-based file sharing services provided by Microsoft.

PaaS refers to Platform as a Services specifically relates to databases running on Azure or AWS as specified within clause 1.6.

Platform means the Third-Party Software Vendor software solution.

Policies and Compliance means the configuration or the Protected Data, including content, schedule and retention, and the adherence to the rules defined.

Project means all work to be performed during the Due Diligence Stage, the Build Stage and Acceptance Testing to deliver the Solution to the Customer in accordance with this Statement of Work.

Project Manager means the Interactive or Customer staff member responsible for delivery of the CMS SOW.

Protected Data means Customer Data that is configured to be protected by the Services.

Protected Object means an item that is configured to be protected by the Services.

Recovery Point Objective means the number and recency of backups available for restore.

Role Based Access Control means a security framework that regulates access to resources or systems based on the roles of individual users within an organisation.

Services in these Terms means the Managed Cloud Data Protection for Microsoft 365, IaaS and PaaS Services on Azure, AWS, and/or VMWare on-premises.

Service Desk means the first point of contact between Interactive and the Customer in respect of reporting and communicating Incidents.

Service Request means a request for service from the Customer, which may be a Simple or Complex Service Request.

SharePoint refers to a suite of cloud-based file services provided by Microsoft.

Simple Service Request means a request from the Customer for a simple move, add, change or delete to the Services, determined by the Interactive to be a request that:

(a) is non-complex and does not require planning or due diligence;

(b) can be completed in 4 hours or less, by a single engineer and during Business Hours; and

(c) does not require representation at Interactive's change advisory board.

Solution means the proof of concept or technical design of the Services contained in the CMS SOW.

Subscription means the individual Managed Cloud Data Protection for Microsoft 365 Services Interactive agrees to make available as specified in the Master Deliverables table in the CMS SOW.

Subscription Usage means the amount, by volume, consumed by each Service on a monthly basis.

Teams means a suite of cloud-based collaboration services provided by Microsoft.

Tenant Backup Storage means the total amount of Backup Storage consumed by a Customer.

Third-Party Software means programs or applications created by companies other than Interactive, which Interactive provides or licenses to the Customer in accordance with the CMS SOW, which includes but is not limited to Microsoft Software.

Third-**Party Software Vendor** means a company that creates Third Party Software or supplies Third Party Software to Interactive.

Users means a licensed Microsoft 365 user which is protected by the Services.

Workload means any IaaS machine, PaaS Service, File and Object Storage, Microsoft 365 User or Microsoft Dynamics 365 User that is protected by the Services.