Cloud9 Service Description
G-Cloud10

Hewlett Packard Enterprise

CISCO

janet

Crown Commercial Service Supplier

Version 1.0

Table of Contents

1. About Cloud9

History and Purpose

Cloud9 is a wholly owned brand of Innovate LTD and was formed in 2013. Innovate was formed in 2005 as an IT Managed Services provider to UK businesses, however the more successful Innovate become, the more field engineers it needed, the more contracts it required to continue to support the increased number of engineers. In addition the support desk was handling hundreds of new incidents every day and could have over a thousand open incidents at any one time.

Cloud9 was created to solve a number of challenges:

1. Deliver IT as it should be, improve customer experience and reduce churn

2. Reduce the number of support incidents (currently averaging less than 8 per day)

3. Focus on delivering innovation and business outcomes rather than maintaining legacy, outdated environments

Proposition

The first iteration of Cloud9 was a highly optimised Virtual Desktop Infrastructure. Initially this was for internal use as a way of quickly simulating and testing customer environments to reduce engineering hours spent build machines manually. In a short space of time, Cloud9 1.0 was released to existing customers with a high percent of take-up. To date we have a very low attrition rate, our largest customer in 2016 was a 1.5tn EUR bank, we run a highly resiliency VDI environment for the private equity division, they had a total of 8 incidents.

Delivering Cloud; Properly

Delivering highly optimised, fault tolerant Virtual Desktop Infrastructure well, you have need expertise in very specific areas:

1. Storage

2. DR & Business Continuity

3. Networking, latency & Security

4. Graphic Rendering

5. Citrix Optimisation

6. Cloud design

7. Software distribution & Application sequencing

To be able to do VDI well, the rest of the Cloud Service stack is fairly simple in comparison.

In addition, it also means that Cloud9 support the rest of the stack with capabilities around:

1. Infrastructure as a Service

2. Platform as a Service

3. Software as a Service – we also have software vendors using Cloud9 as a platform to distributing SaaS or IOT solutions

4. Back-up, DR & Business Continuity

5. Security; AV, IDS, IPS, DDOS, Prevent, Remote Access

6. Storage (Object & Block)

Jisc & the Janet Network

Cloud9 is available to Jisc customers as a directly connected Cloud Service platform on the Janet network.

Janet is highly connected into Public Sector, with peering's into PSN and healthcare networks (N3 & HCSN).

Jisc are offering Cloud9 services to Jisc customers directly and through Jisc Commercial.

Cloud9 v other Private Cloud Service Providers

No two Cloud Service Providers are equal. Most CSP's have come from an IT infrastructure or data-centre background and offer basic services only; such as Infrastructure and Platform as a Service. The majority of whom offer these services on dedicated server hardware; such as 1u or 2u Servers, or on dedicated blade architecture, some with shared storage. These environments are rarely optimised and services rarely.

Most CSP's are themselves traditional organisations, they target and report traditionally and use standard IT service management tools, systems and processes. By all intense and purposes, they are traditional organisations.

For these reasons many key CSP's are struggling; many have folded, including some very big names, including HPE and Cisco, two for the biggest names in Cloud have failed as Cloud Service Providers.

Cloud9 firmly believe in doing things differently and have continually been re-engineering the business to transform from a traditional IT service provider to a Cloud Services Provider. Everything we do is around optimisation, Business Process Management and continual performance improvement.

Cloud9 offers Organisations the ability to move whatever they want, however they want, whenever they want to a single Cloud platform that can be certified with full platform governance and security.

Cloud9 v Public Cloud

Public Cloud looks cheap and is seem as a known entity that many organisations are trying to move to, as they have been for a very long time. Makes you as the question; why is it taking so long? Well Public

Cloud simply isn't the answer for UK Public Sector. Azure and AWS are trying to force it to work however fundamentally it does, the key reasons are:

1. The vast majority of organisations moving to Cloud need to re-architecture services for the Cloud. You get no assistance from AWS or Azure to do that.

2. You pay for it regardless of how good it is or how well it works for you.

3. Pricing is complex and unpredictable additional costs of secure connectivity

4. Moving from complex onsite capex model to complex – Multi-Cloud opex environment, hard to govern, test DR, document and secure

5. Lack of direct support, exposed to vendors maintenance procedures

6. Higher number of outages and incidents

7. Lower performance and higher total cost

2. Support for Shared Service

Many authorities are merging to moving towards shared services, which presents significant infrastructure and network challenges. Essentially Cloud9 are able to treat a Shared Service environment as a single organisation or as a multitude of three organisations; two individual and a single shared services environment.

Shared services has a significant focus around access control, monitoring, security, networking, data management and service migration. These environments are often evolving over a period of time and Cloud9 are able to securely support the every changing requirements of the users, individual organisations and shared services environment.

3. Cloud9 & Data Centre Certification

Cloud9 does not own any data centre facilities, we collocate with best of breed providers to suit the purpose of delivering highly scalable, secure and robust services that are geographically dispersed.

At a minimum our Data Centre environments meet IL3 standards with ISO 27001 compliance.

We only use UK mainland Data Centre facilities.

Our current Data Centre footprint includes:

- Manchester – PCI Compliance, PAS 2060, Cyber Essentials, ISO 9001, 14001, 27001 NICEIC

- Hayes – Tier III, List X

- London – ISO 27001, ISO50001

- Newbury – IL3, PCI Compliance, ISO271001

Innovate (who own the Cloud9 brand) are working towards ISO 27001 and expect to have this in place during May 2017.

We are happy to accommodate customer requests for certification or additional security levels for specific purposes, this will be done on a case by case basis where the Requestor will cover the sponsorship of a submission and the associated costs.

4. Services Available on G-Cloud

Cloud Hosting – Infrastructure as a Service

Cloud9 offer full Infrastructure and Platform as a Service which covers:

- HyperV
- VMWare
- XenServer
- KVM

We charge for Infrastructure based on:

1) CPU & RAM
2) Class and type of storage (Block or Object) including variable IOPS
3) Dedicated element such as Cisco ASA, load balancer
4) Network Interface
5) Dedicated Network port
6) Janet connectivity
7) Bandwidth
8) Level of Professional Services required

Cloud Hosting – Platform as a Service

Cloud9 supports a multitude of platform operating systems and database technologies as standard, you can you a standard build which you can modify or add a corporate template build to your dedicated UI. Platforms include:

Microsoft:

- Windows Server - 2012r2, Essentials, 2012 Datacenter, 2008, Remote Desktop
- SharePoint
- SQL Server
- BizTalk Server
- Visual Studio
- Dynamics

Linux:

- Ubuntu
- Coreos
- Centos
- Suse

Oracle
Puppet Labs

Cloud9 offers either platform monitoring only, which includes an option for Cisco FirePower for network level IDS/IPS and traffic monitoring, or Managed Platforms.

Managed Platforms

Here you can select what level of support you require on which servers or services you need. Our Cloud9 architects can provide:

1. Monitoring only
2. Environment performance – actively assist with platform and service performance and density to support user experience and total capacity
3. Patching & Maintenance – whereby Cloud9 will add your servers (all or individual) to our patching schedule, we can also accommodate bespoke patching schedules to reduce business impact

For Platform as a Service we charge as above but including:

1) Operating System Licensing (if required, we can use expecting licensing is most cases)
2) 2nd Line Support (we don't offer 1st line end user helpdesk)
3) OS or Database Patching & Maintenance

Back-up, Disaster Recover & Business Continuity

Back-up allows you to point a back-up agent from your Hypervisor or machine to Back-up location on the Cloud9 environment. Back-ups are encrypted as sources, over the wire and at rest.

Disaster Recovery allows you to restore a back-up to either a machine on your network or to a Cloud9 server that is made available to you on a dedicated vLAN.

Business Continuity allows you to have fully available hot standby machines (or load-balanced in an active/active configuration) pre-deployed on a dedicated, highly secure Cloud9 vLAN.

These 3 options vary in terms on Restore Time, Point & Device Objective.

Veeam

Cloud9 fully supports Veeam, including Veeam Cloud Connect

Infrascale

Cloud9 also work closely with Infrascale which can be a suitable alternative to Veeam in certain circumstances.

Virtual Desktop Infrastructure

As a VDI specialist Cloud9 supports Citrix XenServer, XenApp & XenDesktop. We have a team who specialise in just optimising the VDI environment, from storage, networking and at the Citrix level. We work closely with customers to look at VDI performance and deployment optimisation as well as application sequencing and distribution.

We charge for VDI based on:

- CPU, RAM & HDD per VDI

- VDI Image creating

- VDI Image management & patching

- VDI 2nd Line Support (we don't offer 1st line end user helpdesk)

- Windows OS licensing (where required)

- Microsoft Office

Microsoft Applications – Software as a Service

Also available are Microsoft Applications, based on Infrastructure and Platform services as described above, including:

- SharePoint

- CRM

- Skype for Business

- SQL

Software as a Service

Cloud9 has a number of Software vendors who use the Cloud9 platform to provide SaaS to end customers, they are available through Cloud9 (we act as a reseller and don't directly support these applications) or from the Software Vendor, and these include:

IOCOM

[IOCOM](#) – Advanced Collaboration and video Conferencing, focused on NHS, Education, Public and Private sector, highly innovative, lower cost and higher performance.

The IOCOM Visual Business Platform (VBP) enables organisations to connect and collaborate internally and externally with their customers, business partners and suppliers in real-time and without boundaries. Organisations can use IOCOM directly from Cloud9, it is the best solution when you cannot be physically present but want all of the benefits of highly sophisticated, face-to-face interaction and the power of unlimited image/data sources and screens.

IOCOM is engineered differently than other video conferencing platforms using patented technology that enables unlimited independent data, audio and video streams. It can be deployed as a hosted service or as a completely private solution to meet the highest security requirements with advanced encryption capabilities.

Leveraging the power and scalability of Cloud9, the IOCOM is a software based solution is used by clients ranging from the cross-platform native IOCOM (Windows, OS X / MacOS, Linux, iOS, Android, and WebRTC) to White/Private labelled versions and custom integrations using native client or web based APIs. Interoperability features include meeting participants from H.323, SIP and PSTN endpoints.

IOCOM are an existing Cloud9 customer and use the Cloud9 platform to deliver service, this allows us to monitor and maintain performance and work closely with them for support and development.

Netsweeper

[Netsweeper](#) are an Industry leader in Content Filtering and Internet Security including Prevent for Education, with a significant market share in this sector. Focusing on OFCOM compliance, Prevent and anti-radicallisation.

Key features:

1. Cloud9 Based Granular Filtering

2. Real Time Categorisation: https://www.netsweeper.com/live-stats/

3. 90+ different categories with billions of URLs categorised to date

4. A complete selective SSL filtering solution for categorising encrypted HTTPS websites

5. Dynamic malware protection and security

6. A Prevent duty of care category list

7. Intuitive customisable alerting and report

8. Deployed in minutes

9. Per user filtering available with Active Directory

10. Filtering in over 30 different languages

Key benefits:

1. Real-time classification of User requests

2. 0 Hour detection of web threats

3. Central Policy Enforcement, Reporting and Logging

4. Reduce risks of inappropriate web sites being accessed

5. Automated daily, weekly, monthly reporting

6. Per user filtering and reporting

7. Delegated Management for devolved control and multi tenancy of the system

8. Improve productivity by restricted access to business related web sites

9. Compliant with UK Government mandated law

Netsweeper are also a Cloud9 customer and use the platform to service customers in various sectors including Education. Cloud9 work closely with the infrastructure team at Netsweeper to ensure service performance.

Exchange as a Service

Cloud9 can provide Exchange as a Service to users, this can be either as a dedicated Exchange Server instance or on a multi-tenancy – per mailbox service.

Anti-Spam – MailCleaner

MailCleaner is a business anti-spam gateway installed between your mail infrastructure and the Internet. It offers professional protection against viruses and eliminates up to 99% of spam.

Skype for Business

Cloud9 offer Skype for Business on dedicated servers supporting your Unified Communication requirements. It is possible to also use Skype for Business as a PBX replacement for VoIP however this requires significant configuration and can be costly, other VoIP services can integrate with Skype for Business that can be significantly easy to manage and lower total cost of ownership.

Tute

Tute offer a remote teaching experience design to support at home learning for additional tuition and to assist schools with substitute teachers. Home learning is extremely popular, highly secure and allows multiple pupils to share the cost of additional tuition. In the UK Schools spend over £1bn for substitute teachers, have them on demand, anywhere and at short notice, solves significant challenges. Remote teaching is also applicable to other sector such as rehabilitation and reform of prisoner through re-education.

Our teachers use our award-winning Learning Cloud to support the very best interactive and engaging lessons. Students really love learning with Tute, with 91% of pupils in recent research saying that they enjoyed their small group lesson, with 96% feeling safe.

Service Features:

1. Delivery of synchronous and asynchronous online teaching

2. The Learning Cloud enables access to Tute interventions and courses

3. Safeguarded platform (lessons are recorded) and fully SEND compliant

4. Available in 71 different languages

5. No need for specialist equipment as accessible via a browser

6. Bett award-winning service for teaching, learning and assessment

7. Simple VLE-type functionality for asynchronous support and feedback

8. Attendance reporting available with auto-absence notification and prompts

Service benefits

1. Cloud platform allows for differentiated learning and digital literacy reinforcement

2. Anytime, anywhere access to live teaching on demand

3. Support pupils out of school via online teaching

4. Extend teaching provision into evenings, weekends and school holidays

5. Reinforce digital literacy skills in students

6. Re-engage with disaffected pupils who are unresponsive in traditional classes

7. Recorded lessons ensure safeguarding, and quality assurance

8. Catalyse improved parental engagement

9. Browser-based access, so no downloads or specialist equipment needed

Professional Services

Cloud9 offer a full range of professional services to effectively support customers. We also subcontract to 3rd parties for specific services, these include:

Stable Logic - Cloud Readiness and Transformation Consultancy

StableLogic are an independent consultancy comprising auditing, benchmarking, cloud business case development and transformation. Strategy development of cloud service migrations including SaaS, PaaS and IaaS. Extensive cloud telephony and contact centre experience. Advice on the implications for WAN, LAN, Storage, Compliance, PCI-DSS, Security, Risk and impact of service levels and support.

Key features:

1. Audit of applications, licences, hardware, storage, network and telephony

2. Cost and service quality benchmarking - on-premise vs cloud

3. Business case analysis and development, including public sector discounts

4. Strategy Development comprising costs, service delivery and service support

5. LAN and WAN review and optimisation for cloud services

6. Cloud PBX and Contact Centre strategy and cloud transformation

7. Requirements gathering and development of specifications and statements of requirement

8. Cloud procurement support with extensive public sector procurement experience

9. Service Design including review of team roles and skill requirements

10. Cloud service management including cost auditing, performance reviews and management

Key benefits:

1. Identify cost savings from cloud transformation

2. Comprehensive list of all services, systems and applications

3. Business case and migration plan to facilitate the cloud migration

4. Confidence in the cloud service and support arrangements

5. Reduced costs by optimising the cloud service design

6. Optimised service levels for users from redesigned network

7. Telecommunications and mobile cost reductions and service improvements

8. Enhanced delivery to Service Users from increased responsiveness

9. New communication options for Service Users from cloud contact centres

10. A comprehensive technical plan, applications, platforms and networks

5. Purpose & Scope

This Service Description is for G-Cloud procurement and is a generic document to describe the Cloud9 services available on the G-Cloud framework.

This document accompanies the CCS Call Off Agreement with details of a Services ordered and a Statement of Works, it will also detail the specific commercial terms and deliverables.

6. Definitions

Definitions. Unless otherwise defined herein, the following capitalized terms shall have the following meanings:

"Acceptable Use Policy" means our acceptable use policy, as set out in Appendix 1 to this Service Description.

"Administrator" means the End Customers nominated administrator who has the authority to purchase Cloud Services and manage those services on the End Customers behalf.

"Cloud9", "we" and "our" means Innovate Limited and "you" means you, the End Customer.

"Cloud Services" means Cloud9's cloud services as set out on and provided through the Cloud Services Portal, and as further defined in this Service Description.

"Cloud Services Portal" means the Cloud9 Internet site for discovery, browsing, subscribing, consumption, reporting and customer administration of the Cloud Services.

"End Customer" shall mean the organisation using the Cloud9 Services delivered by Innovate.

"Hardware" means servers, telecommunications and other equipment that are listed in a Schedule or Statement of Work, if applicable, and that are to be supplied either by Innovate ("Innovate-Supplied Hardware") or the End Customer ("the Customer-Supplied Hardware") for the purpose of rendering the Services.

"Initial Term" means one month from the date we advise you that the Cloud Services are available for End Customer use

"Innovate-Supplied Software" means software provided by Innovate as listed in a Statement of Works or Sales Order and that may be accessed by the End Customer solely in connection with the use of the Services. Innovate-Supplied Software is not licensed to the End Customer.

"Microsoft Licence Terms" mean the licence terms as set out in Appendix 2 to this Service Description, as may be amended by Microsoft from time to time.

"Protected System" means the complete backup of Cloud9's operating environment and critical files of a specific computer or server, necessary to ensure its functionality.

"Service Levels" or "SLA" means the service levels that apply to the Cloud Services as set out in this Service Description for each Cloud Service

"Services" means the services (including all associated Innovate-Supplied Software and Innovate-Supplied Hardware) purchased by the End Customer as described in a Statement of Work or Sales Order.

"Software" shall mean all software in object code form, provided by Company for installation on Cloud9's computer(s) or hardware system(s) through which the Service is accessed. The Software will include all documentation, Updates and Upgrades, if any, which are made available to Cloud9 hereunder.

"Statement of Work" or "SOW" means a statement of work delivered to the End Customer.

"Standard Terms" means Cloud9's standard terms for business customers.

"Third-Party Software" means any Software that is owned by a third party and licensed by the End Customer either from a third-party vendor or through Innovate pursuant to a separate agreement or Statement of Work, as applicable, and excludes Innovate-Supplied Software.

"Uptime availability failure" shall mean a complete failure of all services resulting in Customer being unable to perform any actions whatsoever. For the avoidance of doubt this excludes any single service or component.

7. Suspension or Termination

7.1. Any rights for Innovate to suspend or terminate the Cloud Services are in addition to our rights to suspend or terminate End Customer service under the Terms.

7.2. We may suspend or cancel any or all of the Services and you must continue to pay all charges relating to the relevant suspended services during the period of suspension if we reasonably believe that the End Customer is in breach of:

7.3. the Acceptable Use Policy;

7.4. the Microsoft Licence Terms;

7.5. the terms and conditions set out in this Service Description; or

7.6. any user guides provided by us.

7.7. In addition to our other rights to cancel or suspend the Cloud Services, we may also suspend or cancel the Cloud Services (but without you incurring any charges relating to such services during the period of suspension) due to a reasonable suspicion on our behalf that the continued provision of a product, service or feature may compromise the security of our service platform, for example due to hacking attempts or denial of service attacks or a vulnerability discovered in relation to a particular item of technology which we use to deliver the Cloud Services.

7.8. Where we suspend or cancel any or all of the Cloud Services, we will provide you and the End Customer with as much notice as is reasonably possible in the circumstances prior to suspending or cancelling the services.

8. Acceptable Use Policy

The End Customer must use the Cloud Services in accordance with the Acceptable Use Policy as detail in Appendix 1.

9. User and Responsibility Guides

The End Customer must follow our reasonable directions in relation to:

1. use of the Service; and

2. the data that is stored or hosted as part of the Service

We may provide user guides relating to the Cloud Services which will set out relevant technical information related to the Services as well as instructions for use.

10. Help Desk

10.1.   The End Customer will contact the Cloud9 Help Desk directly for Support with the Service. Innovate will provide a Customer Incident Number to the End Customer and manage the incident to resolution with the End Customer.

10.2.   The End Customer must provide details of key personnel who are Administrators of the Service, have completed 1st line diagnostics and can provide error logs to Innovate when contacting the Help Desk. The details of the End Customers key personnel will be in project plan once a SoW or Sales Order has been signed by the Parties.

11. Cloud Services Portal

11.1.   As part of the Service, we will provide the End Customer Administrator with a user account and password enabling access our online Cloud Services Portal so that they can administer them.

11.2.   The accessibility and functionality of the online Cloud Services Portal may be affected by the end Customers internet connection, browser and/or the computer system being used.

12. Security

We aim to protect our equipment and service platform against intrusions, viruses, trojan horses, worms, time bombs and other similar harmful software which may affect the Service, as well as vulnerabilities which may expose our equipment and service platform to the risk of intrusion or attack. We do not, however, guarantee such protection.

Failure by the End Customer to comply with any of the terms detailed in this clause 10 will be deemed a material breach of the Agreement and Innovate reserves the right to suspend or terminate any or all Service with immediate effect.

12.1. End Customers' must take steps to prevent unauthorised access to the Service and our service platform, for example, by not disclosing security credentials (such as user names and passwords) related to the services purchased as part of the Cloud Services.

12.2. End Customers' are responsible for the use of the Cloud Services by their users.

12.3. End Customers' are also responsible for maintaining the confidentiality of passwords and all activities that occur under the End Customers' password.

12.4. The End Customer must notify us immediately of any unauthorised use of any password/s or any other breach of security related to the Cloud Services Portal or the Cloud Services.

12.5. The Cloud Services do not include the following security features:

- For the server: intrusion detection, intrusion prevention, anti-virus and host intrusion protection; and

- For the network: network intrusion detection and network intrusion prevention.

12.6. The End Customer agrees not to access or attempt to access the Cloud9 internal network

12.7. The End Customer must have written authority from Innovate to perform any type of penetration testing in relation to the Cloud Services

13. Service Software

13.1. We use Software to provide the Service. We do not guarantee that such software is error-free.

13.2. As part of your Service, we may provide a non-exclusive, non-transferable licence to use certain software ("Service Software") for the sole purpose of End Customers' accessing and using the Service.

13.3. The End Customer must comply (and ensure that all users comply) with all licence terms applicable to the Service Software, this Service Description, the Terms and the Microsoft Licence Terms set out in Appendix 2.

13.4. Because of the nature of the Cloud Services, which are made up of technology and services provided by our third party suppliers, we may not have control over certain terms and conditions which the third party supplier requires the End Customer to accept or otherwise enter into when using the Service.

13.5. We will endeavour to provide the End Customer with a copy of these third party terms and conditions.

13.6. If the End Customer does not agree to the third party terms which we provide, we may not be able to provide certain products, services or features. By accepting the third party terms and conditions, the End Customer must comply with those terms and conditions. Failure to do so may

result in a material breach of Terms of Service and we may be required by the relevant third party to cancel the Service.

13.7.   Except as permitted by law, the End Customer must not (and must ensure that all users do not):

- remove any copyright, trade mark or similar notices on the Service Software;

- attempt to reverse engineer, decompile, disassemble, or derive any part of the source code of the Service Software; or

- modify, translate, or create derivative works based on the Service Software.

13.8.   The End Customer must install Service Software, other software, upgrades and patches as directed by us. If you fail to do so, we may suspend or refuse to support the Service.

14.   End Customer Software

14.1.   The End Customer must not use third party applications in connection with the Services which have licence terms and conditions which conflict with or could cause a to breach the Terms of this Service Description.

14.2.   Where the End Customer uses third party software, they are solely responsible for all terms of service and use of that software; including its licensing, maintenance and integrity.

15.   End Customer Data

15.1.   If we host or store data as part of the Service, the End Customer grants us a licence to host or store data for all purposes required for or related to our provision of the Services.

15.2.   If we do not think that any aspect of the data meets certain required standards or is illegal, we may suspend or cancel the Service until such data has been removed. Some examples of data that does not meet our standards includes pornographic, offensive or defamatory content or content that promotes hate or violence.

15.3.   Unless agreed otherwise in a Statement of Work, the End Customer is responsible for backing up all aspects of the data, including applications, databases, files and folders. Notwithstanding any other clause in this Service Description or any other terms between us, we are not liable for any loss or corruption of data irrespective of how such loss arose.

15.4.   We may delete End Customer data immediately on expiration of Services. The End Customer is responsible for transferring data elsewhere.

16.   Privacy

16.1.   Only in order to deliver or Support the Services, we may be required to and the End Customer agrees to allow us to disclose personal information we collect from the End Customer and

any users to third parties such as our suppliers, contractors and third party service providers (or their suppliers). These will be in specific circumstances such as for Virtual Desktop Infrastructure. All our Suppliers are bound by confidentiality and we share the minimum amount of information as required

16.2. The End Customer must ensure they have taken all legally necessary steps to allow us and our third party suppliers to collect personal information from any users of the Service and to use, disclose, store and transfer such personal information. The End Customer agrees to indemnify us against any claim, cost, loss or liability which may arise in connection with your failure to do so.

17. Take Down Notices and Directions

17.1. The End Customer must promptly notify us if they receive any mandatory take-down, service cessation or link deletion notices from any regulatory authority that relates to hosted content or data stored on our services platform. The End Customer agrees to promptly comply with any such notices and directions.

17.2. We may immediately disable or suspend to hosted content by written notice if:

- The End Customer fails to comply with, or we receive, any mandatory take-down, service cessation or deletion notices from a regulatory authority that relates to hosted content or data or any part of the Service; or

- we reasonably suspect that hosted content or any part of the Service breaches any laws, regulations, determinations or industry codes applicable to the Service or hosted content, or infringes the rights (including intellectual property rights) of any person or organisation.

18. Intellectual Property

18.1. Where we provide documents, processes, service configurations or software as part of the Service, we (or our licensors) will:

- continue to own the intellectual property rights in those materials; and

- grant a non-exclusive, non-transferable licence to use that material solely for purposes required for use of the Services.

18.2. The End Customer agrees to immediately inform us if they become aware of any infringement or suspected infringement of our intellectual property rights.

19. End Customer Records

19.1. The End Customer is responsible for ensuring that they comply with all laws or regulations which require them to retain certain records, data and information.

20.   Virtualisation

20.1.   Many of the products, services and features provided under the Cloud Services are provided through the use of virtualisation technology and the End Customer shall acknowledge and agree that the hardware and software that we use to provide the Service may be shared with other customers.

21.   Billing

21.2.   We will commence billing for the Services from the date we advise the Service is live and has been Accepted by the End Customer.

22.   End Customer Acceptance

22.1.   Innovate will notify the End Customer by email when the Service has been implemented and is ready for testing or hand-over. The End Customer shall have a period of 10 working days from the date of receipt of the notification to complete any testing. After this period the Service will be Accepted by the End Customer, unless the End Customer identifies a major failure during testing or the Service is unfit for purpose.

22.2.   The End Customer may reject the Service and the Service will be Not Accepted. Innovate will put right any failures within 30 working days, after which period if Innovate cannot remedy the failures the End Customer can Reject the Service and forthwith terminate the Statement of Work or Sales Order.

23.   Cloud Services - Detailed Service Description

In addition to the General Terms above, the following terms apply to Cloud Services.

Cloud Services including Cloud Servers consist of computing infrastructure on demand which can include:

- Virtual CPU, RAM or Storage

- Virtualisation technologies hosting virtual machines

- Software Appliances such as a Firewall or load balancer

- Software Defined Networking

- Network Interface or Public IP Address

- Server monitoring or management

- Operating System (see below for further details)

- Virtual servers of various sizing configurations, with a Windows Server 2008 R2 64Bit, Windows Server 2012, Windows Server 2012 R2, Redhat Linux, CentOS, or Suse Linux operating system;

- Storage management and backup management of the configuration of the virtual server; and

- Data centre network management, including installation, management and monitoring of the data centre network.

- Software as a Service such as; Microsoft Exchange, SharePoint

- Virtual Desktop Infrastructure

- Back-up, Disaster Recovery or Business Continuity Services

All Cloud Services will be provided from data centres located in England unless otherwise detailed in a Statement of Works.

24. Services

24.1.   Cloud Services provide dedicated and virtualised infrastructure resources that are located in managed data centres and delivered as a Service.

24.2.   Cloud Services can be used in the following configurations:

24.3.   Virtual Private Cloud. You can combine Cloud Services (Cloud Server) with Cloud9 IP-VPN (Private IP) to create a Virtual Private Cloud service. The Cloud Servers in this configuration exist within a private sub-compartment and only be accessible from the IP-VPN or a direct IP connection via a pre-authorised dedicated connection.

24.4.   Public Accessible Cloud. You can combine Cloud Services (Cloud Server) with a fixed broadband plan to create a publicly accessible cloud service. The Cloud Servers in this configuration exist within a public sub-compartment and a Managed Firewall component must be added to secure your service.

24.5.   The End Customer may choose from the following Cloud Service products:

- Cloud9 Server Managed with a managed operating system and disk (storage), CPU & RAM (memory) flex; or

- Cloud9 Server Unmanaged with a customer-managed operating system and disk (storage), CPU & RAM (memory) flex or

- Cloud9 Server Managed with a managed operating system and disk (storage) flex only; or

- Cloud9 Server Unmanaged with a customer-managed operating system and disk (storage) flex only

- With a Cloud9 Server, the End Customer may use the Cloud Services Portal to create and configure virtual servers to allocate CPU and RAM resources including virtual disks.

24.6.　　We do not provide physical access to the Service environment including server infrastructure.

25.　Operating System

The Service may include the provision of an operating system which is provided on the Microsoft Licence Terms set out in Appendix 2 of this Service Description.

The following actions are not permitted:

- Host name changes (these must be set out in the build sheet);

- Installation of non-Cloud9 provided operating systems or versions;

- Changing the size, the drive letter or other settings of the storage partition, even if where the capability exists due to being granted administrative rights.

26.　Customer Self-Managed Operating System Instance

26.1.　　Innovate will provide a customer self-managed virtual server that is reserved within the virtualised environment. The End Customer will receive root access and administration rights to the self-managed OS.

26.2.　　If the Service is impacted through the End Customers' use of the Cloud Services Portal, we will attempt to help reinstate the Service or recover data, but do not guarantee that we will be able to fully restore the Service or any data. Innovate may charge for such assistance.

26.3.　　The End Customer is responsible for sourcing, installing and configuring all end-point security software which they wish to install on any virtual servers (including anti-virus and intrusion prevention software).

26.4.　　Where Red Hat Enterprise Linux is requested as the operating system, the End Customer must accept Red Hat's Software Subscription Agreement for End Users in the Cloud (redhat.com/licenses/cloud_cssa/).

26.5.　　The End Customer accepts all risk of use of the Red Hat Enterprise Linux software, including without limitation, the risk of software being subject to the terms of the Software Subscription Agreement, with a requirement that the source code to such software be made publicly available.

27.　Managed Operating System Instance

27.1.　　Innovate will provide the End Customer with a managed virtual server that is reserved within the virtualised environment. This includes management, monitoring, security, antivirus and backup activities in connection with the Operating System. No administration rights are provided to the End

Customer, however for installation of application software, the End Customer will be granted administration rights.

27.2.   Where Red Hat Enterprise Linux is requested as the operating system, the End Customer must accept Red Hat's Software Subscription Agreement for End Users in the Cloud (redhat.com/licenses/cloud_cssa/).

27.3.   The End Customer accepts all risk of use of the Red Hat Enterprise Linux software, including without limitation, the risk of software being subject to the terms of the Software Subscription Agreement, with a requirement that the source code to such software be made publicly available.

28.   Storage

28.1.   We may provide End Customer access to storage capacity on our service platform that can be used by the Administrator for various purposes including to store data and applications.

28.2.   Multiple virtual disks are permitted. It is mandatory to have one (1) virtual disk for each server and is reserved for the operating system.

28.3.   The End Customer can add additional virtual disks via the Cloud Services Portal. The Administrator may select the size of further virtual disks. Virtual disks cannot be removed separately.

28.4.   The Administrator is responsible for ensuring that all disks provided under this Service have sufficient free storage capacity for system requirements and the operating system.

29.   Cloud9 Operational Activities

The following table sets out which operational actions Innovate will perform and components supplied in relation to the Infrastructure Services. Pricing for these elements are detailed in the Cloud Price Book.

	Cloud9 Managed OS	Customer Managed OS
Virtualisation Host Management		
Availability monitoring	Included	Included
Hardware management & monitoring	Included	Included
Virtual Server Services		
Server provisioning	Included	Included
Hypervisor patch management	Included	Not Included

Security management (configuration of options)	Included	Not Included
OS Backup	Included	Included
Data Backup	Included	Included
Operating System		
Provision of OS image	Included	Included
OS patch management	Included	Not Included
OS & hardware availability monitoring	Included	Not Included
Event detection & notification (availability, capacity & performance)	Included	Not Included
Antivirus protection (deployment & updates)	Included	Not Included
Server Description		
Server	Virtual	Virtual
Hypervisor (virtualisation layer)	Microsoft Hyper-V	Microsoft Hyper-V
End User Operating System	Current Version(s): Windows Server 2008 R2 64Bit, Windows Server 2012, Windows Server 2012 R2, CentOS 6 & &, Red Hat Enterprise Linux Server Rel 6	Current Version(s): Windows Server 2008 R2 64Bit, Windows Server 2012, Windows Server 2012 R2, CentOS 6 & &, Red Hat Enterprise Linux Server Rel 6
Fixed Storage Unit for OS (end user)	50GB	50GB
Additional Data Drive Storage Bundle options per server (GB)	50, 100, 250, 500, 750 or 1000	50, 100, 250, 500, 750 or 1000
CPU options per service instance (central processing units)	1, 2, 4, 6, or 8	1, 2, 4, 6, or 8
Gigabytes (GB) of RAM options per service instance	Increments of 1GB	Increments of 1GB
Encryption applied to each service instance	RDP native encryption. SSL and Two Factor encryption optional	RDP native encryption. SSL and Two Factor encryption optional

*References to "Included" mean that Cloud9 will supply the component or function as part of the Cloud Services (Cloud Server).

** Anti-virus software is not included with Red Hat Linux operating system instances

30. Roles and Responsibilities

The following table sets out the responsibilities for management of the Cloud Services

Function	Cloud9 Managed OS		Customer Managed OS	
	Cloud9	Customer	Cloud9	Customer
Maintain hardware standards	R		R	
Installation of OS	R	I, C	R	I, C
Maintain OS standards	R			R
Service installation, configuration and integration	R		R	
Management Software installation, configuration and integration	R			R
Application software installation, configuration and integration		R		R
Providing log-on credentials	R	I	R	I
OS Administration Rights	R			R
Virus protection	R			R
Backup – OS & data	R		R	
Security standards implementation	R			R
Patch and Release Management	R			R

Key: "R" = Responsible; "C" = Consulted; "I" = Informed

Note: To the extent that a particular function is identified as a customer responsibility (identified in the table by the letter "R"), this indicates that Cloud9 will not provide this function as part of the Cloud Services (Cloud Server).

* Virus protection is not included with Cloud9 Managed Red Hat Linux OS instance

31. Backup Services – Cloud9 Virtual Machine

Cloud9's Data Protection Appliance provides an integrated Data Protection Platform that includes cloud backup, archiving, and disaster recovery.

- Any Device, Any OS. Protect data and applications no matter where they live, including physical and virtual servers, laptops/desktops, and mobile devices. We support more than 50 versions of operating systems, including Windows, Unix, Linux, AIX, VMware, Mac, and Android.

- Single Pane of Glass. Now MSPs have a single, cloud-based management console to manage multiple clients, monitor backups remotely, and easily troubleshoot issues. No VPN or direct network access is needed to manage backups.

The Data Protection Appliance is a robust business continuity and DR solution equipped with leading-edge technology designed to minimize downtime, expedite time to protection, and simplify the data recovery process.

- Disaster Recovery as a Service. The Data Protection Appliance includes new DRaaS functionality that lets you "instantly" boot a protected server, right from the appliance or from the cloud.

- Agentless VMware Backup. Includes agentless "host level" backup to protect virtual machines without requiring any software on the individual VMs. Now, you can backup and restore entire VM images, specific files and folders, and automatically detect and protect newly created VMs.

- WAN Optimization: Our WAN acceleration technologies optimize network throughput of data between the appliance and the cloud, and include traffic shaping, bandwidth limiting, over-the-WAN deduplication, and resilient-resumption technology.

Backup services include the provision of backup for the operating system, data and databases to enable the restoration of data after an interruption or event which causes data loss.

Backups are accomplished by copying the specific data (OS disk and data disks) to a backup media in compliance with the features set out in the below table:

9.1. Encryption

UltraSafe Private Key Encryption accounts are protected with unique user-defined encryption keys. With UltraSafe Private Key Encryption, keys are NEVER stored or saved in our systems. This means absolutely no one is able to access files except for the account-owner. Note: Because of their nature, Cloud9 cannot reset the password or encryption of UltraSafe accounts. If you lose the password the data will be un-recoverable.

Cloud9 also offers double-blind encryption which is based on the premise that your data should be encrypted twice – once at the source side and then again in our cloud. Similarly, we encrypt your files on the source device with an encryption key that you hold, using UltraSafe's 256-bit AES encryption. Files are then transferred to and from the cloud via a Secure Sockets Layer (SSL) tunnel. Once the files arrive in our cloud, they are encrypted again with a second layer of encryption in which Cloud9 holds the key. The process of recovering the data requires a secure handshake where both keys need to be present in order to decrypt the data. Given recent security breaches, you should insist on this level of military-grade encryption.

9.2. Actions and Responsibilities – Back-up as a Service

This Service also covers Disaster Recover and Business Continuity as a Service, the use the same principles but some service elements may vary, these will be detailed in the Statement of Works or Sales Order.

Service	Actions	Requirements	Responsible
Requirements	Plan of back-up & restore points, include RTO	Detail of core and non-core applications and data sizes, elements to be backed-up and back-up schedule required	End Customer
Local seeding	Install seeding device into End Customer's environment (if part of the SoW)	8U of rack space with 1 x 1Gbps Ethernet Network Connection	Cloud9 & End Customer
	Configure the Virtual Appliances onto each network		Cloud9
Agent deployment	Push the backup agent onto each Server	Domain or Local Admin account require. Possibly requires additional SQL services if not already installed	End Customer & Cloud9
Scheduling	Build the schedules for each Server or task	Confirmation of the backup schedules + signoff required from End Customer	End Customer
Initial Seed	Perform an initial seed of the data	Increased monitoring required from End Customer to ensure that no services are impacted	End Customer
Migrate Data	Move the seeded date into the Cloud9 environment		Cloud9
Update Seeded Data	Perform an updated back-up of seeded data	Increased monitoring required from End Customer to ensure that no services are impacted	End Customer & Cloud9
Data Replication	Perform a site to site replication of the backup data	Increased monitoring required from End Customer to ensure that no services are impacted	Cloud9 & End Customer
Handover	Transition the Service in Business As Usual and	Technical handover to End Customer	Cloud9 & End Customer

	handover		
BAU	End Customer assumes full control of the service	End Customer monitors and managed to back-up services, ensure they are successful, completes restoration testing	End Customer

The customer is responsible for understanding the back-up and restoration objectives, this includes detailing the specific elements to back-up:

1. Data (files, folders)

2. Databases

3. Applications

4. Operating Systems

5. Full Virtual or Physical machine configuration

The customer should also detail the criticality of each service, application or server, this could cover:

1. Business critical

2. Important

3. Non-critical

For each we would expect to see a Restore Time Objective and back-up schedule requirement such as real-time, hourly, daily, weekly, monthly.

The End Customer has full responsibility for providing this data and ensuring they have set the right back-up schedules and have complete restoration testing.

32. Managed Firewall & Load Balancer

Managed Firewall provides a highly available, multilayer, stateful inspection firewall service. Stateful Inspection provides accurate and highly efficient traffic inspection with full application-layer state awareness for a strong level of security and scalability.

The Managed Firewall service offers full 24x7 management, monitoring and administration of all supported firewall devices.

The Managed Firewall allows a Public IP address to be assigned to an OSI via Network Address Translation (NAT), with rules for allowed access from the Internet to the OSI.

The End Customer must assign at least 1 Public IP address to use Cloud Servers in a Public Cloud configuration. Additional Public IP addresses can be purchased for an additional cost on request.

There is a monthly fee for each Public IP address. Internet bandwidth is limited to one of the following configurations: 1Mbps, 2Mbps, 5Mbps, 10Mbps & 100Mbps. Additional bandwidth up to 100Gbps is available and may be an additional cost.

Additional VLANs can be configured and firewall rules can be defined to support inter-VLAN traffic.

Managed Firewall change management is provided on the following basis:

- Lead time for change request: 3 days; and

- Change window: 8pm to 8am Mon-Fri

33. Cloud9 - Virtual Desktop Infrastructure (Desktop as a Service)

Cloud9 Desktop as a Service VDI is comprised of the following per user variables:

- Virtual CPU, RAM and desktop storage

- Microsoft Windows 7 or 8

- Microsoft Office Pro

- End Customer Golden Image

- Zero Client Terminal

Zero Client Terminals

- Configuration

- Hardware replacement & warrant

  o Where Innovate supply a Zero client as part of the service, it will come with a 3 year return to base warranty and helpdesk support

- Network Time Server

- Zero Client requirements – Out of the box the Zero client includes the unit and a power supply. The End Customer will need to supply the following components:

  o USB keyboard

  o USB mouse

  o Monitor

  o Monitor adaptor (DVI or Display Port)

  o Ethernet network cable

o   LAN/WAN Internal network

Image Management

Innovate will deliver the initial Golden image unless agreed otherwise in the Statement of Work. The End Customer is responsible for providing a complete desktop build sheet which details all the applications and driver required.

Once built the End Customer will test and Accept or Reject the Image, where rejected due to performance, Innovate will look to optimise the image to an agreed level of performance. Where the End Customer rejects the image due to having incorrectly specified the image requirements in the build document, Innovate reserve the right to change for Professional Service.

Once the End Customer has Accepted the image, the customer can either take responsibility for the management of the Image(s) which includes application and OS updates. Or request innovate to remain responsible for image management, which will be charges as Professional Services.

VDI Requirements

- Each user requires a minimum of 200KB (concurrent), this depends on applications and usage (voice, video and 3D graphics will require more bandwidth)

- The End Customer is solely responsible for the LAN/WAN including cabling and connectivity

- The End Customer is responsible for all network and user configuration components, including (unless agreed otherwise in the SoW):

    1. Active Directory

    2. Security Groups

    3. Domain's including Domain Controllers

    4. All other elements not specifically detailed in a Statement of Works or Sales Order

Appendix 1:

End Customer Acceptable Use Policy

Cloud Services

Cloud9 expects that You (the customer) will use the Cloud Services ("Services") in accordance with this Acceptable Use Policy ("AUP" or "Policy"). Any illegal, unauthorised, or improper use of the Services could be harmful to Cloud9, its suppliers, its licensors, other customers, the technological integrity of Cloud9 infrastructure, or Services, or may otherwise damage Cloud9's reputation.

Consequently, this Policy describes prohibited uses of the Services, including (but not limited to) the Market Place Portal. Cloud9 may modify this Policy at any time on 14 days' notice by emailing You.

By using the Services (including accessing the Market Place Portal), You agree to comply with this Policy. If You breach a material term of this Policy or authorise or help others to do so, and such breach remains un-remedied after reasonable written notice from Cloud9 (no less than 14 days), Cloud9 may suspend some or all affected Services or terminate Your use of the Services in accordance with the Standard Terms and/or the Service Description.

If a breach of a material term of this Policy involves any illegal activity conducted by You, then Cloud9 reserves the right to suspend the Services without providing notice.

This Policy forms part of the terms of the agreement for providing and use of the Services. You are solely responsible for violations of this Policy by You, including your employees or contractors.

Obligation to Report

In delivering the Services, Cloud9 provides the physical or virtual servers, related storage and other resources, and support services according to the terms of the Service Description.

In the course of delivering the Services, Cloud9 does not monitor, and may not be aware of, Your use of the Services, including Your loading and managing of Your application software, data or content. Except as needed to deliver the Services, as authorised by You, or as required by law, Cloud9 will not have access to Your application software, data or content.

Therefore, if You become aware of any violation of this Policy, You agree to notify Cloud9 as soon as reasonably practicable and cooperate in any efforts to stop or remedy the violation. To report any such violation or suspicion of such violation, You should contact the Cloud9 Help Desk on 0330 9991111.

Cloud9 may investigate any violation of this Policy or misuse of the Services or the Market Place Portal, although Cloud9 is not obligated to do so. Cloud9 may deem it necessary to report any activity that it suspects violates any law or regulation to appropriate law enforcement officials or regulators, without necessarily advising You.

Subject to Cloud9's obligations of confidentiality (a) such reporting in the preceding paragraph may include disclosing appropriate information, and network and systems information related to alleged violations of this AUP, the Standard Terms or the Service Description, and (b) Cloud9 may cooperate with appropriate public agencies or other appropriate third parties to assist with the investigation and prosecution of illegal conduct related to alleged violations of this Policy.

Accurate Information Required

You agree to use reasonable endeavours to provide accurate and complete information when You purchase or use the Services, and You agree to use reasonable endeavours to keep such information accurate and complete during the entire time that You use the Services.

No Illegal, Harmful, or Offensive Usage or Content

By using the Services, You represent that You will use the Services only in accordance with the Standard Terms, the Service Description, this Policy and with all applicable laws in all relevant jurisdictions.

You may not use, or encourage, promote, facilitate, or instruct others to use the Services for any use that is reasonably considered to be illegal, harmful, or offensive, or to knowingly transmit, store, or otherwise make available any content that is reasonably considered to be illegal, harmful, or offensive and in breach of this Agreement. These prohibited activities and content involve:

- Illegal activities, including disseminating, promoting, or facilitating pornography or any activity that is likely to be in breach of, or does breach, any applicable laws, codes, or regulations including data protection.

- Any offensive content that is defamatory, obscene, deceptive, abusive, an invasion of privacy, objectionable, or otherwise inappropriate.

- Any content that infringes or misappropriates the intellectual property or proprietary rights of others or assists others in infringing such rights.

- Any activity that is reasonably likely to be harmful to the Services or to Cloud9's or its suppliers' reputation, including engaging in any fraudulent or deceptive practices.

No Security Violations

You may not use the Services to violate, or attempt to violate, the security or integrity of any network, computer, or communications system, software application, or network or computing device ("System"). These prohibited activities include You taking, or attempting to take, any of the following actions:

- Accessing or using any such System without permission.

- Probing, scanning, or testing the vulnerability of such System, or breaching any security measures without express authorisation of the owner of the System.

- Monitoring data or traffic on any System without such permission.

- Falsifying the origin of any TCP-IP packet headers, email headers, or any part of a message.

- Gaining unauthorised access to the Services or any other accounts, computer systems, or networks, whether through hacking, password mining, reverse engineering, or any other means.

No Interference or Disruption of Services or Others' Networks, Systems, or Internet Connections

You may not make network connections to any users, hosts, or networks unless You have permission to communicate with them. You may not take any action, or attempt any action, that interferes with or disrupts the proper functioning of a network or system. These prohibited activities involve You taking, or attempting to take, any of the following actions (unless obligated by law or permitted otherwise under the Agreement):

- Engaging in any activity that interferes with or adversely affects other Cloud9 customers' use of the Services.

- Collecting information by deceit, under false pretences, or by impersonating any person or entity or otherwise misrepresenting Your affiliation with a person or entity.

- Using any content or technology that may damage, interfere with, intercept, or take unauthorised control of any system, program, or data, including, but not limited to, viruses, worms, or time bombs.

- Using the Services in any manner that appears to Cloud9 to threaten the Service Infrastructure. This includes You providing inadequate security, allowing unauthorised third party access, or attempting to circumvent Cloud9's measures for controlling, monitoring, or billing usage.

- Using viruses, worms, corrupt files, Trojan horses, or other forms of corruptive code, or any other content which may compromise the Services, Network or Computing Infrastructure operations, or its performance for other Cloud9 customers.

- Interfering with the proper functioning of any System, including any deliberate attempt to overload a System by any means.

- Monitoring or crawling a System so that such System is impaired or disrupted.

- Conducting or condoning denial of service attacks.

- Avoiding any use limitations placed on a System, such as access and storage limitations.

Appendix 2:

Microsoft Licence Terms

END USER LICENSE TERMS

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE

This document governs the use of Microsoft software, which may include associated media, printed materials, and "online" or electronic documentation (individually and collectively, "Products") provided by Cloud9 (hereinafter referred to as "Customer"). Customer does not own the Products and the use thereof is subject to certain rights and limitations of which Customer must inform you. Your right to use the Products is subject to the terms of your agreement with Customer, and to your understanding of, compliance with, and consent to the following terms and conditions, which Customer does not have authority to vary, alter, or amend.

1. Definitions.

"Client Software" means software that allows a Device to access or utilize the services or functionality provided by the Server Software.

"Device" means each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistant, "smart phone," server or other electronic device.

"Server Software" means software that provides services or functionality on a computer acting as a server.

"Software Documentation" means any end user document included with server software.

"Redistribution Software" means the software described in Paragraph 4 ("Use of Redistribution Software") below.

2. Ownership of Products.

The Products are licensed to Customer from an affiliate of the Microsoft Corporation (collectively "Microsoft"). All title and intellectual property rights in and to the Products (and the constituent elements thereof, including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Products) are owned by Microsoft or its suppliers. The Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the Products does not transfer any ownership of the Products or any intellectual property rights to you.

3. Use of CLIENT SOFTWARE.

You may use the Client Software installed on your Devices by Customer only in accordance with the instructions, and only in connection with the services, provided to you by Customer. The terms of this

document permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during your use of the Client Software.

4. USE OF REDISTRIBUTION SOFTWARE.

 In connection with the services provided to you by Customer, you may have access to certain "sample," "redistributable" and/or software development ("SDK") software code and tools (individually and collectively "Redistribution Software"). YOU MAY NOT USE, MODIFY, COPY, AND/OR DISTRIBUTE ANY REDISTRIBUTION SOFTWARE UNLESS YOU EXPRESSLY AGREE TO AND COMPLY WITH CERTAIN ADDITIONAL TERMS CONTAINED IN THE SERVICES PROVIDER USE RIGHTS ("SPUR") APPLICABLE TO CUSTOMER, WHICH TERMS MUST BE PROVIDED TO YOU BY CUSTOMER. Microsoft does not permit you to use any Redistribution Software unless you expressly agree to and comply with such additional terms, as provided to you by Customer.

5. Copies.

You may not make any copies of the Products; provided, however, that you may (a) make one copy of Client Software on your Device as expressly authorized by Customer; and (b) you may make copies of certain Redistribution Software in accordance with Paragraph 4 (Use of Redistribution Software). You must erase or destroy all such Client Software and/or Redistribution Software upon termination or cancellation of your agreement with Customer, upon notice from Customer or upon transfer of your Device to another person or entity, whichever occurs first. You may not copy any printed materials accompanying the Products.

6. Limitations on Reverse Engineering, Decompilation and Disassembly.

You may not reverse engineer, decompile, or disassemble the Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.

7. No Rental.

You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Products to any third party, and may not permit any third party to have access to and/or use the functionality of the Products except for the sole purpose of accessing the functionality of the Products in the form of software services in accordance with the terms of this agreement and any agreement between you and Customer.

8. Termination.

 Without prejudice to any other rights, Customer may terminate your rights to use the Products if you fail to comply with these terms and conditions. In the event of termination or cancellation of your agreement with Customer or Customer's agreement with Microsoft under which the Products are licensed, you must stop using and/or accessing the Products, and destroy all copies of the Products and all of their component parts.

 9. No Warranties, LIABILITIES OR REMEDIES BY MICROSOFT. ANY WARRANTIES, LIABILITY FOR DAMAGES AND REMEDIES, IF ANY, ARE PROVIDED SOLELY BY CUSTOMER AND NOT BY MICROSOFT, ITS AFFILIATES OR SUBSIDIARIES.

10. PRODUCT SUPPORT.

Any support for the Products is provided to you by Customer and is not provided by Microsoft, its affiliates or subsidiaries.

11. NOT FAULT TOLERANT.

 THE PRODUCTS MAY CONTAIN TECHNOLOGY THAT IS NOT FAULT TOLERANT AND ARE NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN ENVIRONMENTS OR APPLICATIONS IN WHICH THE FAILURE OF THE PRODUCTS COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL, PROPERTY OR ENVIRONMENTAL DAMAGE.

12. EXPORT RESTRICTIONS.

The Products are subject to U.S. export jurisdiction. Customer must comply with all applicable laws including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see http://www.microsoft.com/exporting/.

13. LIABILITY FOR BREACH.

In addition to any liability you may have to Customer, you agree that you will also be legally responsible directly to Microsoft for any breach of these terms and conditions.

Appendix 3
Service levels

SLA Priority Levels

1. The End Customer will contact the Company helpdesk directly or phone or by email

    a. Phone – 0330 9991111

    b. Email – support@innovate.uk.com

2. The End Customer must have completed first line support prior to raising a Support Incident with the Support Desk

    a. The End Customer must detail the remedial actions taken and the incident details

    b. The End Customer must be able to provide error logs and details of the incident

3. The Company will provide the Customer with a unique incident number

4. The Company will provide support 7am – 7pm, 7 Days a week (excluding public holidays)

5. Only approved named End Customer contacts can raise Incidents with the Company Help Desk

6. Impact is a measures the effect of an Incident. Impact is often based on how service levels are affected. The Service Desk ticketing system codes are as follows:

Code	Urgency	Example
1	Extensive/Widespread	An incident affecting the entire campus or a critical process like payroll or instruction in multiple classes, or is university-wide.
2	Significant/Large	An incident affecting multiple departments, one college/division, instruction in one class or a building.
3	Moderate/Limited	An incident affecting multiple users or a department or a standard process that's not critical.
4	Minor/Localised	An incident affecting one or few users or a non-critical process.

7. Urgency is a measure of how long it will be until an Incident has a significant impact on the Business. For example, a high Impact Incident may have low Urgency, if the Impact will not affect the university until the end of the quarter. The Service Desk ticketing system codes are as follows:

Code	Urgency	Example

1	Very High	A full service outage of a critical system. System is non-operational. Urgent response.
2	High	An incident that disrupts a users' ability to do work or an issue that partially impacts a very important person or process. Quick response.
3	Medium	An incident that partially impacts the user's ability to do work or one for which a workaround exists. Assistance is needed. Response as soon as possible.
4	Low	An incident that has no impact on users' ability to do work. Response is not critical.

8. Priority identifies the relative importance of an Incident. Incident priority is based on the combined Impact and Urgency assignments, and is used to identify the required action times. Priorities are assigned by the Service Desk.

		Impact			
		Widespread	Large	Limited	Localised
Urgency	Critical	P1	P1	P2	P2
	High	P1	P2	P2	P3
	Medium	P2	P2	P3	P4
	Low	P2	P3	P4	P4

9. Response and Resolution Targets

Priority	Response Target	Resolution Target
P1	30 Minutes	2 Hours
P2	1 Hour	4 Hours
P3	2 Hours	8 Hours
P4	4 Hours	16 Hours

Cloud9 Helpdesk & Support Services

Elements provided and covered by Innovate for the Services

- 2nd line Help Desk Support for all IT assets in Schedule A

- Service Management & maintenance

- Incident Management

- Cloud9 Hardware Support on assets detailed in Schedule A.

- Cloud9 Software Support on software detailed in Schedule A

- Remote Cloud9 Managed Service

- Cloud9 status monitoring and altering

- Cloud9 capacity monitoring

- Cloud9 Reporting

Elements NOT covered by Innovate

- Onsite Support

- 1st line support

- Data centre environments

- LAN & WAN network & connectivity

- Installation and configuration of new Services

- Installation and configuration of new Hardware

- Re-creation of irrecoverable data

- Customer Data

- Contractual issues between the Customer and Customers 3rd party suppliers

- Bespoke software, application and website support and development

- Customer Supplier Software and databases

- End user training

- Moving (either physically or logically) the existing Systems

- Changes to the Systems or Services

- Errors caused by the Customer or any of its nominated 3rd parties

Cloud9 Core Service Availability and Service Credits

Cloud9 Core Services Availability	Percentage of Service Credits Due
Cloud9 Services Availability 99.99% or Higher Less than or equal to 43 minutes downtime	None
Cloud9 Services Availability 99.5% - 99.89% From 44 to 220 minutes of downtime	5%
Cloud9 Services Availability 99.49% - 99.00% From 221 minutes to 438 minutes of downtime	10%
Cloud9 Services Availability 98.99% - 97.00% From 438.1 and 1296 minutes of downtime	15%
Cloud9 Services Availability 96.90% - 96.00% From 1296.1 and 1728 minutes of downtime	20%
Cloud9 Services of less than 96.00% More than or equal to 1729 minutes of downtime	25%

Escalation Process

Once an error has been logged an Incident will be escalated one of two ways.

Functional Escalation – Where the an Innovate engineer does not have details of known error or knowledge base articles relating to an identical or similar type of error and the engineer is not suited to trouble-shoot the error he/she will escalate immediately to the next Escalation Point.

Timed Escalation – Where the an Innovate engineer has details of a known error or knowledge base article outlining the fix and/or steps to trouble-shoot the issue further he/she will be given an amount of time before there is a recommendation for escalation. The escalation will take place in accordance with the table below except if the engineer is actually implementing a fix or workaround which is time dependent and it is deemed by the Service Desk team leader that an escalation will only prolong the time to implement a fix.

Priority	Time To Escalation	Escalation Point
Priority 1	30 Minutes	Top Tier
Priority 2	1 Hour	Top Tier
Priority 3	2 Hours	Next Tier
Priority 4	12 Hours	Next Tier
Priority 5	N/A	N/A

Service Credit Exceptions

The Customer is limited to receiving an aggregate Service Credit of 50% for the applicable calendar month under all SLAs between the Customer and Innovate.

Service Credit will not be issued under this SLA for any Covered Services outage that, as determined by Innovate in its reasonable judgment, results from:

The Customer-initiated changes, whether implemented by the Customer or Innovate on behalf of the Customer;

The Customer exceeding system capacity;

Viruses, except to the extent that such outage results from a failure to apply a generally available and approved countermeasure within six hours of a documented outbreak.

The Customer's failure to adhere to Innovate's change-management process and procedures;

Force Majeure or natural disasters;

Any event or condition not within the reasonable control of Innovate;

Violations of Innovate's Acceptable-Use Policy;

The negligence or wilful misconduct of the Customer, its agents or others it authorized to use the Services;

Any failure of any component for which Innovate is not solely responsible, including, without limitation, all the Customer-provided or the Customer-managed electrical-power sources, networking equipment, computer hardware, computer software or website content;

Any failure of the Customer-provided local-access facilities;

Any scheduled maintenance up to an accumulated total of 16 hours per month, provided that four business days' standard notification of the scheduled maintenance event is given;

Any emergency maintenance up to an accumulated total of four hours per month, provided that (a) the need for emergency maintenance prior to a scheduled-maintenance window can be established, (b) delaying the maintenance presents a material risk of unplanned downtime and (c) a minimum one hour's standard notification is given;

Any failures that cannot be corrected because the Customer is inaccessible; or

Incorrect or inadequate configuration of Cloud9 resources (including without limitation all the Customer-managed Services) by the Customer.