Cloud Direct

Cloud Direct Enterprise Mobility and Security Service Level Agreement

Revision 2.0

Contents

1 Document Control

Please be advised, we reserve the right to change or amend this agreement from time to time. Please ensure that you are referring to the latest revision of the Cloud Direct Enterprise Mobility and Security Service Level Agreement available from the PROVIDE™ portal.

2 What is Enterprise Mobility and Security?

Enterprise Mobility and Security (EMS) is a cloud based, subscription version of a range of Microsoft products. Available through the internet, EMS provides the means of managing challenges that arise from enterprise mobility and bring your own device (BYOD). It encompasses four areas of mobility protection; identity and access management (Azure Active Directory), mobile device and application management (Microsoft Intune), securing content (Azure Information Protection) and shadow-IT audits and behaviour based analytics (Microsoft Cloud App Security). By purchasing these licences through the cloud model, you can scale your licences according to your needs and maintain the latest technology within your business.

The EMS services covered by this SLA are:

- Enterprise Mobility and Security E3 and E5
- Azure Active Directory; Basic and Premium P1 and P2
- Microsoft Intune
- Azure Information Protection Plan 1 and P2
- Azure Multi-Factor Authentication
- Microsoft Cloud App Security
- The above licences for Government
- The above licences for Education

3 What is a Service Level Agreement (SLA)?

An SLA is a legally binding commitment to achieve a specific level of service. If this target is not achieved, the service provider will commit to compensating the customer based on previously established penalties. Consequently, a vendor willing to commit to an SLA is confident in the ability of the service and therefore creates customer reassurance.

Cloud Direct views an SLA as a two-way agreement in which you the Customer also acknowledge your responsibilities to ensure the smooth operation of the supplied Service.

In the critical area of electronic communications and flexible office productivity tools it is important that business users have robust, cost-effective and above all, consistent level of service and performance.

4 What is behind Cloud Direct's SLA?

'Cloud Direct' is the trading name for On Direct Business Services Ltd. Specialising in Mobility solutions, Cloud Direct are a leading broker of cloud services including backup and disaster recovery, collaboration and protection tools, communication services including broadband and leased lines, VoIP telephony / unified communication solutions, and a range of hosted server and desktop platforms. Cloud Direct holds ISO27001 (IT Security Techniques) and ISO20000 (IT Service Management) accreditations for the provision and support of Cloud IT backup, security and disaster recovery services.

Cloud Direct supports EMS technology delivered by Microsoft (NASDAQ :MSFT mkt. cap. $250bn). The Microsoft EMS service is ISO27001 accredited.

5 What is offered by Cloud Direct's SLA?

Cloud Direct is committed to providing exceptional customer service at every opportunity and our key customer satisfaction measure is Net Promoter Score (www.netpromoter.com). Some aspects of the supplied service such as a high level of system availability should be taken as read. Our Technical Services Team will endeavour to provide you with that 'extra mile' of service that, whilst not contractual, is what we believe you deserve.

The following sections describe our service level commitments and should be read in conjunction with our published Terms and Conditions (see www.clouddirect.net/legal for the latest version). This SLA may also be varied from time to time.

If you have any comments or observations about our performance and the service we provide you should contact our Head of Operations, Mark Gold on 0800 0789 438 or email mark.gold@clouddirect.net.

6 Data Location and Service Security

With EMS, you get peace of mind knowing that your data and services are highly available and secure. EMS offers the following benefits:

6.1 Datacentre Location

- Although Microsoft have a global network of datacentres, for customers within the EU the primary and secondary data centres are in Ireland and the Netherlands. Customers should assume that their customer data may be processed in either the primary or the secondary datacentre.
- Microsoft services are fully compliant with the EU Data Protection Directive and therefore, the UK Data Protection Act.
- All datacentres are ISO 27001.

6.2 Datacentre features and redundancy

- Content is replicated from the primary datacentre to the secondary datacentre so replication is constant.
- Your data is stored in a redundant environment with robust backup, restoration, and failover capabilities to enable availability to your services. You will not be notified when failover occurs as typically failover does not result in service interruption.
- Microsoft offer multiple levels of physical redundancy at the disk, NIC, power supply, and server levels.
- Data centres located in seismically safe zones.
- Automated monitoring and recovery system; 24/7 Microsoft engineering teams are standing by to fix anything that the automated systems are not able to handle.
- For more information, please see: https://www.microsoft.com/en-gb/server-cloud/cloud-os/global-datacenters.aspx.

6.3 Datacentre Security

- Microsoft offer many physical and technology-based security features within their datacentres including 24/7 on site security, CCTV and encrypted servers.
- For more information, please see: https://www.microsoft.com/en-gb/server-cloud/cloud-os/global-datacenters.aspx.

6.4 Data transit and storage

- Like their datacentres, Microsoft ensure all their cloud services offer the highest levels of security available and have numerous security accreditations for their services including ISO 27001, ISO27018, SOC1 and SOC2. They also comply with country specific standards like the EU Data Protection Directive and G-Cloud.
- For more information about security and compliance of EMS services please visit the Microsoft Trust Centre here: https://www.microsoft.com/en-us/TrustCenter.
    - From this main webpage, you can visit sections for Microsoft Intune and Azure (for Active Directory and Rights Management).

6.5 Service updates and patching:

- The EMS service offers the latest versions of the associated technology at all times. These updates will be in three forms:
    - Break/fix updates and security patches are pushed out at the backend and implemented straight on the datacentre servers. There is no customer action required.
    - Major feature updates for components of EMS that are implemented at the datacentre like Active Directory and Rights Management are pushed out at the backend and implemented straight on the datacentre servers. There is no customer action required.
    - Major feature updates for components of EMS that are client facing will prompt users for an update of an agent or software. We advise you to action these update requests as soon as possible.

7 Scope of Supply

Please refer to your Sales Agreement for details of your specific purchased services. All our EMS products come with 24/7 support via telephone, PROVIDE™ and email as detailed below.

To get your service running smoothly you may require bespoke configuration and setup and depending on your desired deployment model, connection to existing on-premise equipment. These services are not included as standard. If you require these additional service options, please contact the Cloud Direct Sales team on 0800 0789 437 to discuss your requirements in detail.

Identity and access management is all about controlling; who has access and what they have access to. Azure Active Directory is Microsoft's comprehensive Identity as a Service (IdaaS) solution, enabling Identity and Access Management capabilities for Cloud and SaaS apps. It has two main features around this; authentication to confirm that an individual/group are who they say they are and authorisation to allow the individual/group appropriate access to what they are trying to access. There are three types of deployment options:

- Cloud only is for those who only want to work through the likes of Office 365 and where there is no on-premise directories or where this service wants to work in isolation from those on-premise services. A user is created and managed in Office 365 and stored in Azure Active Directory with the password also being verified there.

- Synchronised offers the ability to sync with an on-premise directory so the user identity is managed in an on-premise server and the accounts and password hashes are synchronised to Azure Active Directory. The user enters the same password on-premise as they do in the cloud, and this is verified by Azure Active Directory.
- Federated is like synchronised identity, but the user password is verified by the on-premise identity provider. This means that the password hash does not need to be synced to Azure Active Directory. This model uses Active Directory Federated Services or a third-party identity provider. This model is the most complex and requires more network and server infrastructure.

There are three licences available Azure Active Directory Basic, Premium P1 and Premium P2; any of the above deployment options can be achieved on these licences. Azure Active Directory offers some extended functionality over the basic version including, an unlimited number of applications, advanced security reports, self-service management and usage reports.

With Microsoft Intune, organisations can provide access to apps whilst preventing data leaks without requiring employees to enrol in full Mobile Device Management (MDM) through offering Mobile Application Management (MAM). MDM controls the whole device and just about everything on it, whereas, MAM is more granular, and restricts control solely to applications and corporate resources. In this case, when a business wipes a device (for example, when reported lost or stolen) only corporate apps and data will be wiped, leaving personal apps and data intact. The IT admin can configure device management policies in the Intune portal such as having a password or PIN, encryption turned on, regularly updated and jailbreak detection. By using Azure Active Directory with Intune, companies can also configure and conditional access policies such as devices must be managed by Intune, only allowing the storage of business data within business applications (for instance, business email attachments can only be saved in OneDrive) and have encryption turned on to access business systems. Under the Microsoft Intune licence, you have two deployment options; standalone, where you manage the service through the cloud Intune admin console or hybrid, where you can integrate with System Centre Configuration Manager.

Information Protection is all about making sure information is shared safely and data isn’t compromised while recognising that employee mobility and productivity is not possible through traditional security tools such as firewalls, control lists and NTFS permissions. Azure Information Protection encrypts individual files and manages access to those files based on rights related to an individual’s Active Directory credentials. Restrictions and policies can be added to all Microsoft Office documents including Email with Outlook such as encryption with password, restrict access, restrict editing and restrict the ability to Forward, Reply, or Reply all within email. Azure Information Protection comes with many pre-set templates but new custom templates can also be configured. Unlike more traditional information protection, you maintain control of data after it has left the organisation, as the restrictions are associated to the data itself. With Azure Information Protection, you can set document expiration dates, document tracking and reporting to see who has accessed, or been denied access to the document (through Azure Active Directory credentials) and revoke access to a document after it has left the organisation, regardless of where it is stored.

Microsoft Cloud App Security helps organisations understand their shadow-IT problem. Shadow-IT are applications or programs used within a business that haven’t been sanctioned for use. An example of this is employees using their personal Dropbox account so they can continue working on something from home. Cloud App Security enable you to do a full audit within your organisation to understand what is being used and the potential risk that exposure brings without the need to put agents on every device. Granular data-control security policies can be built easily; whether you use out-of-the-box policies or build and customise your own. Every insight is actionable, allowing you to remediate with a single click or implement data sharing and granular usage policies. Complete governance of data in the cloud, such as files that are stored in cloud drives, as attachments, or within cloud application. Use pre-defined fields or extend existing enterprise Data Loss Protection (DLP) policies to your SaaS applications. Dynamic reports can run on DLP violations, sensitive file sharing, and data sharing violations. Data control in the cloud helps you comply with regulatory mandates such as PCI, HIPPA, and more. User behavioural analytics helps you to stay ahead of attackers. You can identify anomalies in your cloud usage that may be indicative of a data breach. Cloud App Security advanced machine learning heuristics learn how each user interacts with each SaaS application and, through behavioural analysis, assesses the risks in each transaction. This includes simultaneous logins from two countries, the sudden download of terabytes of data, or multiple failed login attempts that may signify a brute force attack.

The four above components can be purchased as part of a bundled licence or as individual components.

8 Scope of Support

Cloud Direct are pleased to provide support for genuine technical issues and troubleshooting. This is where features of the product or service, or, the product or service itself can be demonstrated as not operating correctly or users are unable to access the services through approved platforms. Furthermore, Cloud Direct will assist with a range of administrative functions and activities that typically require an experienced administrative user.
As examples, we have provided some typical supported and unsupported scenarios.

8.1 Examples of Supported Scenarios

Examples of typically supported scenarios are:

- Password resets.
- Errors or user issues relating to Active Directory.[1]
- Errors or user issues relating to Azure Rights Management.[1]
- Errors relating to Microsoft Intune.[1]
- Single reinstallation when replacing hardware relating to Microsoft Intune.
- Investigating and addressing an instance of a service outage.

8.2 Examples of Unsupported Scenarios

We will always endeavour to go the extra mile for our customers where we have the resources to do so. Our support philosophy is to resolve issues with a feature or function that is not operating correctly within its definition, as opposed to providing user training and support for working features. There is a wide range of support materials on the Microsoft Knowledgebase for EMS and its components which can help offer assistance for deployment. See https://support.microsoft.com/en-gb.

Examples of typically unsupported scenarios are:

- General desktop application or operating system support.
- Break/fix or issues relating to an on-premise Active Directory server.[2]
- Assistance in a full deployment of EMS or its components.
- Support for any connectivity or networking problems (e.g. internet / router / firewall access) where those services are not purchased through Cloud Direct.

[1] Excluding issues associated with Internet access, other network problems or device issues where those services have not been provided by Cloud Direct.

[2] Unless your Active Directory Server is supported by Cloud Direct.

9 Support Case Prioritisation

As outlined in the Cloud Direct Support Agreement, issues reported to us by customers are categorised into one of four levels: Standard, Moderate, High and Critical. Although we will determine the final priority designation of your reported issue please see the below examples as indicators of how we will categorise your EMS issue if one should arise:

Standard - An issue that does not interfere with your business such as a request for a repeat invoice or support on how to do something relating to your EMS service.

Moderate - An issue that does not interfere with the majority of features from your EMS service such as configuration/setup issue or an interruption to service for a single user.

High - An issue that results in an interruption to the service that effects multiple users.

Critical[1] - An issue where all users are unable to make use of EMS services, such as an inability to use Active Directory services – you must make us aware of any such critical situation by phone to avoid delays.

10 Our Responsibilities

To provide you with an enterprise-class EMS service and the highest level of customer service, as described in this SLA and your contract with us, we commit to:

- Contact you once the service is installed, setup and migrated (if we are performing the setup and migration), if necessary, we will contact you to check you are happy with the service and all is working well. We refer to this process as 'On-Boarding'.
- Provide free of charge updates to the service, at regular intervals and inform you of specific requirements for upgrades.
- Maintain your data in a secure manner and will not provide access to your data without appropriate security checks being completed. If we are not convinced of a caller's right to access your account, we will seek further clarification from a senior representative from your company.
- Help you with the re-installation of purchased products (eg. PC and Phone) into your company systems if you suffer a device failure but our responsibility ends with actions directly pertaining to the products purchased from us and the scope of supply and support.
- Contact you at least once a year to seek your customer Net Promoter (satisfaction) Score and any feedback you may have. We will act on your feedback.
- Make your departure, should you choose to leave Cloud Direct, as smooth as possible and continue to support you until the end of the contracted term and assist where possible with account closure.

11 Your Responsibilities

To ensure we can effectively deliver your service we require your cooperation in the following areas:

[1] Excluding issues associated with Internet access, other network problems or device issues where those services have not been provided by Cloud Direct.

- To provide a stable computer environment on which the service is installed and which meets the system operating requirements including sufficient internet bandwidth and latency performance. Before installation (and any upgrades) you will refer to any Installation / Release Notes and associated service documentation provided by Microsoft or Cloud Direct.
- Service performance can be directly influenced by your internet bandwidth and latency. Service performance issues are normally the result of internet service interruptions and you should check this before contacting us.
- Before signing our Service Agreement, you will check your equipment and operating system environment against the service minimum requirements.
- If making use of the Active Directory function you must ensure you have checked the pre-requisites for the particular type of deployment you would like.
- Dependent upon your connection type you may be charged by your ISP (including additional mobile charges) based on your usage of this Service. You are responsible for all associated data transmission / receipt costs. Care is advised when using roaming 3G/4G mobile services.
- To ensure your use of the Service does not affect the operation of the overall service platform. In the event that your usage is adversely affecting the overall platform, it may be suspended or terminated without liability to Cloud Direct upon prior written notice (or immediately without notice in the event of a technical emergency).
- You will notify us of your desire to cancel the service, giving the appropriate notice, as described in our Terms and Conditions.

Please refer to our full Terms and Conditions at http://www.clouddirect.net/legal for a complete breakdown of both your and our contractual responsibilities.

12 Service Availability and Financial Claims

We commit to our customers that the EMS services will have an uptime of 99.9% and above (excluding planned maintenance). This is worked out over a month. To calculate the uptime of a service, we use the following formula:

$$\frac{\text{Total number of minutes in a month – Minutes Downtime}}{\text{Total number of minutes in a month}} \quad \text{x 100}$$

Service Downtime is measured from the time a case is raised with us by you until the EMS service is restored.

Any rebate will be prorated based on number of affected users.

This SLA does not apply to any performance or availability issues in conjunction with:

- Factors outside of our control.
- As a result of your, or third party services, hardware or software.
- Your use of the service after you were advised by us to modify your use and did not do so.
- Being on a trial of the service.
- An unauthorised action or inaction by you or your employees, agents, contractors, vendors or anyone gaining access to the EMS network through your passwords or equipment.
- Your failure to adhere to any required configurations, supported platforms and outlined policies for acceptable use. This includes any changes made during the service such as changing your operating system.

- Reserved licences which have not been paid for at the time of the downtime.

If the uptime falls below 99.9% for any given month, you may be eligible for the following rebate:

Online service availability in a given month (excluding planned maintenance)	**Rebate (% of per affected User monthly recurring charge)**
Less than 99.9% and greater than or equal to 99.0%	10%
Less than 99.0% and greater than or equal to 95.0%	25%
Less than 95.0%	50%

If you wish to make a claim for non-conformance against this SLA you should do so in writing to support@clouddirect.net citing your reasons in full, the duration of the downtime, the number of users affected and relevant Cloud Direct Support Case numbers within 10 calendar days of the online service interruption.

Our Directors will review any incident raised by evaluating all the information reasonably available to them and make a good faith judgment on whether a Rebate is owed. You must be in compliance with our contractual agreement and this SLA in order to be eligible for a Rebate. If we determine that a Rebate is owed to you, we will apply the Rebate to your next invoice; you may not offset the Rebate yourself from any payments owed. If you receive an SLA Rebate this is your sole and exclusive remedy for any performance or availability issues for any EMS service covered by this SLA.