This Service Schedule for **Hosted Messaging Services v8.0. 0** (the "Service") replaces all previously signed / incorporated version(s) of the Service Schedule(s) Hosted Messaging Services (if any) and forms part of the Master Services Agreement and Master Services Schedule. Its provisions are an integral part of the Master Services Agreement. Words and expressions defined in the General Conditions and Master Services Schedule shall (unless otherwise defined in this Services Schedule) bear the same meanings where used in this Service Schedule. In this Service Schedule the following words and phrases shall have the following meanings unless the context otherwise requires:

1. Interpretation

1.1. "**Cloud Workspace Suite**" means a collection of Service editions, options and showcase features which have been bundled together and provide (i) a convenient way to order and (ii) are provided at a lower fee than when ordered separately.

1.2. "**License Mobility**" means the ability for a Customer to deploy its current Exchange licenses in SP's datacentre via Microsoft's License Mobility program. Microsoft's License Mobility program is available to its Volume Licensing customers (Server and CAL licenses under Open, Select or Enterprise Agreements). SP can only accept Exchange licenses when they're covered by active Microsoft Software Assurance ('SA') contracts.

2. Service Overview

2.1. The Service provides access to one or more of the following delivered stand-alone or as part of the Cloud Workspace Suite:

2.1.1. Microsoft Exchange™ email technology via a hosted cloud-based service.

2.1.2. DiscoveryVault™ email archiving using MessageSolution™ technology via a hosted cloud-based service.

2.1.3. SyncVault™ collaboration using Ctera™ technology via hosted cloud-based service.

2.1.4. Microsoft Project™ technology via a hosted cloud-based service.

2.1.5. Microsoft SharePoint™ technology via a hosted cloud-based service.

2.1.6. Microsoft Skype™ technology via a hosted cloud-based service.

2.1.7. Microsoft Office™ technology via a hosted cloud-based service.

2.1.8. Showcase Functionality via a hosted cloud-based service.

3. Standard Components

3.1. Customers may select from various mailbox types in one of the following: (1) **Hosted Exchange Small Business Edition** – up to 100 (one hundred) mailboxes per Customer hosted and managed by SP in a single South African datacentre, (2) **Hosted Exchange Medium and Enterprise Edition** – mailboxes hosted and managed by SP and replicated between dual South African datacentres with no restriction on the number of mailboxes per company, and (3) **Microsoft Exchange Online** – mailboxes hosted and managed by Microsoft from international datacentres.

3.2. **Email filtering**

3.2.1. All mailboxes include inbound and outbound email filtering.

3.2.1.1. Hosted Exchange Small Business Edition as well as the Medium and Enterprise Edition use technology from SpamExperts™.

3.2.2. Microsoft Exchange Online technology from Microsoft Exchange Online Protection Email Filtering™.

3.3. **DiscoveryVault email archiving**

3.3.1. DiscoveryVault email archiving is a standard component of Hosted Exchange Medium and Enterprise Edition – Professional mailboxes, and may optionally be added to any other mailbox for an additional fee.

3.4. **Support**

3.4.1. Support is not included as a standard component and is provided on either SLA (Service Level Agreement or per hour)

Initial

4. Hosted Exchange Small Business Edition

4.1. **Hosted Exchange Small Business Edition – Lite Mailbox**

4.1.1. Outlook Web Access (“OWA”).

4.1.2. Internet Message Access Protocol (“IMAP”).

4.1.3. Simple Mail Transfer Protocol (“SMTP”).

4.1.4. Post Office Protocol (“POP”).

4.1.5. Support for a single, second level domain for a single user.

4.1.6. Tasks and Rules.

4.1.7. Personal Folders (not shared with other users).

4.1.8. Personal Calendar (not shared with other users).

4.1.9. Personal Contacts (not shared with other users).

4.1.10. Support for Organisation Wide Global Address List (up to a maximum of 100 (one hundred) users).

4.1.11. Incoming and Outgoing Email Filtering.

4.1.12. Management of the Service including Fault Reporting.

4.1.13. Mailbox hosted and managed by SP in South African data centre(s).

4.1.14. Deleted Item Cache (24 Hours).

4.2. **Hosted Exchange Small Business Edition – Standard Mailbox**

Includes the features of Hosted Exchange Small Business Lite Mailbox plus:

4.2.1. Deleted Item Cache (7 Days).

4.2.2. ActiveSync Mobile Notification of events in the server software via mobile devices.

4.2.3. ActiveSync Mobile Synchronization over wireless networks with the server software inbox, calendar, address book and tasks.

4.2.4. Shared Folders (up to a maximum of 100 (one hundred) users).

4.2.5. Shared Calendars (up to a maximum of 100 (one hundred) users).

4.2.6. Shared Contacts (up to a maximum of 100 (one hundred) users).

4.2.7. Shared Tasks and rules (up to a maximum of 100 (one hundred) users).

4.2.8. Group scheduling, including viewing free/busy times of others (up to a maximum of 100 (one hundred) users)

MAPI via RPC/HTTPS.

5. Hosted Exchange Enterprise Edition

5.1. **Hosted Exchange Medium and Enterprise Edition – Super Lite Mailbox**

5.1.1. Outlook Web Access (“OWA”).

5.1.2. Internet Message Access Protocol (“IMAP”).

5.1.3. Simple Mail Transfer Protocol (“SMTP”).

5.1.4. Post Office Protocol (“POP”).

5.1.5. Support for a single, second level domain for a single user.

5.1.6. Tasks and Rules.

5.1.7. Personal Folders (not shared with other users).

5.1.8. Personal Calendar (not shared with other users).

5.1.9. Personal Contacts (not shared with other users).

5.1.10. Support for Organisation Wide Global Address List.

5.1.11. Incoming and Outgoing Email Filtering

5.1.12. Management of the Service including Fault Reporting.

5.1.13. Mailbox hosted and managed by SP in South African data centre(s).

Initial

5.2. **Hosted Exchange Medium and Enterprise Edition – Lite Mailbox**

Includes the features of Hosted Exchange Medium and Enterprise - Super Lite Mailbox plus:

5.2.1. Deleted Item Cache (24 Hours).

5.2.2. Lagged database availability group replication to second data centre.

5.3. **Hosted Exchange Medium and Enterprise Edition – Standard Mailbox**

Includes the features of Hosted Exchange Medium and Enterprise – Lite Mailbox plus:

5.3.1. Deleted Item Cache (7 Days).

5.3.2. ActiveSync Mobile Notification of events in the server software via mobile devices.

5.3.3. ActiveSync Mobile Synchronization over wireless networks with the server software inbox, calendar, address book and tasks.

5.3.4. Shared Calendars.

5.3.5. Shared Contacts.

5.3.6. Group scheduling, including viewing free/busy times of others.

5.3.7. MAPI via RPC/HTTPS.

5.4. **Hosted Exchange Medium and Enterprise Edition – Professional Mailbox**

Includes the features of Hosted Exchange Medium and Enterprise Standard Mailbox plus:

5.4.1. Deleted Item Cache (14 Days).

5.4.2. DiscoveryVault™ email archiving.

5.4.2.1. Included DiscoveryVault™ email archiving is not enabled by default. Professional Mailboxes may have archiving enabled at no additional charge provided that Customer has followed SP's standard ordering process to enable archiving.

6. Microsoft Exchange Online

6.1. **Microsoft Exchange Online 1**

6.1.1. Microsoft Exchange Online 1 is a Microsoft Online Service which includes the following features:

6.1.2. Outlook Web Access ("OWA").

6.1.3. Internet Message Access Protocol ("IMAP").

6.1.4. Simple Mail Transfer Protocol ("SMTP").

6.1.5. Post Office Protocol ("POP").

6.1.6. Support for a single, second level domain for a single user.

6.1.7. Tasks and Rules.

6.1.8. Deleted Item Cache (14 Days).

6.1.9. ActiveSync Mobile Notification of events in the server software via mobile devices.

6.1.10. ActiveSync Mobile Synchronization over wireless networks with the server software inbox, calendar, address book and tasks.

6.1.11. Shared Calendars.

6.1.12. Shared Contacts.

6.1.13. Group scheduling, including viewing free/busy times of others.

6.1.14. MAPI via RPC/HTTPS

6.1.15. Support for Organisation Wide Global Address List.

6.1.16. Microsoft Exchange Online Protection Email Filtering.

6.1.16.1. Microsoft Exchange Online is hosted and managed by Microsoft in international public cloud data centre(s)

7. Incoming and Outgoing Email Filtering

A number of proprietary self-learning smart technologies that have been deployed to eliminate spam, virus, phishing and malware attacks.

7.1. **Bounce Spam Protection ('BSP')**

Initial

7.1.1. "Bounce spam" can be an annoying problem. The email SMTP protocol is a very simple protocol that was defined in 1982. Spam was not yet a problem and to keep things as simple as possible, no security measures were implemented in the protocol itself. The result of this is that there is no verification whatsoever that the "From:" address in an email message actually belongs to the sender. To try and avoid spam filters, spammers will typically use random email addresses as fake senders. This way they can avoid any simple spam filter that blacklists based on the sender email address. It is important however that the email address they use as a sender does exist, since spam filters can apply a "sender verification check" to ensure that the sending address itself exists.

7.1.1.1. BSP supports SPF, DKIM and BATV signing to identify and block "bounce-spam".

7.2. **SMTP and DATA level filtering**

7.2.1. These filtering methods have been specifically designed to avoid false positives. Many different checks are performed to avoid making mistakes based on only a single classifier. Two levels of filtering can be distinguished. Filtering at the "SMTP level" and filtering at the "DATA level". Using a combination of many different advanced filters and the compliance with the RFCs on how to handle connections, the technologies ensure email can never disappear. The sender is always informed by their sending server that the message was rejected - in addition, messages blocked at the "DATA level" are available in the quarantine system.

7.2.2. SMTP Level:

7.2.2.1. Wherever possible, incoming email connections are not blocked until after the "rcpt to:" SMTP command. This ensures connections are properly logged as belonging to a recipient domain. Before the "DATA level" is reached, the connection is checked to see if it complies with RFC standards, is not listed on internal and/or external blacklists, and several other parameters. If the connection appears to be coming from an unknown source that does not yet have a verified reputation in our systems, it may be temporarily rejected with a 4xx code. In that case the sending server will queue the email, and automatically retry delivery. After 10 minutes the connection will be accepted by the cluster (on any of the filtering nodes), and the internal whitelists will be automatically adjusted to avoid causing similar email delivery delays in future. This concept is also known as greylisting, however the implementation is more sophisticated than traditional greylisting systems as all nodes are fully synchronized, and only connections from servers that are unknown in our network are temporarily delayed. Therefore email delays because of greylisting on active filtering clusters are quite uncommon. If the connection appears to originate from a spamming source, often the connection is also temporarily rejected with a 4xx code. This way even if the server would have been wrongly listed (e.g. on an external blacklist) as a spamming source, or if the spamming problem has been resolved on the sending server, the email still does not get lost and will be delivered to the final recipient. Only if the connection is from a known, spam-only source, or if the behaviour is in direct conflict with the RFC standards, will a connection be permanently rejected with a 5xx error code. If an email is rejected for a legitimate sender, the sender will always receive a bounce notification from their sending server. This issue only occurs when there are serious problems with the sending server that should be resolved at the sender's side.

7.2.3. Data Level:

7.2.3.1. After the "DATA level" is reached the system will scan the email content of the message based on a combination of advanced statistical filtering technologies, spam fingerprint databases, viruses, phishing, and spyware. Email detected as spam is either temporarily rejected (4xx error code) or permanently rejected (5xx error code) depending on the total score. Email which is permanently rejected at this level as spam is quarantined and available for release (except for viruses). In the event that a legitimate email is permanently blocked, the sending server will also always inform the sender that the email was not delivered.

7.3. **Email Encryption**

7.3.1. Incoming and Outgoing Email Filtering fully supports incoming connections protected using TLS. Deliveries are always made over TLS when supported by the destination mail server. This ensures that email is securely transmitted.

7.4. **Spam Quarantine**

7.4.1. The quarantine system can be accessed using the web interface. Note that the use of the quarantine is optional, and not a necessity. Emails placed in quarantine have been rejected with a 5xx SMTP rejection code at SMTP level, so legitimate sending servers will have informed the sender about the rejection. Spam messages that were temporarily rejected at SMTP level are not listed in the quarantine, and will be automatically retried by legitimate sending servers. By default, quarantined spam is stored for 14 (fourteen) days.

Initial

7.4.1.1. From the web interface users can either delete or release messages blocked as spam. In case an email has been incorrectly blocked, clicking release will result in delivery of the false positive to the original recipient. It will also trigger a report about an incorrect classification to our systems to further improve the filtering.

7.5. **Virus Scanning**

7.6. Viruses often spread via email, therefore it is important to virus-scan emails before they arrive on the mail-client of a user. Inbound and Outbound filtering actively blocks both spam and viruses.

7.6.1. Since viruses are generally spread as spam emails, the majority of email viruses are already blocked before they are scanned with our antivirus engine, because of our antispam technologies. Our virus definition database is updated every 30 (thirty) minutes via ClamAV as well as additional datasets to ensure real-time, optimal protection against the latest virus outbreaks. Our internal reputation systems also contribute to virus scanning and ensure optimal protection against not only spam, but also malware, phishing, and viruses.

7.7. **Email Queuing**

7.7.1. Organisations no longer risk email delays, interception, damage, or loss. The services are designed to instantaneously begin email queuing when a loss in connectivity is detected between the Service and one or more of a business's message transfer agent (MTA) servers. Once the connection with the email server(s) is restored, current and spooled email is delivered to the email server.

7.7.2. Messages queued for known valid recipients because of temporary problems with the destination route (for example network problems) are automatically retried for delivery at the following approximate intervals:

7.7.2.1. During the first 2 hours, delivery is retried at a fixed interval of 15 minutes.

7.7.2.2. During the next 14 hours, delivery is retried at a variable interval, starting at 15 minutes and multiplying by 1.5 with each attempt (e.g. after 15 minutes, then 22.5 minutes, then 34 minutes, and so on).

7.7.2.3. From 16 hours since the initial failure, until 4 days have passed, delivery is retried at a fixed interval of every 6 hours.

7.7.2.4. After 4 days we generate a bounce to the sender. If the bounce cannot be delivered immediately, it will be frozen. After this time, delivery of the message will have permanently failed.

7.7.3. When a message is frozen, (when a message can neither be delivered to its recipients nor returned to its sender) no more automatic delivery attempts are made. SP can "thaw" (force retry) such messages when the problem has been corrected.

7.7.4. Message queuing caches valid recipients for up to 4 days. When a cached entry has expired, mail will no longer queue for these recipients and will instead be temporarily rejected so that it can be queued on the sending server. The sending server in such case will automatically retry delivery.

7.8. **Email Continuity**

7.8.1. Email queuing and outbound filtering can be used in combination to provide email continuity whenever the email server is unavailable.

7.8.2. Access to inbound email during a mail server outage:

7.8.2.1. Queued email can be read via the Email Filtering web interface or via any IMAP client which supports write-only folder access. Note: Some versions of Microsoft Outlook do not support write-only folders via IMAP.

7.8.2.2. When the email server is available, queued mail will be automatically delivered to the email server.

7.9. Outbound email capability during a mail server outage:

7.9.1. Users can be configured with permission to send email via the outbound filtering servers using any authenticated SMTP client.

7.9.1.1. Note: Email sent via Outbound Email Filtering is not journaled by default even if email archiving is enabled. This can be enabled at an additional charge.

8. DiscoveryVault™ Email Archiving

8.1. DiscoveryVault™ email Archiving enables automatic and secure archiving of internal, inbound and outbound email messages to a centralized, secure location. With the DiscoveryVault Email Archiving, businesses will benefit from the following features:

8.2. **Managed Storage**

8.2.1. DiscoveryVault™ email Archiving is available with no pre-set storage limits, and requires no additional on-premises software or hardware integration.

8.2.2. Support for 1 year or multi-year storage periods.

8.3. **End-user self-service:**

8.3.1. Enables users to review their own archived messages without requiring assistance from IT staff.

8.4. **Advanced Search:**

8.4.1. Provides authorized staff members with quick, accurate search capabilities for retrieval of archived messages, based on search criteria that include message headers, subject, body content, attachments and common fields such as Sender, Recipient and Date. Authorized staff can choose to initiate a search via simple, advanced, or Archive ID search interfaces.

8.5. **Definable retention:**

8.6. Allows businesses to dictate how long messages will be retained in the archive based on legal and regulatory requirements. The Service provides options for 1 year or multi-years of retention, as well as Historical Data Storage.

8.7. **Secure data transport and storage:**

8.7.1. Ensures privacy via enforceable transport encryption and 256-bit storage encryption.

8.8. **Transactional data acquisition:**

8.8.1. Provides near real-time archiving and rapid message retrieval, as opposed to delayed point-in-time snapshot back-ups.

8.9. **Parallel Search Technology:**

8.9.1. Enables efficient multi-tasking through the intuitive web interface, which is designed to improve workflow and results.

8.9.2. Administrators can view search parameters and results conveniently on one screen.

8.10. **Saved searches:**

8.10.1. Reduces overhead by retaining search parameters for later use.

8.11. **Policy-Driven Archiving:**

8.11.1. Effective policies are the backbone of compliance efforts.

8.11.2. DiscoveryVault™ Email Archive allows for the creation of an unlimited amount of archiving policies by specifying email retention periods, filtration rules, contents and/or attachments, and other parameters.

8.11.3. Policies can be applied to entire geographic locations, departments, or teams, all the way down to the individual user level.

8.12. **Historical Archive Import**

8.12.1. Allows businesses to conveniently store previous email data securely off site.

8.12.2. All historical data is indexed to enable rapid search and retrieval.

8.12.3. Available as a paid for service for DiscoveryVault Email Archiving.

8.13. **Archive Export**

8.13.1. Ability to export archived email from the Service.

8.13.2. Available as a paid for service for DiscoveryVault Email Archiving.

9. Optional Services

9.1. These optional services have been designed to work with Hosted Messaging and may be included for an additional fee.

9.2. Support is not included with optional services and is provided via one of the following for an additional fee: (1) **Support Services Subscription**, (2) **Managed Care Subscription**, or (3) **Cloud Workspace Suite Subscription**. Customers who have not subscribed for Managed Care or Cloud Workspace Suite who wish to log service requests directly with SP are required to conclude a separate Support Services Schedule and associated Support Services Subscription

9.2.1. **Hosted Blackberry Enterprise Services**

9.2.1.1. Hosted Blackberry Enterprise Services allows users to access their mailboxes from a Blackberry Mobile device.

Initial

9.3. **SyncVault File Collaboration Services**

9.3.1. ***Sync/ Share:***

9.3.1.1. Web-based and mobile access to files and folders stored on the SyncVault Portal.

9.3.1.2. Drive mapping and bi-directional sync agents for Windows, Linux and Mac OS.

9.3.1.3. Mobile sync on iOS, Android mobile devices with remote wipe support.

9.3.1.4. Multi-folder support enables users to sync pre-existing and multiple file folders.

9.3.1.5. Support for password protected cloud drives and data encryption.

9.3.1.6. Email-based invitations to files and folders with 2-factor authentication.

9.3.1.7. Option for remote device wipe and/or lock.

9.3.2. ***Project Team Collaboration****:*

9.3.2.1. Define read/write privileges and time limited access.

9.3.2.2. Bi-Directional synchronisation of folders on user's PCs with each other.

9.3.2.3. One-way synchronisation for file syndication.

9.3.2.4. Conflict resolution in case of divergent file versions.

9.3.2.5. Ad-hoc sharing using time0limited invitation URLs.

9.3.2.6. Rose-based privileges for allowing users to create shared project folders.

9.3.3. ***Security:***

9.3.3.1. Source-based, 256bit AES encryption of data in flight and at rest with customer defined encryption keys.

9.3.3.2. Source-based deduplication and compression for optimized data delivery and WAN utilization.

9.3.3.3. Dynamic DNS for remote access to files.

9.3.3.4. Versioning support to recover previous file versions.

9.3.4. ***Integration:*** *(Requires ID Sync)*

9.3.4.1. Support for both Active Directory (AD) and LDAP authentication.

9.3.4.2. User authentication based on customer's AD without leaving the intranet.

9.3.4.3. Support for corporate AD "forests" in and cross-domain trusts SyncVault Portal.

9.3.4.4. Ability to define virtual sub-portals that map to specific AD OU's.

9.3.4.5. Military-grade data encryption at rest and in transit; with customer / tenant defined encryption keys.

9.3.5. ***Administration:***

9.3.5.1. Central policy-based management of agents and appliances, firmware and plans are centrally distributed.

9.3.5.2. Template-based management that allows for simple provisioning and adjustment to user and appliance configuration including storage quotas and software updates.

9.3.5.3. Real-time monitoring and alerting on connectivity etc.

9.3.5.4. Logging of system events (logins, failed logins, backups, errors) and reporting.

9.3.5.5. Multi-tier user management, with role-based delegation and control over tenant user & administrator privileges.

9.3.5.6. Highly scalable solution designed for centralized, policy-based management of millions of endpoints, 1000s of appliances and 1000s of tenants.

9.3.6. ***Cloud Storage Gateway:*** *(Requires one or more CXXX Gateway(s))*

9.3.6.1. NAS Server with Quota Management and Access Control lists.

9.3.6.2. Sync directories across gateways and mobile devices.

9.3.6.3. Thin local snapshots.

9.3.6.4. Configurable cloud-based snapshot retention.

9.3.6.5. Automated replication to the SyncVault portal in the cloud.

9.3.6.6. Cloud seeding for initial file and backup ingest.

9.3.6.7. Support for NFS, CIFS, AFP, WebDAV and Rsync protocols.

9.4. **Microsoft Project Online**

Initial

9.4.1. Microsoft Project Online is a flexible online solution for project portfolio management (PPM) and everyday work. Delivered as a Microsoft Online Service, Project Online enables organizations to get started quickly with powerful project management capabilities to plan, prioritize, and manage projects and project portfolio investments. Project Online can be used by administrators, portfolio managers, portfolio viewers, project managers, resource managers, team leads, and team members.

9.4.2. Project Online and Project Lite are both Project Portfolio Management ('PPM') solutions. Project Online is not a web-based version of Microsoft Project Professional 2013, a project management solution. Project Online is a completely separate service that offers full portfolio and project management capabilities on the web.

9.4.3. Project management features are supported by using the Project desktop application, purchased either as a single download license for Project Professional 2013 or as a monthly subscription license to Project Pro for Office 365.

9.4.4. The following PPM options that are available:

9.4.5. ***Project Online:***

9.4.5.1. A monthly subscription service that is offered as a standalone service or as an add-on.

9.4.5.2. Includes: Reporting & business intelligence.

9.4.5.3. Includes: Demand management.

9.4.5.4. Includes: Portfolio selection and optimisation.

9.4.5.5. Includes: All the features of Project Lite (below).

9.4.6. ***Project Lite:***

9.4.6.1. A monthly subscription service that is offered as an add-on for customers who have Project Online.

9.4.6.2. Organizations must have Project Online in order to use Project Lite. Project Lite is suitable for project team members to manage their tasks and timesheets, and collaborate on projects. Depending on their role, users are assigned either the Project Online license or the Project Lite license (but not both).

9.4.6.3. Includes: Task management.

9.4.6.4. Includes: Document sharing.

9.4.6.5. Includes: Support for Skype for business presence.

9.4.6.6. Includes: Timesheet submission.

9.4.6.7. Includes: SharePoint task sync.

9.5. **Microsoft Project Pro for Office 365**

9.6. Microsoft Project Pro for Office 365 delivers the latest version of Project Professional as a desktop subscription through Office 365, and software is automatically kept up to date with options for customizable policies.

9.7. Project Pro for Office 365 provides more options for project management through its integration with SharePoint Online. Teams can create, assign, and update tasks, add a timeline to their SharePoint site. Task details can be viewed in Project Pro for Office 365 for additional project management rigor and reporting. Team tasks can also be imported into Microsoft Project Portfolio Management (PPM) solutions, such as Project Online or Project Lite, for more advanced scenarios.

9.8. **Microsoft SharePoint Online 1**

9.8.1. Microsoft SharePoint Online 1 is a Microsoft Online Service which includes the following features:

9.8.2. ***Application features:***

9.8.2.1. Application Catalogue and marketplace.

9.8.3. ***Collaboration features:***

9.8.3.1. Team Sites.

9.8.3.2. Work management.

9.8.3.3. External sharing.

9.8.4. ***Search features:***

9.8.4.1. Basic search.

9.8.5. Standard search.

9.8.6. ***Content Management features:***

Initial

9.8.6.1. Content management.

9.8.6.2. Records management.

9.8.7. ***Business Solutions features:***

9.8.7.1. Access services.

9.8.7.2. SharePoint workflow.

9.8.8. SharePoint Online is hosted and managed by Microsoft in international public cloud data centre(s).

9.9. **Microsoft SharePoint Online 2**

9.9.1.1. Microsoft SharePoint Online 2 is a Microsoft Online Service which includes all the features of Microsoft SharePoint Online 1 plus:

9.9.2. ***Search features*:**

9.9.2.1. Enterprise search.

9.9.3. ***Content management features:***

9.9.3.1. E-discovery, ACM and compliance.

9.9.4. ***Business Intelligence features:***

9.9.4.1. Excel Services, PowerPivot and PowerView.

9.9.5. ***Business Solutions:***

9.9.6. Visio services.

9.9.7. Form based applications.

9.9.8. Business connectivity services.

9.10. **Microsoft Skype for Business Standard**

9.10.1. Microsoft Skype for Business Standard is a Microsoft Online Service which includes the following features:

9.10.2. Presence and group instant messaging.

9.10.3. File transfer from within an instant messaging session.

9.10.4. Application Catalogue and marketplace.

9.10.5. Audio and HD video calling to Skype for Business users.

9.10.6. Skype for Business Online is hosted and managed by Microsoft in international public cloud data centre(s).

9.11. **Microsoft Skype for Business Enterprise**

9.11.1. Microsoft Skype for Business Enterprise is a Microsoft Online Service which includes all the features of Microsoft Skype for Business Standard plus:

9.11.2. Group HD video calling.

9.11.3. Schedule meetings in Outlook.

9.11.4. Join meetings anonymously from web browsers.

9.11.5. Meeting controls for presenters and a meeting lobby for attendees.

9.11.6. Remote control of others' desktops.

9.11.7. Audio and video recording in meetings.

9.11.8. Interoperability with 3rd party dial-in conferencing providers.

9.12. **ID Sync Identity Management**

9.12.1.1. ID Sync provides event driven, real time integration between SP Control Panel and Customer Active Directory ('AD'). Allows for instant provisioning directly from Active Directory's Users and Computers.

9.12.1.2. Includes: Global Access List (GAL) Integration.

9.12.1.3. Includes: Support for AD Security Groups and Distribution Lists.

9.12.1.4. Includes: Full AD transaction auditing and reporting.

9.13. **Microsoft Office 365 Business**

Initial

9.13.1. Microsoft Office 365 Business is a Microsoft Online Service which includes the following features:

9.13.1.1. Microsoft Office Suite applications (1) Word, (2) Excel, (3) PowerPoint, (4) Outlook, (5) OneNote, (6) Publisher and (7) Sway

9.13.1.2. Each user can install Microsoft Office on 5 (five) Pcs or Macs, 5 (five) tablets (Windows, iPad, and Android), and 5 (five) phones.

9.13.1.3. Office Online which enables the creation and editing of Word, OneNote, PowerPoint, and Excel documents from a browser.

9.13.1.4. Support for Active Directory integration.

9.13.1.5. May only be used by organisations with a maximum of 300 (three hundred) users.

9.14. **Microsoft Office 365 Pro Plus**

9.14.1. Microsoft Office 365 Pro Plus is a Microsoft Online Service which includes the following features of Microsoft Office 365 Business plus:

9.14.1.1. Additional Microsoft Office Suite applications (1) Skype client, (2) Access

9.14.1.2. Business Intelligence features are enabled in Microsoft Excel.

9.14.1.3. May be used in virtual desktop enabled with Microsoft Remote Desktop services.

9.14.1.4. May be used by organisations of any size.

10. Access to the Service

10.1. The Service may be accessed via the internet or via a leased line, private circuit or Virtual Private Network (VPN). Internet access or network connection is not provided under this Service Schedule.

11. Storage, online support for the Technical Contact(s)

11.1. SP will provide a delegated provisioning tool, which will enable the System administrator(s) to manage user accounts and distribution lists; create new accounts, allocate resources and run reports.

12. Storage, backup and recovery

12.1. **Mailbox Storage**

12.1.1. Each mailbox will be allocated a storage quota corresponding to the edition specified in the prevailing Service Fees Schedule.

12.1.2. Mailbox storage may not be pooled and is reserved for each mailbox.

12.1.3. The user will be automatically notified by e-mail when the allocated storage capacity is nearing its agreed limit.

12.2. **SharePoint Backup and Storage**

12.2.1. The parent SharePoint site will be allocated all SharePoint storage which will be utilised by subordinate sites.

12.2.2. Additional storage requirements outside these limits will incur additional fees.

12.2.3. Backup will be provided by a rolling 14 day Deleted Items dumpster. Dumpster storage contributes to SharePoint storage quota.

12.3. **Hosted Exchange Backup and Recovery**

12.3.1. Backup will be provided by a rolling Deleted Items cache which can be accessed by users; and

12.3.2. By means of database availability groups, which depending on the edition, lagged copies of which may be replicated to a second data centre.

12.3.3. The following editions of mailboxes ('Single DC Mailboxes') are not replicated to a second data centre:

12.3.3.1. Hosted Exchange Small Business Lite Edition.

12.3.3.2. Hosted Exchange Small Business Standard Edition.

12.3.3.3. Hosted Exchange Super Lite Edition.

12.3.4. Data loss may occur in the event of loss/failure of some or all of the infrastructure in the data centre where the Single DC Mailboxes are provisioned.

Initial

12.3.5. Additionally, Customers who have a Cloud-Workspace subscription which includes RecoveryVault Express workstation backup may configure client-side backup of their outlook profiles. It is the sole responsibility of the Customer to monitor and manage all client-side backups.

12.4. **SyncVault™ Storage, backup and recovery**

12.4.1. Each user will be allocated SyncVault™ storage.

12.4.1.1. Additional storage within pre agreed limits may be allocated by the Technical Contact via the delegated provisioning tool.

12.4.1.2. Additional storage requirements outside these limits will incur additional fees.

12.4.1.3. SP shall be entitled to require a minimum storage allocation per user and vary these minimum requirements by way of 30 (thirty) days prior written notice.

12.4.2. Backup will be provided only by a rolling deleted Items cache which can be accessed by the Administrator or user.

12.4.3. Post-termination destruction of content:

12.4.3.1. After expiration of a Subscription or termination of this Agreement for any reason, SP or an applicable Software vendor, reserves the right to remove or destroy all content stored for that Subscription as part of the Service.

12.4.3.2. Prior to expiration of such period, SP may provide limited access to an account to permit retrieval or deletion of content (but not to change or add to existing content), provided that all fees due and owing to SP have been paid and the subscription was not terminated by SP.

12.4.3.3. Moreover, upon termination for any reason, users will no longer be able to access content stored in any SyncVault™ drive of the local computer(s) and must move Content from local SyncVault™ drives to some other drive prior to termination.

12.4.3.4. Content is account-specific; hence, purchasing a subscription to a new account will not enable access Content stored in another account.

13. Email Transmission Policy

13.1. SP prohibits the use of the Service to accept or transmit unsolicited bulk email.

13.2. In addition, email sent, or caused to be sent, to or through the Service that makes use of deceptive addressing will be deemed to be counterfeit and is prohibited.

13.3. Similarly, email that is relayed from any third party's email server(s) without the permission of that third party, or which employs similar techniques to hide or obscure the source of the email, is also prohibited.

13.4. SP does not authorize anyone to send email or cause email to be sent through the Service that violates SP' Email and Web Security Terms and Conditions.

13.5. Violations of this policy will result in immediate suspension of the Service and may result in civil and criminal penalties against the sender.

13.6. **Policy for Outbound Email Delivery**

13.6.1. Outbound email is defined as any email originating from customer mail server and delivered to recipients by the Service.

13.6.2. The following standards will apply, at SP's sole discretion, to the delivery of outbound email through the Service:

13.6.2.1. Connections from unsecured systems will be refused, including those that are open relays, open proxies, open routers, or any other system that has been determined by SP to be susceptible to unauthorized use.

13.6.2.2. Connections from systems that use dynamically assigned or residential IP addresses will be refused.

13.6.2.3. Messages that exceed 50 (fifty) megabytes in size will be refused.

13.6.2.4. Outbound connections will be refused from senders who are unable to accept at least 90 percent of bounce-return messages (such as "mailer-daemon failure" and/or "mailer daemon error" messages) generated by outbound email activity.

13.6.2.5. Complaints and/or blacklist data obtained from sources deemed credible by SP may be used as justification for suspending outbound delivery.

13.6.2.6. Unsolicited and/or bulk email will not be delivered and may result in suspension of outbound delivery.

13.6.3. In the event that outbound email delivery is suspended due to violations of this policy, SP will make a reasonable attempt to notify the Technical Contact of record for the account.

13.6.4. SP reserves the right modify its Transmission policy in its sole discretion without notice provided that any changes to its Transmission policy are posted on SP's public website.

Initial

13.7. **Outbound Abuse Policy**

13.7.1. As part of the around-the-clock monitoring and protection provided, SP helps to ensure the network integrity by identifying the following outbound threats:

13.7.1.1. Bulk Distributions.

13.7.1.2. Malicious spam, including Spam bots.

13.7.1.3. Open Relays.

13.7.2. All of these outbound threats are a violation of SP's Transmission Policy.

13.7.3. When a domain is found, in SP's sole discretion to be in violation of the Transmission Policy, and a decision has been made to suspend services, SP will make a reasonable effort to notify the Technical Contact.

13.7.4. Technical Contact will be provided with data on the source of the violation, which may include some or all of the following information:

13.7.4.1. Offending domain

13.7.4.2. Sending IP

13.7.4.3. Message Subject Line

13.7.4.4. Sending Address

13.7.4.5. Recipient Address

13.7.4.6. Aggregate Number of Messages Sent.

13.7.5. Please note that the pieces of data included in the service request may vary based on the type of Outbound Abuse being investigated.

13.7.6. Any violation may result in having outbound services for one (or all domains) suspended until the source of the issue is found and corrected.

13.7.7. Repeated violations for the same type of issue may result in having the outbound service permanently revoked.

13.7.8. SP may consider reinstatement of suspended outbound services after each of the following questions has been addressed to SP's satisfaction:

13.7.8.1. Provide detailed steps that were taken to diagnose the incident and verify the source of outbound mail documented in the service request.

13.7.8.2. Identify the verified source of the outbound mail. If a mass-mailer worm or other internal infection was found, provide the name of the worm or details on the vulnerability and details on how this has been remediated.

13.7.8.3. Identify the steps taken to correct the problem. Provide details on the actions performed, including the names of the tools and utilities used to identify and remediate the issues. (NOTE – Blocking access to a single computer on your network that is infected is NOT sufficient to allow reinstatement).

13.7.8.4. Outline steps taken to prevent future occurrences. Provide details on active steps being taken such as automated virus signature updates and malware scans.

13.7.9. Information requested above must be supplied to SP in order to be considered for reinstatement.

13.7.10. Requests for reinstatement may require 24 hours for examination and evaluation.

13.7.11. In very limited cases, SP may make the decision to permanently revoke Outbound Filtering.

13.7.12. As part of the suspension of Outbound Filtering, SP will remove the outbound IP and package from the Control Panel.

13.7.13. SP is not responsible for removing the smart host entry for the Service and establishing a different smart host or relay on their mail server by entering the appropriate IP or hostname.

14. Email Transmission Troubleshooting

14.1. Some or all of the following information may be required when logging a service request for troubleshooting:

14.1.1. Sending IP

14.1.2. Message Subject Line

14.1.3. Sending Address and Recipient address

14.1.4. Control console

14.1.5. Domain(s) affected

14.1.6. Scope of domains affected: All domains / Some domains / Single domain

14.1.7. Scope of messages affected: All messages / Some messages / Single message / No message impact

14.1.8. Scope of users affected: All users / Some users / Single user / No user impact

Initial

14.1.9. Description of the primary issue

14.1.10. Frequency of the issue

14.1.11. Date and time of transmission

14.1.12. Message header or bounce message

14.1.13. Message ID

14.1.14. Mail server logs

15. Email Journaling and journaling agent

15.1. "Journaling" is the ability to record all communications, including email communications, in an organization for use in the organization's email retention or archival strategy. To meet an increasing number of regulatory and compliance requirements, many organizations must maintain records of communications that occur when employees perform daily business tasks.

15.2. In a Hosted Exchange organization, all email traffic is routed by mailbox servers. All messages traverse at least one server running the transport service in their lifetime. When journaling is enabled for a mailbox, a compliance-focused Journaling transport agent processes messages on these mailbox servers. It fires on the *OnSubmittedMessage* and *OnRoutedMessag*e transport events.

15.3. Journaling can be enabled for organisations that are enabled for Hosted Email Archiving.

15.4. The following is required for any journaling where Hosted Messaging Services Email Archiving is not used:

15.4.1. A Hosted Exchange Professional mailbox to be designated as the target journal mailbox.

15.4.2. An active Support Services subscription.

15.4.3. A 3rd party Archive service configured to collect and process messages from the journal mailbox.

15.4.4. All mailboxes within the organisation need to be enabled for archiving.

16. Email Migration Management Accelerator

16.1. The Email Migration and Management Accelerator ('EMMA') provides orchestration tools to ensure a seamless migration of the mailbox contents of a pre-existing e-mail environment to Hosted Exchange.

16.2. EMMA will migrate mailbox content from a Microsoft Exchange Server environment, as well as POP3 and IMAP mailboxes, to Hosted Exchange.

16.3. Our migration methodology is formulated in two steps:

16.3.1. Step One: Completion of a Hosted Exchange template which contains all the user details for the mailbox creation.

16.3.2. Step Two: Alteration of organisation's domain name so that mail is delivered to SP which in turn redirects mail back to the existing server until migration. This will assist with the DNS cut over as mail will be spooled to ensure no mail is lost. Our Auto-configuration tool allows creation and configuring of new profiles on each users' PC without impacting them. Mail can be ingested in two ways:

16.3.2.1. Export the old mail from the old mail profile to a PST file and links the PST to the new profile or;

16.3.2.2. Mail can be extracted and imported into the new mail box via one of the three migration methods: Flash, Backfill or Co-existence.

17. Technical requirements

17.1. The following minimum system requirements are required in order to access the Service:-

17.1.1. Internet Explorer 11 (OWA access) or greater.

17.1.2. Hosted Exchange and Exchange Online works with any version of Outlook that is in mainstream support from Microsoft, which includes the latest version of Outlook 2016, Outlook 2013, and Outlook 2011 for Mac. Outlook 2010 SP2 (October 2015 PU KB3085604) – will be supported in Hosted Exchange with reduced functionality until October 2016. As of 1st of May 2016, the Minimum required updates for mainstream versions of Outlook are:

17.1.2.1. Outlook 2016: April 2016 PU KB3114972

17.1.2.2. Outlook 2013: Service Pack 1 with April 2016 PU KB3114941

17.1.3. Inbound email quarantine access via IMAP requires a mail client which supports write-only access.

17.1.3.1. Note: Microsoft Outlook does not support write-only access via IMAP.

17.1.4. Windows 7 SP1 (RPC/HTTP Compression).

Initial

17.1.5. For optimum Hosted Exchange use, SP recommends a bandwidth allocation of 16k per user.

17.1.6. Additional bandwidth may be required when making use of SharePoint. Suggested bandwidth requirements for a range of user community sizes are available upon request.

17.1.7. SP recommends a bandwidth allocation of 64k per 10 (ten) Gigabytes of SyncVault™ Storage updates made per month.

17.1.7.1. Additional bandwidth will be required when re- synchronising or recreating a user's SyncVault™ storage.

17.1.7.2. ID Sync requires Windows Server 2008 or higher, NET Framework 4.0, and Microsoft SQL Server Express with a Native Client.

18. Service Availability

18.1. If the Service is unavailable it must be reported to the SP and acknowledged by SP.

18.2. The period of Downtime will be calculated from when the fault is reported, SP has issued a fault report reference and has acknowledged this as a fault on the Service.

18.3. Following investigation and repair SP will advise the time that the Service was restored. This will be deemed to be the end of the Downtime unless the fix is not confirmed.

18.4. **Hosted Exchange and Exchange Online**

18.4.1. "**Downtime**" means any period of time when users are unable to send or receive email with Outlook Web Access.

18.4.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

$$\frac{\text{User Minutes - Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in User Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident

18.4.3. Exclusions to Service Availability Guarantee:

18.4.3.1. Mailboxes protected by an email filtering service from a provider other than SP will be excluded from the Service availability guarantee.

18.4.3.2. Any incident lasting less than 15 (fifteen) minutes.

18.4.4. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 98 %	14.4 hours	No Credit	50%	
< 95 %	36 hours	100%		

18.5. **Microsoft Office 365 Business and Microsoft Office 365 ProPlus**

18.5.1. "**Downtime**" means any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

18.5.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

$$\frac{\text{User Minutes - Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in User Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident

18.5.3. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 99 %	7.2 hours	No Credit	50%	
< 95 %	36 hours	100%		

18.6. **Microsoft Project Online**

18.6.1. "**Downtime**" means any period of time when users are unable to read or write any portion of a SharePoint Online site collection with Project Web App for which they have appropriate permissions.

18.6.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

Initial

$$\frac{\text{User Minutes - Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in User Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident

18.6.3. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 99 %	7.2 hours	No Credit	50%	
< 95 %	36 hours	100%		

18.7. **Microsoft SharePoint Online**

18.7.1. "**Downtime**" means period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

18.7.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

$$\frac{\text{User Minutes - Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in User Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident

18.7.3. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 99 %	7.2 hours	No Credit	50%	
< 95 %	36 hours	100%		

18.8. **Microsoft Skype for Business Online**

18.8.1. "**Downtime**" means any period of time when end users are unable to see presence status, conduct instant messaging conversations, or (in the case of Skype for Business Online Plan 2) - initiate online meetings.

18.8.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

$$\frac{\text{User Minutes - Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in User Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident

18.8.3. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 99 %	7.2 hours	No Credit	50%	
< 95 %	36 hours	100%		

18.9. **Microsoft Skype for Business Online – PSTN Calling and PSTN Conferencing**

18.9.1. "**Downtime**" means any period of time when end users are unable to initiate a PSTN call or unable to dial into a PSTN conference.

18.9.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

$$\frac{\text{User Minutes - Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in User Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident

Initial

18.9.3. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 99 %	7.2 hours	No Credit	50%	
< 95 %	36 hours	100%		

18.10. **Microsoft Skype for Business Online – Voice Quality**

18.10.1. This applies to any eligible call placed by any voice service user within the subscription (enabled for making any type of call VOIP or PSTN).

18.10.2. "**Eligible Call**" means a Skype for Business placed call (within a subscription) that meets both conditions below:

18.10.2.1. The call was placed from a Skype for Business Certified IP Desk phones on wired Ethernet

18.10.2.2. Packet Loss, Jitter and Latency issues on the call were due to networks managed by Microsoft.

18.10.3. "**Total Calls**" is the total number of Eligible Calls

18.10.4. "**Poor Quality Calls**" is the total number of Eligible Calls that are classified as poor based on numerous factors that could impact call quality in the networks managed by Microsoft. While the current Poor Call classifier is built primarily on network parameters like RTT (Roundtrip Time), Packet Loss Rate, Jitter and Packet Loss-Delay Concealment Factors, it is dynamic and continually updated based on new learnings from analysis using millions of Skype and Skype for Business calls and evolution of Devices, Algorithms and end user ratings.

18.10.5. "**Monthly Good Call Rate**" is calculated using the following formula:

$$\frac{\text{Total Calls} - \text{Poor Quality Calls}}{\text{Total Calls}} \times 100$$

18.10.6. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 99 %	7.2 hours	No Credit	50%	
< 95 %	36 hours	100%		

Initial