NJ Deliver STATE MESSAGING SYSTEM

Security Plan

NJDelivery Tenant Policy

Department or Agency Type	Enterprise Fit	Enterprise DNS	State Policies	EESGCIS
State O365 tenant	Best	Y	Y	Y
Separate O365 tenant with addressing	Exception	Y	Y	Y
Separate O365 tenant and non-addressing	Exception	Optional	Optional	Optional

1. State O365 tenant – Executive branch Departments and Agencies are expected to migrate to (or join) the State O365 tenant, administered by OIT. This will ensure maximum savings to the State, provide a seamless integration of the department's or agency's address book into the State Global Address List, and ensure maximum conformance with State security policies, standards, and procedures.

2. Separate O365 tenant with addressing – A major Department or Agency is required to use the addressing in the nj.gov domain (e.g., @agency_name.nj.gov) or njagency_name.gov domain (e.g., @njagency_name.gov), and seeks to establish a separate O365 tenant, the department or agency must submit a justification to OIT. Any department or agency granted an exception must participate in the enterprise DNS service (administered by OIT) and conform to the enterprise security policies, standards, and procedures (defined by OIT), including using the Enterprise E-mail Security, Relaying and Content Inspection Gateways (EESGCIS) (administered by OIT).

3. Separate O365 tenant and non-addressing – If any other agency (Commissions and Authorities) who are not subject to the State of New Jersey's Executive Order State of New Jersey. N.J.S.A. 52:18a-230 b and are not using the addressing nj.gov domain (e.g., @agency_name.nj.gov), and seeks to establish a separate O365 tenant, the agency must submit a justification to OIT. Any agency granted an exception has the option to participate in the enterprise DNS service (administered by OIT) and conform to the enterprise security policies, standards, and procedures (defined by OIT), including using the Enterprise E-mail Security, Relaying and Content Inspection Gateways (administered by OIT).

Messaging

	On-Premise	Office 365
Risks	1) On-Premise State Employees will access the Messaging environment from the office or remotely through the State's VPN and Portal. Users that access their email via VPN will be able to store their messages in a locally cached OST file. VPN use requires a State provided computer. 2) The State may have no legal rights to the personal computer. 3) On-Premise State Contractors will access the Messaging environment through Portal.	1) Office 365 offers an employee access to the Microsoft services and data from a home computer. All email content (cached locally) can be stored to the home computer. The State may have no legal rights to the personal computer. 2) State IT have no method for verifying if a personal computer has the appropriate security software and Microsoft updates to protect the State's infrastructure and intellectual propriety.
NJ State Government Disclaimer displayed prior to log in	Yes	Yes
NJ State Government Email Disclaimer	Yes	Yes

	On-Premise	Office 365
Employee acceptance and trust	Relies on employee's trust not to store content on home or untrusted computers. Management and auditing of events will be required.	Relies on employee's trust not to store content on home or untrusted computers. Management and auditing of events will be required.
User must sign the NJDelivery@ User Agreement	The agency is responsible to ensure employees sign the user agreement.	The agency is responsible to ensure employees sign the user agreement.
Physical Hardware Monitoring	24x7 Monitoring through the Performance system. All servers are located at the Hub and Hamilton locations are monitored. Physical access control uses multiple authentications and security processes, including badges and smart cards, on-premise security guards, continuous video surveillance, and single-factor authentication. Based on the OIT Policy "OIT Facility and Computer Room Access - HUB, SAC, OARS & Riverview."	24x7 Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication.

	On-Premise	Office 365
Tenants	The on premise Messaging environment 365 is designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments.	Office 365 is designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments.

	On-Premise	Office 365
Network Security	Firewall Intrusion Detection (Prevention planning underway) Denial of Service Secure physical separation from other State security zones and Intranet Port scanning and remediation, and perimeter vulnerability scanning	Firewall Intrusion Prevention Denial of Service Secure physical separation of critical back-end servers and storage devices from the public-facing interfaces Port scanning and remediation, and perimeter vulnerability scanning
Systems are secure (harden) Security Best Practice	On-premise servers and services were hardened based on the Center for Internet Security (CIS) Benchmark tool and the State's minimum system security and protection policy and standard. Continuous Virus Protection enabled reporting to the State's Security Incident Event Management (SIEM) System. Operating System and software patching to the latest updated security software.	Office 365 is a security-hardened service that has security features built into the service. Microsoft has a best practice to secure their systems. Security Development Life Cycle. Operating System and software patching to the latest updated security software.

	On-Premise	Office 365
Access Management	Role-based controls, delegated administration Integration with Active Directory and Portal	Client-based access control, open to the Internet Role-based controls, delegated administration Office 365 integration with Active Directory Federation Services (AD FS) (Encrypted) Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process.

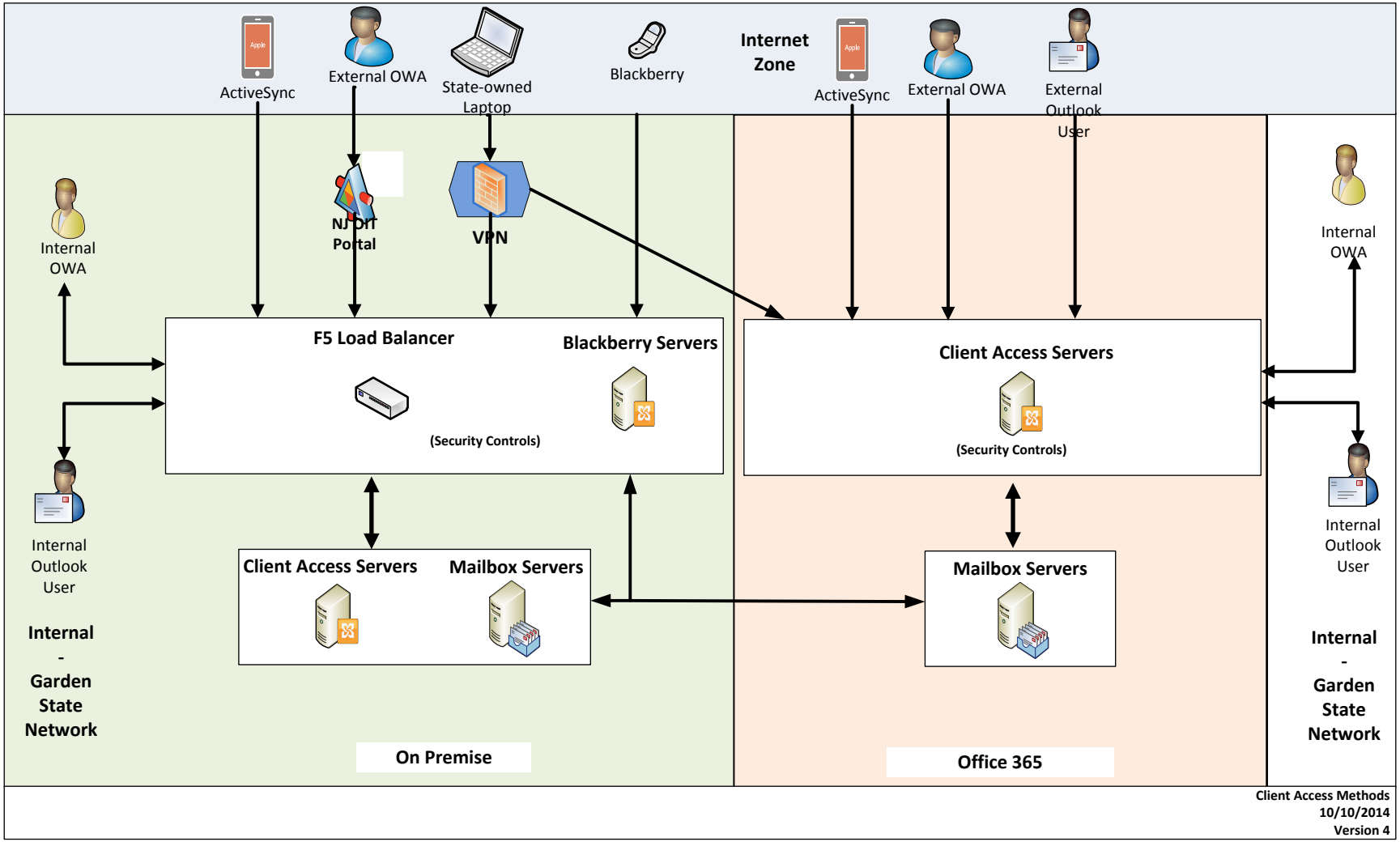
	On-Premise	Office 365
Client Access Communication Protocols	Primary – RPC over HTTPS Secure sockets layer (SSL) for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP within the Intranet. Allows access to Outlook Web App through the State Portal, limited access to ActiveSync for mobile device directly through the Internet, and access to the State's Blackberry 5 system directly through the Internet. TLS between agencies' email routing systems through the State of NJ's Enterprise Email Relay and Content Inspection.	Primary - RPC over HTTPS Secure sockets layer (SSL) for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP. Allows Outlook Web App, limited access to ActiveSync for mobile device directly through the Internet, and access to the State's Blackberry 5 system directly through the Internet. TLS between Office 365 and external servers for both inbound and outbound email through the State of NJ's Enterprise Email Relay and Content Inspection.

	On-Premise	Office 365
Encrypted Data	Data at rest is not encrypted as it is stored on the enterprise SAN	All email content is encrypted on disk using BitLocker Advanced Encryption Standard (AES) encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/message tracking logs.
Data Loss Prevention	Monitor content through the State of NJ's Enterprise Email Relay and Content Inspection. Long term block with notification.	Users are blocked when attempting to send sensitive data. • Currently in audit mode
Audit and retention	Enable log events on the Servers, including viewing, and editing. Plan to forward log events to the State of NJ's SIEM. Retention schedule is set to indefinite years unless the agency has an approved electronic file plan that may dispose of the audit records less than or indefinite years.	Enable log events, including viewing, editing, and deleting content. Retention schedule is set to indefinite years unless the agency has an approved electronic file plan that may dispose of the audit records less than or indefinite years.

	On-Premise	Office 365
eDiscovery	Retention schedule default 7 years unless the agency has an approved electronic file plan that may dispose of the audit records less than or greater than 7 years.	- eDiscovery and data spillage - delegate to specialist users for compliance. Retention schedule default 7 years unless the agency has an approved electronic file plan that may dispose of the audit records less than or greater than 7 years.
Anti-malware/anti-spam controls	Inbound and outbound email routed through the State of NJ's Enterprise Email Relay and Content Inspection. External (Proofpoint on Demand), and Internal (On-premise).	Inbound and outbound email routed through the State of NJ Enterprise Email Relay and Content Inspection (Proofpoint on Demand)
Authentication	Single factor (transition to multi-factor)	Single factor (transition to multi-factor)

	On-Premise	Office 365
Independent verification and compliance	State owned certification and accreditation.	Office 365 has obtained independent verification, including ISO 27001 and SSAE16 SOC 1 (Type II) audits, is able to transfer data outside of the European Union through the U.S.-EU Safe Harbor Framework and the EU Model Clauses, is willing to sign a HIPAA Business Associate Agreement (BAA) with all customers, has received authority to operate from a U.S. federal agency under FISMA, and has disclosed security measures through the Cloud Security Alliance's public registry.

Client Access Method



Client Access Service Settings

	Microsoft Default	On-Premise	Office 365
Outlook Internal	Cache on	Cache on	Cache on
Outlook External (anywhere)	Cache on	Cache on	Cache on
Outlook Web App for Mobile device	Enabled	Not available	Disabled
• OWA Offline Access	Enabled	Not available	Enabled
Mobile device Web client with Active Sync	Enabled w/Quarantined until approval	Enabled w/Quarantined until approval	Enabled w/Quarantined until approval
POP			
• SSL	Enabled	Enabled	Enabled (legacy system required)
IMAP			
• SSL	Enabled	Enabled	Enabled(legacy system required)

MAPI			
• SSL	Enabled	Enabled	Enabled
EWS (Exchange Web Service) Application access	Enabled	Enabled	Enabled

References

Microsoft – Security in Office 365 2013

State of New Jersey Security Policies, Standards and Procedures (http://nj.gov/it/ps/security)

Skype for Business

	On-Premise	Office 365
Risks	1) On-Premise State Employees will access the Lync environment from the office or remotely through the State's VPN. 2) Lync can be accessed on a personal computer and the State may have no legal rights to the personal computer. 3) Files can be transfer to their personal computer. 4) Access to Public IM systems could introduce malware via links.	1) Lync can be accessed on a personal computer and the State may have no legal rights to the personal computer. 2) Files can be transfer to their personal computer. 3) Access to Public IM systems could introduce malware via links. 4) State IT have no method for verifying if a personal computer has the appropriate security software and Microsoft updates to protect the State's infrastructure and intellectual propriety.
NJ State Government Disclaimer displayed prior to log in	Yes	Yes
Encrypted Data (File Store, SQL store, etc.)	In-transit only	In-transit only
Systems Secured (hardened)	Same as Messaging	Same as Messaging
Access management	Same as Messaging	Same as Messaging

	On-Premise	Office 365
Client Access	Primary - Lync 2013 HTTPS ports 80/443 internal Port 8080/4443 external *Only Lync 2013 provides complete logging and archiving functions Others – Lync Mobile, Lync Web App, Lync 2010	Primary – Lync 2013 HTTPS ports 80/443 Microsoft Office 365 traffic (both signal and media traffic) is encrypted by using the Transport Layer Security (TLS) protocol. *Only Lync 2013 provides complete logging and archiving functions Others – Lync Mobile, Lync Web App
Data Loss Prevention	Controls in Place	Controls in Place
Audit and Retention	Enable log events on the Servers, including viewing, and editing. Plan to forward log events to the State of NJ's SIEM. Retention schedule is set to indefinite unless the agency has an approved electronic file plan that may dispose of the audit records less than or indefinite years.	Enable log events, including viewing, editing, and deleting content. Retention schedule is set to indefinite unless the agency has an approved electronic file plan that may dispose of the audit records less than or indefinite years.
eDiscovery	Retention schedule default 7 years unless the agency has an approved electronic file plan that may dispose of the audit records less than or greater than 7 years.	- eDiscovery and data spillage - delegate to specialist users for compliance. Retention schedule default 7 years unless the agency has an approved electronic file plan that may dispose of the audit records less than or greater than 7 years.

	On-Premise	Office 365
Anti-malware/anti-spam controls	No	No
Authentication	Clients will use SRV records for automatic sign in, SRV records will be created to direct users to either the Hamilton or HUB Lync Enterprise Pools	Lync Online now supports both authenticated and unauthenticated Lync Web App attendees. If a user receives a Lync Meeting invitation but does not have an account with your organization, he or she can still join the meeting by using Lync Web App and signing in with the Guest account. Federation in Office 365 is only supported between other Lync/OCS/LCS environments, with appropriately configured Access Proxy or Edge servers.
Independent verification and compliance	Same as Messaging	Same as Messaging

Policies

Policy Name	Scope	Settings	Default	On Premise	Office 365
Global	Global	IM and Presence	Enabled		Enabled
		Conferencing	Company		Company
		PSTN Conferencing	Enabled		
		Enterprise Voice	Enabled		
		Instant Messaging Conferencing service	Enabled	Enabled	Enabled
		Web Conferencing service	Enabled	Enabled	Enabled
		Application Sharing service	Enabled	Enabled	Enabled

Conferencing Policies

Policy Name	Scope	Settings	Default	On Premise	Office 365
Global	Global	Allow participants to invite anonymous users	Enabled	Disabled	Disabled
		Recording	None		
		Allow Federated and anonymous participants to record	Disabled	Disabled	Disabled
		Enable PSTN dial-in conferencing	Disabled	Disabled	Disabled
		Allow anonymous participants to dial out	Enabled	Disabled	Disabled
		Allow multiple video streams	Enabled	n/a	n/a
		Allow participants not enabled for Enterprise Voice to dial out	Disabled	Disabled	Disabled
		Data Collaboration	Enabled		
		Allow federated and anonymous participants to download content	Disabled	Disabled	Disabled
		Allow participants to transfer files	Enabled	Disabled	Disabled
		Enable annotations	Enabled	Enabled	Enabled
		Application Sharing	Enabled	Enabled	Enabled
		Allow participants to take control	Enabled	Enabled	Enabled
		Allow federated and anonymous participants to take control	Enabled	Enabled	Enabled
		Participant Policy	Enable application and desktop sharing		
		Enable Peer to Peer file transfer		Disabled	Disabled
		Enable Peer to Peer recording	Disabled	Disabled	Disabled

Meeting Room Policies

Policy Name	Scope	Settings	Default	On Premise	Office 365
Global	Global	PSTN callers bypass lobby – Enabled	Enabled	Enabled	Enabled
		Designate as presented	Company		
		Assigned conference type by default	Enabled	Enabled	Enabled
		Admit anonymous users by default	Enabled	Disable	Disable

Lync client Settings

	Microsoft Default	On-Premise	Office 365
Lync 2013	Clients will use SRV records for automatic sign in, at present SRV records point to AUS Pool this will change at the end of full project to point to CA Pool. Client-side recording of audio, video, application sharing, desktop sharing, and uploaded content Client-side recording of file transfers, shared OneNote pages, and PowerPoint annotations	All machines have the default admin shares enabled. Logging should be enabled Archiving of IM conversations in Outlook Conversation History Upload files to share with others Client-side archiving of file transfers, shared OneNote pages, and PowerPoint annotations	Logging should be enabled Archiving of IM conversations in Outlook Conversation History Upload files to share with others Client-side archiving of file transfers, shared OneNote pages, and PowerPoint annotations
Lync 2010 Client		Logging should be enabled Archiving of IM conversations in Outlook Conversation History	Logging should be enabled Archiving of IM conversations in Outlook Conversation History
Lync Mobile		Logging should be enabled Archiving of IM conversations in Outlook Conversation History	Logging should be enabled Archiving of IM conversations in Outlook Conversation History

OneDrive for Business

	Office 365
Risks	1) Office 365 offers an employee access to the Microsoft services and data from a home computer. All content (cached locally) can be stored to the home computer. The State may have no legal rights to the personal computer. 2) State IT have no method for verifying if a personal computer has the appropriate security software and Microsoft updates to protect the State's infrastructure and intellectual propriety.
NJ State Government Disclaimer displayed prior to log in	Yes
Encrypted Data (File Store, SQL store, etc.)	Yes
Systems Secured (hardened)	Same as Messaging
Access management	Same as Messaging
Client Access	Primary – HTTPS ports 80/443 Microsoft Office 365 traffic (both signal and media traffic) is encrypted by using the Transport Layer Security (TLS) protocol.

	Office 365
Data Loss Prevention	Yes (requires running queries to identify the sensitive data and working with the containers “sites” owner to have appropriate rights configured for that data.)
Audit and Retention	Enable log events, including viewing, editing, and deleting content. Retention schedule default 7 years unless the agency has an approved electronic file plan that may dispose of the audit records less than or greater than 7 years. ========== Configurable to organization’s retention schedule.
eDiscovery	- eDiscovery and data spillage - delegate to specialist users for compliance. Retention schedule default 7 years unless the agency has an approved electronic file plan that may dispose of the audit records less than or greater than 7 years.
Anti-malware controls	Yes
Authentication	Single factor (transition to multi-factor)
Independent verification and compliance	Same as Messaging