Oakland County Michigan

Technical Design Review

Document Version Date: 6/20/2018

Technical Design Review – Instructions

Purpose:

The Technical Design Review Process of Oakland County's Information Technology Department has been designed to ensure the quality of systems and applications and provide guidance for decision makers. It is a multi-disciplined technical review to ensure that an application / system can proceed into design and can meet or exceed IT standards, security, and performance requirements within cost, at an acceptable risk.

Entry Instructions

Follow the technical design review process defined here.

1. Complete the **Overview** tab in this document.

   Example of a completed Overview tab

2. Provide the detailed System Design Diagram.

   Example of a Detailed System Design Diagram

Approval Criteria:

1. An **approved** detailed system design.
2. Completion of all action items assigned to the project team / solution provider.
3. All issues in the Technical Design Review have been resolved.

Oakland County Michigan
Technical Design Review

Document Version Date: 6/20/2018

Project ID & Name:	
Project Description:	

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Environment						
Infrastructure	Describe the type of infrastructure being proposed (Cloud, Virtual On-Premise, Physical Hardware or Hybrid). Provide the server specifications if the proposed solution is non-Cloud.	Cloud	Virtual On-Premise (VMware)	Physical Hardware		
Network Transport - Connection Type	Describe the Network Connection bandwidth for servers and workstations required for your solution (e.g., 100MB, 1GB or 10GB). Describe if there are any special network requirements for the solution (e.g., Latency, Jitter, etc.)	Required Network Connection Bandwidth: **Server**: 1GB or less **Workstations**: 100MB or Less	Required Network Connection Bandwidth: **Server**: Greater than 1GB but less than 10GB **Workstations**: 100MB to 1GB	Required Network Connection Bandwidth: **Server**: 10GB or greater **Workstations:** 1GB or greater		

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Network Transport - Server Location	Provide connection diagram that shows the specifications for each connection that includes the source and destination for those connections. The specification will include server location (e.g., Internal network, DMZ network, etc.) with port and protocol in use for the connection.	Load balancer(s) and/or Web/Frontend servers in DMZ; other backend servers in Internal network	Single standalone servers in DMZ or Internal network	Specialized networking requirements or network segmentation		
Network Transport - Application Behavior	Describe the testing that is performed with your solution for firewalls, intrusion protection systems, or other security systems.	The solution is fully tested against stateful inspection or next generation firewalls and intrusion protection systems	The solution is not tested against stateful inspection or next generation firewalls and intrusion protection systems	Known issues working with stateful inspection or next generation firewalls and intrusion protection systems.		
Network Transport - Access Layer Changes	Describe any required changes in the access layer of network transport (additional vLAN's, new isolated network, redesign or rework of existing network, etc.)	No Change	Capacity, Mandated or Public Safety	Change required, not related to Capacity, Mandate or Public Safety		
Wireless Services	Describe the wireless services this solution utilizes and the encryption method(s) for transmission.	The solution is NOT planning on leveraging wireless services	The solution is planning on leveraging wireless services with encryption technologies	The solution is planning on leveraging wireless services without encryption technologies		
Operating System (OS)	Describe the Operating System(s) (OS) and OS release(s) on which your solution/product can run.	Windows 2012; Red Hat Linux; Oracle Linux	Supported versions of Windows or Linux Red Hat and Oracle	End of Life (EOL) OS releases or non-standard OS		
Antivirus/Malware	Describe the Antivirus/Malware solution(s) with which your solution/product will function.	Utilizes currently defined standards	Utilizes a non-standard Antivirus and/or Malware	Does not work with Antivirus and/or Malware		

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Database (DB)	Describe the database(s) and DB release(s) with which your solution/product will operate.	MS SQL 2012 or greater	Oracle 12C or greater	Other DB		
Reporting Tools	Describe the reporting packages that are included with your solution/product.	SSRS (SQL Server Reporting Services)	Business Objects	Other		
Type of User	Describe if the users are internal and/or external and how they are defined.	Users defined by Role	Users defined by AD Groups	Users not defined or solution utilizes internal user store within the application		
Number of Users	Describe the number of users to the system by **Type of User**.	Number of users	Not applicable	Number of users unknown		
Application						
Criticality	Describe if the application is **Business**, **Business Critical**, or **Mission Critical**.	Business application	Business Critical application	Mission Critical application		
Compliance	Describe the legal standards with which your solution complies (e.g., HIPAA, PCI, CJIS, SOC 2, etc.).	No compliance requirement	Compliance requirement is unknown	Compliance required (e.g., HIPAA, PCI, CJIS, PII, SOC 2, etc.)		
Application Type	Describe the application type (e.g., SaaS, web application, thick client, etc.).	SaaS (Software as a Service) application	Web application	Thick application		
Custom Programming	If custom programming is needed, describe the language(s) used.	.Net or Python	Not applicable	Java or other		

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Abridged ADA Compliance - WCAG 2.0 Unabridged ADA Compliance - WCAG 2.0	Does the application meet Americans with Disability Act (ADA) requirements.	Meets ADA requirements	Not applicable	Non Compliant		
Application Protection - Web Application Firewall (WAF)	Does the application meet requirements.	Preferred	Acceptable	Review required		
Authentication / Authorization Method	Describe the type of Authentication method that is utilized (e.g., Microsoft AD, LDAP, SAML, etc.).	Active Directory for a user store; SAML, Kerberos, and LDAP are the accepted protocols	NT LAN Manager (NTLM) Authorization	Authorization and/or user store built into the application		
Data						
Data Classification	Describe the data type to be stored in this system (Public, Internal Use Only, Confidential Data, Restricted Data (HIPAA, PCI, CJIS, or PII) or Unknown).	Public or Internal Use data	Confidential data	Restricted data: (HIPAA, PCI, CJIS, or PII) or Unknown		
Data Security	Describe what encryption is to be used, and in what form (at rest, in transit, or both).	Data is encrypted in transit and at rest via Certificate (required for restricted data) No encryption required (acceptable for Public or Internal Use)	Data is encrypted in transit with Certificate (required for confidential data)	Unknown		
Backup and Recovery	Describe the method for backup and recovery (Cloud, Disk to Disk, Disk to Tape, etc.) Describe who is responsible for the backup and recovery.	SAN Replication and Disk to Disk	Disk to Tape	Unknown or no backup		

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO)	Describe your standard Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the solution.	Meets or exceeds Oakland County RTO/RPO	Relies on Oakland County for RTO/RPO	Does not meet Oakland County RTO/RPO		
Retention and Purge	Describe the data retention and purge needs of your solution.	Defined requirements and purge criteria	Not Applicable	Criteria is not defined		
Client						
Network Transport - Workstation Location(s)	Describe your Client connections (LAN, WAN, or Internet based). If peer to peer connections are required, explain why.	All Client connections are from existing local area or wide area network	Unknown client requirements	Peer to peer connectivity or new VLAN required		
Internet Browser	Describe the browser(s) and version(s) you support.	IE, Firefox, Chrome External	Chrome Internal	Other		
Client (Workstation) Hardware / Software	Describe the workstation requirements including Operating System, hardware requirements and any additional software required.	Windows 10	Windows 7	Other OS		
Local Workstation Security	Describe the workstation security requirements for your solution.	No administrative rights required	Elevated rights required	Local administrative rights required		
Maintenance						
Application updates	Describe your release and patch cycles.	Defined release and patch cycle(s)	Not Applicable	No release and/or patch cycles defined		
Disaster Recovery	Describe monitoring and alerting options provided by your solution.	Fully Redundant	Resilient	Single Points of Failure		
Fault Tolerance	Describe your release and patch cycle.	Meets Fault Tolerance Standard	Meets a mid-level Fault Tolerance	Does not meet minimum defined standard for Fault Tolerance		

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Monitoring and Alerting	Describe monitoring and alerting options provided by your solution.	Defined monitoring and alerting	Not Applicable	No monitoring and/or alerting defined		

Area	Function	Standard	Notes
Hardware	Server Platform (Virtual - Hosted)	Amazon Web Services	Preferred Cloud Platform
Hardware	Server Platform (Virtual - on-Prem)	VMware Virtual Server	If Virtual Server is required
Hardware	Server Platform	Dell Blade Server (hardware is 5 years old or newer) If it is a VM, it will be upgraded through a different process and kept current.	Must be a Dell Blade Server; all servers should be Cloud or Virtual if physical server is required.
Network	Network Transport - Server Location	Reduce complexity and cost by standardizing existing networks for server platforms. All front-end servers that terminate public or private connections will be placed in an existing network designed for this purpose (OCDMZ). All back-end servers will be placed in an existing network designed for this purpose (OCSRV, CLMSRV). If any new networks are needed please provide a detailed specification for the new environment. Link: TCP/IP – See Network Transport Design Document	
	Network Transport - Client	Reduce complexity and cost by standardizing existing networks for clients; all client connections will be placed in an existing local area or wide area network (OCLANX, OCWANX). No peer to peer connectivity will be permitted; all traffic will be routed to the client default gateway for security control and bandwidth management. The only exception will be direct LPR printing to the local printer. If any new networks are needed please provide a detailed specification for the new environment. Link: TCP/IP – See Network Transport Design Document	
	Network Transport – Data Transfer Specifications	Provide minimum specifications for network transport that include any jitter, latency, and bandwidth requirements for all connections in the solution. Jitter and latency in milliseconds bandwidth in appropriate industry standard format (kb,mb,gb).	
	Network Transport – Port and Protocol Specifications	Provide connection diagram that shows the specifications for each connection that include the source and destination for the connections. The specification will include port and protocol in use for the connection.	
	Network Transport – Port and Protocol Specifications	Provide any known anomalous behavior of the solution when connections are made through next generation firewalls, state-full inspection firewalls, intrusion protection systems or other known conflicts with security systems.	
OS Release	Operating System - Server	Options with Architectural Approval: Windows 2012 or higher Red Hat Linux Oracle Linux	

Area	Function	Standard	Notes
Software Standards	Antivirus/Malware	McAfee Virus Scan/Enterprise 8.8 and Anti Spyware Enterprise	
Software Standards	Browser	Internet Explorer 11 and Mozilla Firefox	
Software Standards	Defect Management	Bugzilla	
Software Standards	ETL (Extract Transform and Load)	SSIS	
Software Standards	Email/Office Tools	Microsoft Office 365 Word Excel PowerPoint	
Software Standards	Process Flow	Visio	
Software Standards	PMO	Clarity	
Software Standards	Project Management	Open Workbench	
Software Standards	Reverse Proxy / Load Balancer	NGINX Plus	
Software Standards	Source Control, Test Case Management, Bug Management	TFS (Team Foundation Server)	
Software Standards	Time Management System for Contractors	Time Tracker	
Software Standards	User Stores/Identity	Active Directory	
Software Standards	Virtualization	VMWare	

Area	Function	Standard	Notes
Database	Database Release	Standard: SQL Server 2012 or 2016 Optional with Architecture Approval: SQL Server 2012, 2016, Oracle 12c	
Database	Database Compatibility Level	Standard: Highest level supported by SQL version. Lower versions with approval (see MS SQL Compatibility Level on EOL tab).	Standard: Critical DB will reside on their own DB server. Non-Critical and batch workloads will reside on consolidated DB servers.
Database	Database Features	Standard: SSRS, SSAS	
Database	Database Authentication	Kerberos, Local database authentication	
Database	Database Resources	Application databases co-exist in a shared database instance. CPU, memory, initial size, growth rate, and I/O requirements are needed for proper specification/design.	Standard: Critical DB will reside on their own DB server. Non-Critical and batch workloads will reside on consolidated DB servers.
Database	Data Purge	Data purge guidelines known and purge process defined.	
Database	ETL (Extract Transform and Load)	Standard: SQL Server 2012 or 2016, SSIS	
Database	Data Warehouse Tools	Standard: SSIS, SSRS, SSAS	
Database	Database Backups	Standard: SQL Server Backup, Oracle RMAN	
Segmentation	Security	Segment VLAN Traffic	
Reporting Tools	Dell OpenManage	SAN, Hypervisor, and environmental monitoring	
Reporting Tools	IPAM	SolarWinds IPAM	
Reporting Tools	Application, Server, and Network Monitoring	What's Up Gold / SolarWinds / Pingdom / vRealize / vSphere	
Reporting Tools	Web-based	Excel Services and SSRS Alternate Standard: Business Objects	
Type of Users	Users	Includes internal, contractor, CVTs, CLEMIS Agencies, RCOC, external, and public	
Application	SSL	Internal Sites: PKI External Sites (EV and Standard Certificates): Comodo Wildcard Cert: Entrust	Evolving security threats require up-to-date communication practices for secure encrypted connections between servers and clients. SSL certificates are one part of a secure environment.

Area	Function	Definition	Standard
Criticality	Business Application	Redundancy and resiliency is not required. Production is a standalone instance. Development and QA can be a shared instance and decided on an application by application basis.	No review required only if criteria is acceptable.
Criticality	Application Critical	Redundant application and database servers with the ability to a hot failover (taking less than 5 minutes, during business hours, to recover). QA needs to be sized in a manner that matches production (so that true testing can be replicated). Development must be able to run the application in a dynamic/fluid state.	Application review required.
Criticality	Mission Critical Application	Redundant application and database servers with the ability to a hot failover (taking less than 5 minutes, during business hours, to recover). QA needs to be sized in a manner that matches production (so that true testing can be replicated). Development must be able to run the application in a dynamic/fluid state.	Application review required.
Compliance Requirement	CJIS	Application must meet all CJIS compliance standards.	Add data must be encrypted in transit and at rest. Application review required.
Compliance Requirement	HIPPA	Application must meet all HIPPA compliance standards.	Add data must be encrypted in transit and at rest. Application review required.
Compliance Requirement	PCI	Application must meet all PCI compliance standards.	Add data must be encrypted in transit and at rest. Application review required.

Area	Function	Definition	Standard
Compliance Requirement	PII Data	Application must meet all PII data compliance standards.	Add data must be encrypted in transit and at rest. Application review required.
Compliance Requirement	Other	Other standards not covered above.	Add web traffic must be encrypted.
Compliance Requirement	None	Internal use or public data	No encryption required.
App Type	Cloud-Based	Application servers resides in the Cloud and application is browser based.	AWS or Azure
App Type	Thin Application	Application servers resides local on physical or virtual servers. Application is browser based.	Must support current bowsers.
App Type	Thick Client	Application requires installation on the client PC.	Review required.
Custom Programming	Application Code	Software that is specially developed for some specific organization, including COTS packages.	All components of the codebase must be current or n-1. Acceptable languages include .NET Framework, JDK, Java Script Libraries, Java Application Servers, etc.
Authentication / Authorization Method	Active Directory for a user store. SAML, Kerberos, and LDAP are the accepted protocols.	A method of confirming a person's identity.	Active Directory or SAML
Support	Current	OS or application currently supported by vendor.	Current is preferred; n-1 is acceptable.
Support	Extended Support	Extended support by vendor.	Review required.
Support	Extended Support - EOL next Master Plan	Support ending in next Master Plan.	Review required.
Support	Application Release (Age)		Current is preferred; n-1 is acceptable.

Application Protection	SaaS WAF	NGINX WAF	NetScaler w/ Platinum license
OCIT - AWS & SaaS	Preferred	Review required	
OCIT - On Premise and External (Public) Facing	Preferred	Acceptable	Review required
OCIT - On Premise and Internal Facing		Preferred	Review required
CLEMIS - AWS & SaaS	Preferred		
CLEMIS - On Premise and External (Public) Facing	Preferred		Acceptable
CLEMIS - On Premise and Internal Facing			Preferred

Data Classification

Sourced from Appendix A (page 210) of WISP

Classification	Data Classification Description	
Restricted	Definition	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	**SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to Oakland County. Impact could include negatively affecting Oakland County's competitive position, violating regulatory requirements, damaging the County's reputation, violating contractual requirements, and posing an identity theft risk.
Confidential	Definition	Confidential information is highly-valuable, sensitive business information and the level of protection is dictated internally by Oakland County
	Potential Impact of Loss	**MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to Oakland County. Impact could include negatively affecting Oakland County's competitive position, damaging the County's reputation, violating contractual requirements, and exposing the geographic location of individuals.
Internal Use	Definition	Internal Use information is information originated or owned by Oakland County, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the County's business interests.
	Potential Impact of Loss	**MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to Oakland County. Impact could include damaging the County's reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely sharable both internally and externally.
	Potential Impact of Loss	**NO DAMAGE** would occur if Public information were to become available to parties either internal or external to Oakland County. Impact would not be damaging or a risk to business operations.

Data Security

Sourced from Appendix A (page 212) of WISP

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-Oakland County employees	▪ NDA is recommended prior to access by non-Oakland County employees	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark **Open by Addressee Only** ▪ Use **Certified Mail** and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark **Open by Addressee Only** ▪ Use **Certified Mail** and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with County interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*
Web Sites	▪ Posting to intranet sites is prohibited, unless it is pre-approved to contain Restricted data ▪ Posting to Internet sites is prohibited, unless it is pre-approved to contain Restricted data	▪ Posting to publicly-accessible Internet sites is prohibited	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*
Telephone	▪ Confirm participants on the call line ▪ Ensure private location	▪ Confirm participants on the call line ▪ Ensure private location	*No special requirements*	*No special requirements*
Video / Web Conference Call	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line	*No special requirements*

Fax	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside County without manager approval	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside County without manager approval	*No special requirements*	*No special requirements*
Paper, Film/Video, Microfiche	▪ Return to owner for destruction ▪ Owner personally verifies destruction	▪ Shred or delete all documents or place in secure receptacle for future shredding	▪ Shred or delete all documents or place in secure receptacle for future shredding	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of County-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

Backup / Recovery / DR and Replication

Area	Function	Definition	Standard
Back-up/Recovery- Backup	Back-up/Recovery - Backup	The process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.	The back-up process must be to disk. This includes all servers used by the application (e.g., application, DB, Proxy, etc.)
Back-up/Recovery- Backup	Back-up/Recovery - SAN Replication and Replays	Real time replication between SANs.	All production workloads must be replicated to off side DR warm site.
Back-up/Recovery- Backup	DR Toolkits (Runbooks)	Step-by-Step documentation for manual recovery.	All production workloads must have a documented Runbook (DR Toolkit).

Area	Function	Standard
Hardware Type	Desktop	**See Service Center Handbook, Appendix B: Standard Software and Hardware Specifications.**
Hardware Type	Laptop	**See Service Center Handbook, Appendix B: Standard Software and Hardware Specifications.**
Hardware Type	Tablet	**See Service Center Handbook, Appendix B: Standard Software and Hardware Specifications.**
Hardware Type	Phone	iPhone SE (64GB) iPhone 6S (32GB)
OS Release	Operating System - Desktop/Laptop OS	**Windows 10; Optional with Architecture Approval: Windows 7 SP1. See Service Center Handbook, Appendix B: Standard Software and Hardware Specifications.**
Client Software	IE, Firefox, Adobe Acrobat, Mocha	**IE, Firefox; Optional with Architecture Approval: Chrome. See Service Center Handbook, Appendix B: Standard Software and Hardware Specifications.**
Knowledge Management	Collaboration	Office365 SharePoint online
Knowledge Management	Portal	SharePoint 2013 Public Sites in the Cloud Collaboration Sites in the Cloud
Local Security	Security	Non-administrative rights is the standard for Oakland County workstations.
Client Applications	Application Delivery	Thin Client is the preferred standard. If a Thick Client component is required, the standard Oakland County operating system must be used.

Area	Function	Definition	Standard
Application Updates	Business Continuity	OS and security patching	Monthly patching with SCCM
Disaster Recovery	Business Continuity	Dell Compellent SAN replication	Site to site replication for production workloads (SAN replication)
Disaster Recovery	Business Continuity	Dell DR600 Backups	Dell DR6000 backups replicated off site for Test and Development workloads
Reporting Tools	Application, Server, and Network Monitoring	Utilities used to monitor applications, networks, or servers	What's Up Gold / Solar Winds / Pingdom / vRealize / vSphere

Toolset	Standard	N-1 Standard	Unsupported / EOL	Notes
Windows Servers				
MS Windows Server	Server 2019 - Future Release **	Server 2016	2003 or older	** Release date expected Q1 2019
MS Windows Server - if Siteminder is required for Authorization	2008 R2			EOL - 1/2020
Linux Servers				
Red Hat Linux	Red Hat Linux 8 - Future Release **		Red Hat Linux 5	**Release date expected - Dec 2018
Oracle Linux	Oracle Linux 7.6 - Future Release **	Oracle Linux 7	Oracle Linux 5	**Release date expected - Q2 2019
SQL Server Database & Clients				
SQL Server	MS SQL 2019 - Future Release **	MS SQL 2017	MS SQL 2012 SP3 and older	**Release date expected - Q2 2019
Oracle				
Oracle	Oracle Linux 12.3 - Future Release **	Oracle 12.2	2005	** Release date expected 2019 Q1

Fault Tolerance

Business Application	Business Critical Application	Mission Critical Applications
Geo-Clustered	Geo-Clustered	Geo-Clustered
Multi-site Resilient	Multi-site Resilient	Multi-site Resilient
Fully Redundant @ one site	Fully Redundant @ one site	Fully Redundant @ one site
Single Points of Failure	Single Points of Failure	Single Points of Failure or Unknown

Legend	🟦
Preferred	🟩
Acceptable	🟨
Not Acceptable	🟥

Attribute	Definition
Geo-Clustered	High availability cluster systems reduce the possibility of single component failure. Geographically dispersed (or multi-site) cluster. In this configuration, the cluster nodes are separated geographically and quorum (shared) disk is synchronously mirrored between sites (using SAN or vSphere replication). The data disks can also be synchronously mirrored between sites. The cluster is unaware of the geographic distance between its nodes so this must be implemented at the network and storage levels within the infrastructure architecture.
Multi-site Resilient	A Production system designed to recover from a failure by detecting the failed component and restoring service with minimal downtime. This includes all VMware production servers. The system must have data replicated to two or more datacenters. Downtime will occur from a failure, but it is minimized.
Fully Redundant @ one site	Clustered system that resides only at one site. However, the cluster is still vulnerable as there is no protection from location disasters like fires, flood, or malicious damage.
Resilient	A Production system designed to recover from a failure by detecting the failed component and restoring service with minimal downtime. This includes all VMware servers (QA and Development).
Single Points of Failure or Unknown	A Production system with a design that includes one or more single points of failure.

Attribute	Definition
Mission Critical	Fully redundant hardware with load balancing across different locations; zero points of failure. QA needs to be a mirror of Production. Development needs to be robust but not a Production Mirror.
Business Critical Application	Redundant application and database servers with the ability to a hot failover (less than 5 minutes, during business hours, to recover). QA needs to be sized in a manner that matches Production (so that true testing can be replicated). Development must be able to run the application in a dynamic/fluid state.
Business Application	Redundancy and resiliency is not required. Production is a standalone instance. Development and QA can be a shared instance and decided on an application by application basis.

Server Releases (List Updated 5/15/2018)

Release	Release Date	Mainstream Support End Date	Extended Support End Date	Service Pack Support End Date	Notes
Windows Server 2003	5-Mar-2006	Ended	Ended	EOL	EOL
Windows Server 2008	22-Oct-2009	Ended	14-Jan-2020	9-Apr-2013	
Windows Server 2012	25-Nov-2013	9-Oct-2018	10-Jan-2023	N/A	
Windows Server 2016	15-Oct-2016	1-Nov-2022	11-Jan-2027	N/A	Excludes Nano Server
Windows Server 2019 - Future Release		TBD	TBD		Release date expected - Dec 2018
Red Hat Linux 5	15-Mar-2007	Ended	31-Mar-2020	N/A	Needs extended support contract.
Red Hat Linux 6	10-Nov-2010	30-Nov-2020	30-Nov-2023	N/A	Needs extended support contract.
Red Hat Linux 7	10-Jun-2014	30-Jun-2024	Ongoing	N/A	Needs extended support contract.
Red Hat Linux 8 - Future Release		TBD	TBD		Release date expected - Dec 2018
Oracle Linux 6	Feb-2011	Mar-2021	N/A	N/A	
Oracle Linux 7	Jul-2014	Jul-2024	N/A	N/A	

SQL Server Releases (List Updated 5/15/2018)

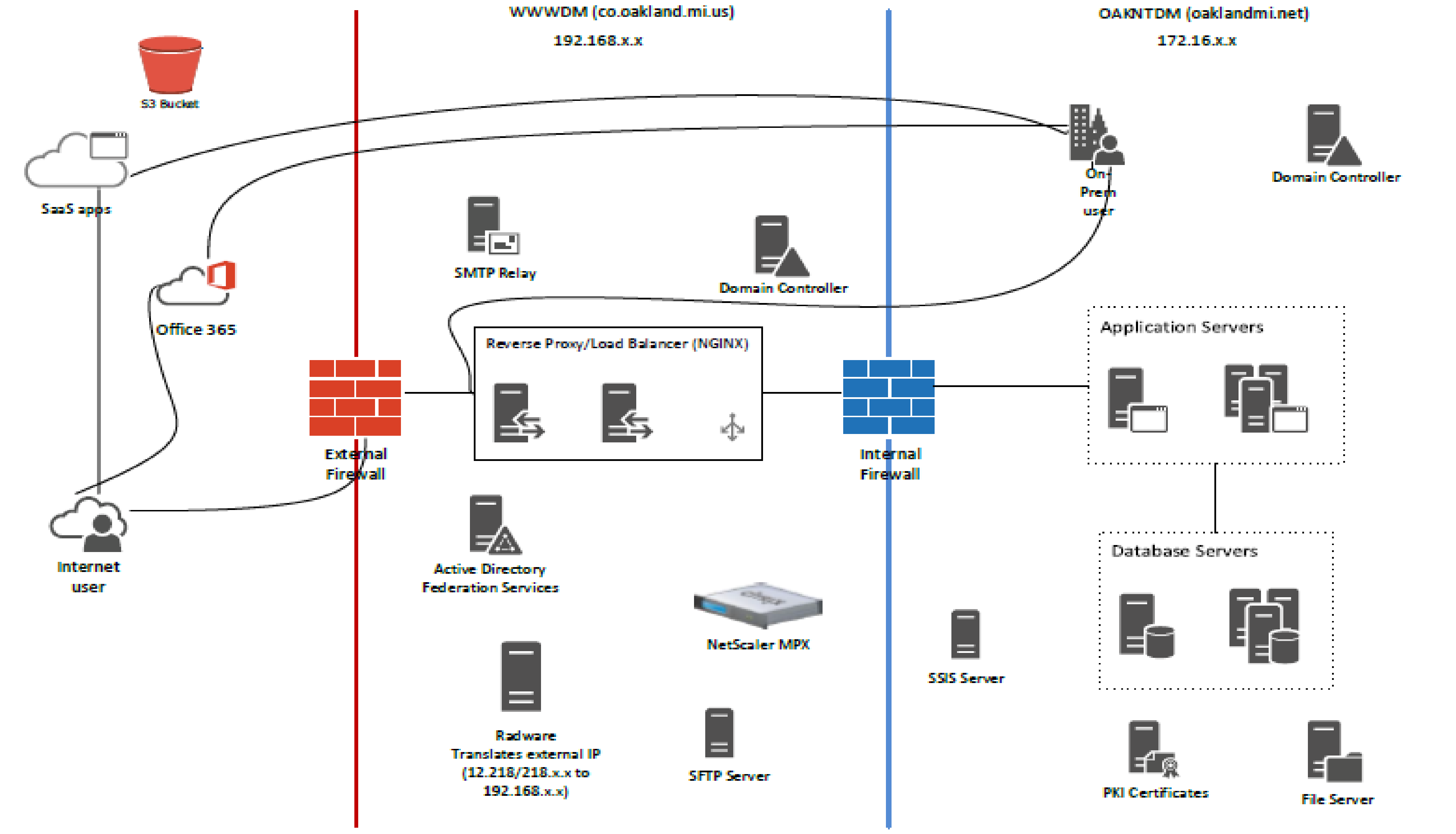
Release	Release Date	Mainstream Support End Date	Extended Support End Date	Service Pack Support End Date	Notes
Microsoft SQL Server 2005	14-Jan-2006	Ended	Ended	EOL	
Microsoft SQL Server 2008 Service Packs 1 - 3	6-Oct-2011	Ended	Ended	EOL	
Microsoft SQL Server 2008 Service Pack 4	30-Sep-2014	Ended	Ended	9-Jul-2019	See Microsoft Service Pack Policy footnote
Microsoft SQL Server 2008 R2 Service Packs 1 - 2	26-Jul-2012	Ended	Ended	EOL	
Microsoft SQL Server 2008 R2 Service Pack 3	26-Sep-2014	8-Jul-2014	9-Jul-2019	Review Note	See Microsoft Service Pack Policy footnote
Microsoft SQL Server 2012 Service Packs 1 - 2	10-Jun-2014	Ended	Ended	EOL	
Microsoft SQL Server 2012 Service Pack 3	1-Dec-2015	Ended	Ended	9-Oct-2018	See Microsoft Service Pack Policy footnote
Microsoft SQL Server 2012 Service Pack 4	1-Dec-2015	Ended	12-Jul-2022	Review Note	See Microsoft Service Pack Policy footnote
Microsoft SQL Server 2016 Service Pack 1	16-Nov-2016	13-Jul-2021	14-Jul-2026	TBD	See Microsoft Service Pack Policy footnote
Microsoft SQL Server 2017	29-Sep-2017	Review Note	12-Oct-2027	TBD	See Microsoft Service Pack Policy footnote

Footnote: Microsoft Policy on Service Pack Releases

Support ends 12 months after the next Service Pack releases or at the end of the product's support lifecycle, whichever comes first. For more information, see the Service Pack Policy at gp_lifecycle_servicepacksupport.

Microsoft SQL servers include both Standard and Enterprise editions

Example Diagram



- All web traffic is https
- Application Server to Database server traffic is TCP
- Application servers bound with OC PKI certificates
- NGINX/Netscaler and reverse proxy servers are bound with COMODO certificates
- g2gcloud.com sites use the wildcard certificate issued by Entrust

11/9/2016

Oakland County Michigan
Technical Design Review
Document Version Date: 6/20/2018

Example Overview	**Below is an example of the completed Overview Tab.**
Project ID & Name:	Enter the project ID and Name Here
Project Description:	Enter the project description here (e.g. Copy and paste Project Description from Clarity if available).

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Environment						
Infrastructure	Describe the type of infrastructure being proposed (Cloud, Virtual On-Premise, Physical Hardware or Hybrid). Provide the server specifications if the proposed solution is non-Cloud.	Cloud	Virtual On-Premise (VMware)	Physical Hardware	On-Premise VMware; Vendor can run on VMware 5.5 or newer	
Network Transport - Connection Type	Describe the Network Connection bandwidth for servers and workstations required for your solution (e.g., 100MB, 1GB or 10GB). Describe if there are any special network requirements for the solution (e.g., Latency, Jitter, etc.)	Required Network Connection Bandwidth: **Server**: 1GB or less **Workstations**: 100MB or Less	Required Network Connection Bandwidth: **Server**: Greater than 1GB but less than 10GB **Workstations**: 100MB to 1GB	Required Network Connection Bandwidth: **Server**: 10GB or greater **Workstations:** 1GB or greater	Web Browser Connection - less than 100 MB Server 1 GB or less needed	

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Network Transport - Server Location	Provide connection diagram that shows the specifications for each connection that includes the source and destination for those connections. The specification will include server location (e.g., Internal network, DMZ network, etc.) with port and protocol in use for the connection.	Load balancer(s) and/or Web/Frontend servers in DMZ; other backend servers in Internal network	Single standalone servers in DMZ or Internal network	Specialized networking requirements or network segmentation	Load Balancers required Application in Three-Tier Structure	
Network Transport - Application Behavior	Describe the testing that is performed with your solution for firewalls, intrusion protection systems, or other security systems.	The solution is fully tested against stateful inspection or next generation firewalls and intrusion protection systems	The solution is not tested against stateful inspection or next generation firewalls and intrusion protection systems	Known issues working with stateful inspection or next generation firewalls and intrusion protection systems.	No reported issues with firewalls or security appliances over port 80 or 443	
Network Transport - Access Layer Changes	Describe any required changes in the access layer of network transport (additional vLAN's, new isolated network, redesign or rework of existing network, etc.)	No Change	Capacity, Mandated or Public Safety	Change required, not related to Capacity, Mandate or Public Safety	No Changes required	
Wireless Services	Describe the wireless services this solution utilizes and the encryption method(s) for transmission.	The solution is NOT planning on leveraging wireless services	The solution is planning on leveraging wireless services with encryption technologies	The solution is planning on leveraging wireless services without encryption technologies	No wireless solution is required	
Operating System (OS)	Describe the Operating System(s) (OS) and OS release(s) on which your solution/product can run.	Windows 2012; Red Hat Linux; Oracle Linux	Supported versions of Windows or Linux Red Hat and Oracle	End of Life (EOL) OS releases or non-standard OS	Windows 2008	
Antivirus/Malware	Describe the Antivirus/Malware solution(s) with which your solution/product will function.	Utilizes currently defined standards	Utilizes a non-standard Antivirus and/or Malware	Does not work with Antivirus and/or Malware	Application will run with any anti-virus software	

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Database (DB)	Describe the database(s) and DB release(s) with which your solution/product will operate.	MS SQL 2012 or greater	Oracle 12C or greater	Other DB	MS SQL 2008	
Reporting Tools	Describe the reporting packages that are included with your solution/product.	SSRS (SQL Server Reporting Services)	Business Objects	Other	Reports are exported in standard Excel format	
Type of User	Describe if the users are internal and/or external and how they are defined.	Users defined by Role	Users defined by AD Groups	Users not defined or solution utilizes internal user store within the application	Application will require two levels of access: Admin and Web User (defined as roles using Active Directory groups)	
Number of Users	Describe the number of users to the system by **Type of User**.	Number of users	Not applicable	Number of users unknown	300 External Web Users 3200 Internal Web Users 15 Internal Admin Users	
Application						
Criticality	Describe if the application is **Business**, **Business Critical**, or **Mission Critical**.	Business application	Business Critical application	Mission Critical application	Business application	
Compliance	Describe the legal standards with which your solution complies (e.g., HIPAA, PCI, CJIS, SOC 2, etc.).	No compliance requirement	Compliance requirement is unknown	Compliance required (e.g., HIPAA, PCI, CJIS, PII, SOC 2, etc.)	Application contains public data only	
Application Type	Describe the application type (e.g., SaaS, web application, thick client, etc.).	SaaS (Software as a Service) application	Web application	Thick application	Web application	
Custom Programming	If custom programming is needed, describe the language(s) used.	.Net or Python	Not applicable	Java or other	N/A	
Abridged ADA Compliance - WCAG 2.0	Does the application meet Americans with Disability Act (ADA) requirements	Meets ADA requirements	Not applicable	Non Compliant	Compliant with ADA	

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Unabridged ADA Compliance - WCAG 2.0	(ADA) requirements.					
Application Protection - Web Application Firewall (WAF)	Does the application meet requirements.	Preferred	Acceptable	Review required	WAF Not required for the application	
Authentication / Authorization Method	Describe the type of Authentication method that is utilized (e.g., Microsoft AD, LDAP, SAML, etc.).	Active Directory for a user store; SAML, Kerberos, and LDAP are the accepted protocols	NT LAN Manager (NTLM) Authorization	Authorization and/or user store built into the application	No Authentication and no User Store required	
Data						
Data Classification	Describe the data type to be stored in this system (Public, Internal Use Only, Confidential Data, Restricted Data (HIPAA, PCI, CJIS, or PII) or Unknown).	Public or Internal Use data	Confidential data	Restricted data: (HIPAA, PCI, CJIS, or PII) or Unknown	Public data	
Data Security	Describe what encryption is to be used, and in what form (at rest, in transit, or both).	Data is encrypted in transit and at rest via Certificate (required for restricted data) No encryption required (acceptable for Public or Internal Use)	Data is encrypted in transit with Certificate (required for confidential data)	Unknown	Encrypted in transit (in motion) using Certificates	
Backup and Recovery	Describe the method for backup and recovery (Cloud, Disk to Disk, Disk to Tape, etc.) Describe who is responsible for the backup and recovery.	SAN Replication and Disk to Disk	Disk to Tape	Unknown or no backup	Disk to Disk - As provided by Oakland County	

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO)	Describe your standard Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the solution.	Meets or exceeds Oakland County RTO/RPO	Relies on Oakland County for RTO/RPO	Does not meet Oakland County RTO/RPO	RTO - 16 hours RPO- Last Transaction	
Retention and Purge	Describe the data retention and purge needs of your solution.	Defined requirements and purge criteria	Not Applicable	Criteria is not defined	Data is live and purged from the DB after 7 days	
Client						
Network Transport - Workstation Location(s)	Describe your Client connections (LAN, WAN, or Internet based). If peer to peer connections are required, explain why.	All Client connections are from existing local area or wide area network	Unknown client requirements	Peer to peer connectivity or new VLAN required	All client connection are from local area network	
Internet Browser	Describe the browser(s) and version(s) you support.	IE, Firefox, Chrome External	Chrome Internal	Other	IE, FF, Chrome - Supported by all HTML 5 Browsers	
Client (Workstation) Hardware / Software	Describe the workstation requirements including Operating System, hardware requirements and any additional software required.	Windows 10	Windows 7	Other OS	Windows 10, Windows 7, MAC - all supported	
Local Workstation Security	Describe the workstation security requirements for your solution.	No administrative rights required	Elevated rights required	Local administrative rights required	No Administrative Rights required	
Maintenance						
Application updates	Describe your release and patch cycles.	Defined release and patch cycle(s)	Not Applicable	No release and/or patch cycles defined	Application Patched Quarterly	
Disaster Recovery	Describe monitoring and alerting options provided by your solution.	Fully Redundant	Resilient	Single Points of Failure	Resilient	
Fault Tolerance	Describe your release and patch cycle.	Meets Fault Tolerance Standard	Meets a mid-level Fault Tolerance	Does not meet minimum defined standard for Fault Tolerance	Business application - VMware resilient, meets fault tolerance standard	

Criteria	Information Requested	Good	Acceptable	Review Required	Response	Notes
Monitoring and Alerting	Describe monitoring and alerting options provided by your solution.	Defined monitoring and alerting	Not Applicable	No monitoring and/or alerting defined	Monitored using Pingdom	