

Appendix 3F(vi)

VIHA IMIT Technologies Standards

INTENT OF THIS DOCUMENT

This document describes the standard technologies supported by VIHA IM/IT. The text may be used for reference in Requests for Proposal (RFPs). The document should be maintained as a whole if inserted into another document.

This is a living document, refreshed biannually. The most recently published version will be found at https://intranet.viha.ca/departments/imit/Pages/standards_guidelines.aspx.

AUTHENTICATION, ACCESS AND PRIVACY

Authentication & Access

- Microsoft Active Directory Win 2003 Native Mode; moving to Windows 2008 Native Forest and Domain Functional mode by end of 2012
- Microsoft ADAM, or LDAP (as required by application); Secure LDAP required for authentication
- Microsoft Identity Integration Server (MIIS) (limited support)
- Microsoft Internet Security & Acceleration Server (ISA) 2006 moving to UAG2010
- Single Sign-On using Citrix Password Manager
- RDP and Citrix Client through Web Interface for remote access
- SSL-VPN client (VIHA-owned laptops & tablets only)
- Remote access to desktops or laptops not supported
- Preference for SPMLv2 – compliant applications

Certificate Services

- PKI through MS Certificate Authority (Windows Server 2003 R2) using custom v2 certificate templates

Privacy and Security Standards

- Refer to the following IMIT Policies:
 - the Authority's Security of Electronic Information Policy No. 16.4.2.1, dated October 2006;
 - the Authority's Security of Health Records Policy No. 1.6.4.2.2, dated November 2006;
 - the Authority's Acceptable Use of Assets and Resources Policy No. 16.4.2.3, dated February 15, 2008;
 - the Authority's Remote Access Policy No. 16.4.2.4, dated February 15, 2008;
 - the Authority's Mobile Computing Policy No. 16.4.2.5, dated February 15, 2008; and
 - the Authority's Remote Assistance and Session Sharing for Support Purposes Policy No. 16.4.2.6, dated February 15, 2011

CLIENT DEVICES

Desktops

- Standardized, organization wide HP and Lenovo desktops & Laptops

- Images custom designed for individual hardware configurations
 - Configurations are reviewed and updated on a regular basis
 - Screen standard of 1024 x 768
 - Preferences for all local devices is USB – serial not always natively available

Legacy Devices

Config	Monitor	Processor		Memory	Hard drive
Desktop CMT	19"	Core 2 Duo E6850	3.0 ghz	4 gb	80 gb
Desktop SFF	19"	Core 2 Duo E6550	2.33 ghz	2 gb	80 gb
Desktop USD	19"	Core 2 Duo E6550	2.33 ghz	2 gb	80 gb
Laptop A	14.1"	Core 2 Duo T8300	2.4 ghz	2 gb	120 gb
Laptop B	15.4"	Core 2 Duo T9300	2.5 ghz	2 gb	120 gb
Tablet	12.1"	Core 2 Duo L7700	1.8 ghz	2 gb	120 gb

New Devices

Config	Monitor	Processor		Memory	Hard drive
Desktop - ultra slim	22"	i5 - 2400		4 gb	250 gb
Desktop - small form	22"	i5 - 2400		4 gb	250 gb
Desktop - tower	22"	i5 - 2400		4 gb	250 gb
Laptop	12"	i5 2520m		4 gb	160 gb
Laptop	14"	i5 2520m		4 gb	160 gb
Laptop	15"	i5 2520m		4 gb	160 gb
Tablet	12.5"	i5 2520m		4 gb	160 gb

Standardized Workstation Software Environment (desktop & laptop/tablet)

- Windows XP SP3
- Microsoft Office 2007
- IE 7
- Citrix Client 11
- RDP Client 6.0
- Cisco VPN client (tablets only)
- Adobe Reader 10.1
- Pathworks VT320
- Macromedia Flash Player 10.2
- Macromedia Shockwave 10
- Windows short-date format: DD-MMM-YYYY
- PointSec Hardware Encryption on laptops and tablets
- McAfee VirusScan Enterprise Version: 8.7.0i
- Group-policy managed desktop settings

Within the year VIHA will be updating this configuration for new installs to

- Windows 7 SP 1
- Microsoft Office 2010 Professional
- IE 9
- Other software updates TBD

License Management

- VIHA prefers the use of server-based license management systems wherever possible, (e.g. licensing servers and services based on the FLEXLM licensing model (Citrix, VMWare and AutoDesk) or MS KVM licensing).
- Licensing control mechanisms should avoid technologies which tie usage to specific workstations.
- Licensing control mechanisms should be compatible with Thin Client, Citrix, Microsoft Application Virtualization (App-V), and Web-based access methods.
- Licensing control mechanisms should be automated and require no administrative intervention for license release.
- Concurrent licensing models are generally preferred, due to the shift- and shared-resource nature of our staff's roles.
- Per-user licensing models are generally preferred to per-workstation licensing models
- Licensing control mechanisms should not require ongoing communication with sites external to VIHA after installation

Mobile Devices

- Mobile devices must adhere to the Authority's Mobile Computing Policy No. 16.4.2.5, dated February 15, 2008;
- Blackberry OS 4.1 and higher
- Support of the following BB devices in VIHA: 8330/8530/9300/9360 Curves, 9800/9810 Torch, 9700/9780 Bold
- Ordering of cell phones and air card
- All new devices must be pre-approved prior to being added to the Enterprise servers

Deployment & Support Tools

Microsoft Systems Center Configuration Manager:

- Microsoft Updates deployment and management
- Core Software updates and large scale software package distributions
- Support Desk remote support
- Device Inventory

Altiris Deployment Solution:

- Standardized Operating system image and post configuration deployment for workstations, Notebooks and servers.
- Software deployment at initial workstation and server deployment.

Microsoft Systems Center Configuration Manager (HealthBC domain):

- Packages created for widespread distribution
 - must be created according to the standards developed in conjunction with HSSBC
 - must be MSI-based
 - must not include dependencies as part of a monolithic package
 - must not include Custom Actions in the MSI

SERVERS AND STORAGE

Servers:

- Preference for Virtualized Servers running on VMware ESX 4.1
- Where physical server is required, standardized HP Servers;

HP Server	Processor	Default Memory	O/S Hard Disk	Default HD Data Storage
BL460-G7 Blade	Intel 64bit	4gb	2 x 146gb	na
DL380-G7	Intel 64bit	4gb	2 x 146gb	upto 6 drives
DL360-G7	Intel 64bit	4gb	2 x 146gb	upto 2 drives
DL580-G7	Intel 64bit	16gb	2 x 146gb	upto 14 drives
Memory and HD data storage may be adjusted as required				

- Standard O/S software and utilities;
 - Windows 2008 R2 Standard or Enterprise Server (x64 preferred)
 - Windows 2008 Standard or Enterprise Server (x64 preferred)
 - Windows 2003 R2 Standard or Enterprise Server (x64 preferred) only to support legacy applications
 - NetBackup 7.0
 - McAfee 4.5 EPO
 - McAfee Antivirus Agent 8.7
 - Diskeeper v2010
 - VMware ESX Virtualization (VI 4.1)
 - MS SCOM 2007 R2
 - Console support via ILO, Terminal Services and Citrix
- All servers must be supportable in a lights-out facility

Enterprise Systems

- VIHA back end systems consist of HP servers of a variety of models and operating systems. For example, we currently have in production:
 - Legacy Cluster with two AlphaServer ES47's running OpenVMS 7.3-2 with the following add-on products:
 - Diskeeper for automated disk defragmentation
 - Hitman for automated system monitoring (ie low disk alerts)
 - ECP for performance monitoring
 - ABS for system backups
 - Multinet for TCP/IP networking
 - Integrated Clinicals (ICS) consisting of HP Service Guard Clusters running HP-UX on HP Integrity servers. In production there will be two HP AlphaServer rx8640's running HP-UX 11.31 with the following add-on products:
 - Serviceguard clustering
 - MirrorDisk/UX
 - HP GlancePlus/UX

- Netbackup
- All systems are fibre connected via HP Director class SAN switches to HP and EMC SAN storage:
 - Tier 2 Storage (standard for clusters) on EVA 5000 @ 2Gbps or EVA 6000 @ 2 Gbps providing FC storage
 - Tier 2 Storage (standard for clusters) on NS480 @ 4Gbps providing both FC and NAS storage
 - Tier 1 Storage (mission critical, high I/O) on XP24000 @ 4Gbps

Enterprise Server Models

- HP Integrity rx8640 Server * 4
- AlphaServer GS1280 * 2 (retired)
- AlphaServer GS160 * 2 (retired)
- AlphaServer ES47 * 2
- AlphaServer ES40 * 2
- AlphaServer DS20E * 2

Enterprise Storage

- HP StorageWorks XP24000 Disk Array * 2
- HP StorageWorks EVA6000 Disk Array * 2
- HP StorageWorks EVA5000 Disk Array * 3
- HP StorageWorks 4/256 SAN Director Switch * 4
- HP MSL6062 4 Drive LTO-4 Ultrium 1840 Tape Library * 4
- HP MSL6000 2 Drive SDLT2 Tape Library * 1
- HP MLS5052 2 Drive SDLT Tape Library * 2

IM/IT SERVICES

Collaboration and Web Services

- WS28R2 64-bit OS only
- IIS 7.5 running 32-bit application pools standard, 64-bit pools supported; Integrated Mode pools by default. Classic mode by exception
- .NET 2.0, 3.0, 3.5, 4.0 are supported. ASP is supported by exception.
- Application delivery is through a combination of Cisco ACE load balancing, Microsoft Application Request Routing, and load-balanced web farm.
- No vendor access to web servers
- Web apps are hosted under apps.viha.ca URL by default but don't necessarily have to reside on the same farm. Exceptions can be granted for security reasons.
- SSL is required; Port 80 connections are not supported
- NTLM authentication is standard; forms-based authentication under special circumstances;
- Basic and Digest authentication not supported
- Native support of MS SQL
- Microsoft SharePoint 2007. SharePoint 2010 will be available mid-2012. The following service applications are not currently available:
 - SSRS
 - Access Services
 - Business Intelligence

- My Sites
- SharePoint solutions must be delivered as WSP solutions. No GAC or manual installs permitted if there are non-Designer changes.
- SharePoint Designer 2007 is available to vendors under special circumstances. It is not available to VIHA users. SharePoint Designer 2010 will be available to clients for SharePoint 2010 but use will be limited to non-look and feel functions.
- InfoPath 2007 is available.
- Some websites and SharePoint sites are available externally via ISA NTLM authentication. All others are only available externally via Citrix.

Printers

- Business (and some clinical) application printing for Windows is available to a variety of HP laser printers via server-based print queues hosted on a Windows 2008 R2 Active-Passive print cluster.
- Cerner-based clinical application printing for Windows is available to a variety of HP laser printers via server-based print queues hosted on a Windows 2003 R2 Active-Passive print cluster.
- HP/UX printing to certain devices is available through managed HP/UX server print queues used for printing clinical data direct from HP/UX applications.
- The list of currently supported HP print and MFP devices is as follows:
 - HP LaserJet P3015x
 - HP LaserJet P4015x
 - HP LaserJet 9050dn
 - HP Color LaserJet CP3525x
 - HP Color LaserJet CP4525dn
 - HP Color LaserJet CP6015x
 - HP LaserJet M3035xs mfp
 - HP LaserJet M5035xs mfp
 - HP LaserJet M4345x mfp
 - HP LaserJet M4345xs mfp
 - HP LaserJet M9050mfp
 - HP Color LaserJet CM3530fs mfp
 - HP Color LaserJet CM4730fsk mfp
 - HP Color LaserJet CM6040f mfp

Network

- There are approximately 175 sites connected to the VIHA network.
- The medium to larger sites are typically connected via Telus Metro WAN services at bandwidths of either 1.5, 10, 100 or 1000 Mbps.
- The smaller sites are typically connected via hardware VPN services using broadband ISP services.
- The LAN infrastructure is typically configured with either 1 or 10 Gbps backbones and 10/100 Mbps access ports.
- A wireless LAN infrastructure has been deployed at some of the medium to larger sites, supporting the 802.11a/b/g protocols.
- Approximately 15,000 devices are connected to the VIHA network. Connected devices include desktops, laptops, printers, MFPs, auto-analyzers, CTs, MRIs, videoconferencing systems, VoIP phones and related infrastructure, voicemail systems, card access systems, building management systems, various alarms systems and a variety of others.

- The network infrastructure is constructed using a variety of Cisco products, including Cisco switches, routers, firewalls, VPN concentrators, VoIP Call Managers, WLAN controllers, wireless access points, network authentication servers, etc.
- The network infrastructure is QoS (Quality of Service) aware, with marking and queuing based on pre-defined types of application traffic.
- The network is configured with multiple VLANs, with assignment of specific devices or applications to certain VLANs based on either QoS or security considerations.
- The network infrastructure supports only one device (MAC address) per access port
- The network infrastructure provides for routed TCP/IP communications between devices.

Wireless LAN

- The VIHA wireless LAN infrastructure has been deployed at a number of medium to large sites.
- The WLAN infrastructure uses Cisco WLCs (Wireless LAN Controllers), LWAPs (Lightweight Access Points) and WCS (Wireless Control System).
- The WLAN supports all of the 802.11 a/b/g protocols.
- The infrastructure is configured with multiple WLANS used to support a variety of computing and communications devices

APPLICATION MANAGEMENT SERVICES

- Application standards, support and development
- Database standards, support and development
- Interface standards, support and development
- System to System and System to Device integration standards and solutions
- Process automation solutions
- Process/System monitoring and alerting solutions
- Reporting standards, support and development
- Data Management – Extract, transform, load, aggregation, cleansing, data quality checks
- Information delivery systems support and development
- Change Management Services
- Solution Development Lifecycle Services
- Configuration Management Services
- Release Management Services
- Problem Management Services
- Enterprise Architecture Services

APPLICATION MANAGEMENT SERVICES SUPPORTED CONFIGURATIONS

Integration and Interfaces

- Interface Engines Supported:
 - Cloverleaf Interface
 - Sybase eBiz
 - Cerner OpenPort
- Messaging Standards Supported:
 - HL7 v. 2.2 to 2.5

- ADT
 - Orders
 - Results
- Transport Protocols Supported:
 - FTP
 - TCP/IP
 - HTTPS
- Integration Standards Supported:
 - CCOW (note: VIHA does not have a CCOW server)
 - SALM

Database Environments

- Oracle Version 10g
- Microsoft SQL Server 2000 and 2005 SP1

Reporting Tools

- Microsoft Reporting Services (SQL) 2005
- Crystal Reports Version XI
- Cognos Version 8.

Main application environments

- Clinical – Cerner Millennium (Cerner Corporation) and PARIS Community Care System (In4Tek Corp)
- Business – MediTech (Medical Information Technology, Inc.), ESP (Kronos Corporation)

Development Languages Supported:

- Microsoft .Net
- Perl
- Java

Service Levels

- Platinum Service – 100% business hours uptime 7X24 support including service request facilitation
 - Fully redundant production environment with no single points of failure in the architecture and/or downtime/failover capabilities allowing for continued automation of workflows with minimal manual intervention required to recover the system and system data.
 - Platinum service not available where solution architecture/technology prevents achievement of 100% uptime target.
 - Separate production, test and development environments
- Gold Service – 99.94% business hours uptime target, 7X24 break/fix support, client business hour service request facilitation
 - Architecture appropriate to uptime target (4 hours of planned downtime per month for 7X24 systems)
 - Separate test environment that duplicates core production architecture
 - Separate development environment if VIHA responsible for development

- Silver Service – 99.94% client business hours uptime target, client business hours break/fix support, IMIT business hours service request facilitation (24x5 M-F excluding statutory holidays)
 - Architecture appropriate to uptime target. 4 hours of planned downtime per month for 7X24 systems.
- Bronze Service – 99.94% regular business hours uptime target (M-F 8am-5pm), regular business hour break/fix and service request support. 4 hours of planned downtime per month for 7X24 systems.

General Standards in Scope for all Solutions:

- Application Services – runnable under OS system account
- Monitoring – all production components hardware/software monitored and alerted on. Response appropriate to Service level.
- Security – systems must have the capability to capture/audit end user interaction with the system.
- Systems need to have multi-factor authentication consisting of a minimum a username and strong password as per the VIHA strong password guidelines.
- Privacy – access to system information needs to be configurable/lockable such that end user access/views of the information comply with VIHA privacy regulations.
- Security and Privacy – Foreign systems receiving/processing information originating from the VIHA enterprise systems must support the same level of information security and privacy as applied to the information in the source system.
- Web, 3 tier, service oriented architectures are desirable for ease of deployment and management. Ability to run under Citrix is preferred.
- Documentation – architecture is fully documented
- Compliance with all IMIT Policies.