Infrastructure Standards

Version 5.0 – April 2016

Version	5.0
TRIM file number	-
Short description	This document provides a list of the infrastructure standards to be applied in the purchase, management and use of technologies and infrastructure that underpins organisational applications and services. The standards do not describe what is currently supported in the CSU environment but rather the minimum versions and technologies that a new technology must interoperate with at the current point in time. This document where relevant links to Technical Specification documents which provide more detail as well as specific work instructions related to the application of these standards at the University.
Relevant to	Officers who have a responsibility in the planning, selection, procurement and implementation of infrastructure components and to prospective and present CSU infrastructure suppliers.
Authority	
Responsible officer	Enterprise Architect, Infrastructure
Responsible office	Enterprise Architecture Division of Information Technology
Date introduced	June 2011
Date(s) modified	March 2012 December 2014 April 2016
Next scheduled review date	April 2017
Related University documents	CSU Enterprise Architecture Principles CSU Data Standards CSU Application Standards CSU Communications Specification CSU AV and Video Conference Specification
Related legislation	
Key words	infrastructure, principles, standards, applications architecture, server, network, desktop, database, hardware, software, authentication

Environments

- Applications which require in-house developed enhancements have a development, QA and Production environment for the relevant components.
- Applications not requiring development should at a minimum have a “Build and Test” and Production Environment.

Remote Management

CSU defines “remote management” as systems that are managed or directly supported by connection to server(s) from outside the University’s network by people other than CSU staff.

Remote management will connect via one or more of the following mechanisms:

- RDP – Remote Desktop Protocol via Terminal Services 2008 Gateway
- SSH2
- Access to secured network segments VPN via Cisco client.

Server Operating Systems

- Red Hat Enterprise Linux (RHEL) 6.x *(7.x Preferred)*
  - NTP
  - Iptables
  - Linux Native Multipathing
  - TCPWrappers
  - SHA-256 Password encryption
  - NIC Bonding

- Windows Server 2012 R2
  - Windows multipathing
  - Windows Firewall – enabled
  - Operating systems will ideally be run in a Virtual Server environment

Server Configuration management

- Puppet Enterprise for UNIX
  - All UNIX systems have a baseline Puppet configuration applied
  - Puppet configuration management for managed UNIX systems
- SCCM 2012 for Windows 2012

Server Hardware

- Cisco UCS 6248 and B200 M3 blades
- Dual Network Interface Cards

Virtualisation

- VMWare Vsphere 6.0.x
- VMWare vCenter Server 6.0.x
- VMWare Site Recovery Manager 6.0.x

Database

- Database - Oracle 11g or 12c on Linux
- Mission critical Databases require ability to support:
  - Database replication - Oracle Data-Guard
  - Database Backup – Oracle Recovery Manager
  - Server redundancy - Real Application Cluster (RAC)
- Database – MySQL on Linux
- Database - Microsoft SQLServer 2012 R2
- Mission critical Databases require ability to support:
  - SQLServer Mirroring

Web and Application Server

- Apache web server 2.x on RHEL *(distro supplied Version)*
- IIS 7.5 on Windows Server 2012 R2
- Tomcat Application Server V7.x on RHEL
- Oracle Web Logic 11g
- Oracle Grid Control 12c

Business Continuity

- Databases must be able to be facilitate a replicated copy at a geographically separate location.
- Solutions should support cross-campus server clusters

Architecture

- The Web, Application and Database components of an application must have the ability to be separated to allow horizontal scaling (utilizing load-balanced pools) of the separate tiers.
- The application should not require system administrator or super-user account privileges to run.

Authentication

- Applications and services not hosted on CSU infrastructure:
    - No CSU-issued authentication credentials are to be entered on applications hosted on non-CSU infrastructure.
    - CSU applications hosted on External infrastructure should use federated idP services provided
        - Shibboleth 2.x
        - SAML 2.x
- Applications and services hosted on CSU infrastructure:
    - SAML 2.x authentication via Shibboleth *(either via mod_shib or within application)*
    - LDAP Compliant
    - NTLM
    - RADIUS
    - Winbind *(local unix authentication only)*

Mail Delivery System

- Unix - sendmail
- Windows – Microsoft Exchange

Storage

- SAN - Netapp FAS8040
- NAS - Netapp FAS8040
- Data ONTAP 8.3P2 clusters
- NAS/SAN replication – SnapMirror
- Disk – 900GB 10K SAS, 4TB 7.2K NL-SAS, SSD

Backup

- Netapp Altavault AVA400 / v4.1.1
- Backup Software
    - Commvault Simpana v10r2 sp12
    - NetApp SnapProtect v10r2 sp11
- Short term backups:
    - SnapProtect - snapshots + snapvault
    - Commvault - Simpana Media Agents
- Long term backups:
    - Netapp Altavault - Cloud backups
    - Tape *(legacy only)*

Fibre Channel Network

- MDS-9148 FC switches
- NX-OS 6.2

Application delivery controller

- Citrix Netscaler load balancers
- Configuration deployed via Puppet
- SSL offload using CSU wildcard or nominated certificate

SSL Certificates

- Access to unlimited number of regular SSL certificates via AusCERT Certificate Services *(allocated via ICS-INF team)*
- CSU Wildcard certificate only available for internally hosted systems via Netscaler load balancer

Network

The requirement for networking at CSU encompasses both the set of standards below as well as the Communications Standard document.

- Ethernet Cabling to desktop (Cat 6)
- IPv4 and IPV6
- 1 Gb to desktop standard(IEEE802.3u)
- 10 Gb fibre channel between centres
- Cisco 3850 series of switches
- Cisco 6800 routers
- Cisco 3750 (layer3) routers
- Cisco IOS 12.2.52
- VPN Cisco ASA5550 and Cisco VPN client
- Security – ACL's
- Power Over Ethernet (POE)
- 802..11AC Wave 2 wireless connectivity (2.4 and 5 GHz)
- Cisco 8300 series Access Points

Desktop

- Windows 7 SP1 64-bit
- Mac OS X 10.11.x
- Microsoft Office 2013
- Internet Explorer 11
- SCCM 2012 R2
- Skype for Business 2013
- Microsoft App-V 4.6.3
- Java 8.66
- Flash 19.x
- Adobe Reader 11.x

Telephony

- VOIP
- Polycom IP 335 & IP 560 (desktop)
- Polycom IP 6000 (conference)
- Standard SIP based (session initiated protocol)

Video Conference

- H.323, SIP, WebRTC and Microsoft Lync
- Video Codecs H.264 SVC (UCIF Profiles 0, 1), H.263, VP8, RTV (licensed from Microsoft®), RDP
- Audio Codecs G.711(a/μ), G.722, G.722.1 (licensed from Polycom®), Siren14™ (licensed from Polycom®), G.722.1C (licensed from Polycom®), G.729, G.729A, G.729B, Opus, MPEG-4 AAC-LD (MPEG-4 video technology licensed by Fraunhofer IIS).
- Content Sharing H.239 (for H.323), BFCP (for SIP), RDP (for Microsoft Lync), VP8 (for WebRTC high framerate), JPG (for apps and web).
- Resolutions from QCIF to 1080p (1920 x 1080)*, 4:3 and 16:9 aspect ratios.
- Bandwidth - Connections from 8 kbps per participant (G.729, audio-only), up to 6 Mbps per participant.
- Support for AES (128-bit key size) and DTLS SRTP encryption
- RTMP Outbound Streaming
- Pexip Infinity Conferencing Platform
  - PexIP Infinity Management Node
  - PexIP Infinity Conference Nodes
  - Infinity Reverse Proxy
  - Covene Cohesion Scheduling
- Polycom DMA Gatekeeper
- Polycom RMA Endpoint Management Platform
- Polycom Capture Server
- Polycom Access Director Firewall Traversal
- Platform Director (Polycom Licensing)
- Polycom Group series VC units (high definition)
- Lync 2013 UC Platform
  - Lync 2013 FEP Servers
  - Lync 2013 Edge Server
- Skype for Business Desktop Video Conferencing

Audio Visual

The requirements for audio visual infrastructure at CSU encompasses the below set of standards as well as the AV and Video Conference Standard.

- AMX RMS (Remote management system)
- AMX AMX DVX, Nx & SVSi control systems
- AMX Touchpanels & Met Pads
- Sony Laser projectors (varied models)
- Williams IR Hearing Augmentation
- Echo 360 Recording Facilities

Server management

- Puppet
- Redhat Satellite
- SNMP
- Out Of band Management and Console
- Monitoring
  - SNMP Alerts
  - Nagios
  - Splunk log monitoring
  - Collectd

Document Control

Version	Author	Issue Date	Revisions
3.0	Kieran Fromholtz	June 2011	Document Created
4.0	Kieran Fromholtz	Dec 2014	Version Updates
5.0	Kieran Fromholtz	Apr 2016	Version Updates