Digital Solutions Division

ACT Government | ACT Health

High Level Vendor Design

Version 2020.1.1-Approved

This page is left intentionally blank

Please Read

IMPORTANT COMPLIANCE REQUIREMENTS

Note: The following instruction applies to all documents in this library.

This is a controlled document and is reviewed on an annual basis. The last review was carried out on November 2019. If you are viewing this document after November 2020, you will need to contact the sender to confirm you are working from the latest revision.

It is the responsibility of the contractor/vendor to read and adhere to the procedures, processes and guidelines set out in the following document when quoting for or carrying out work for ACT Health.

If you have questions or require clarification of any of the procedures, processes or guidelines in the following document please contact the sender of the document in writing with your questions so that a formal response can be provided. If any specific requirement is unclear, it is expected that clarification will be sought from the Health DSD - ICT architect(s), rather than a decision made and a design implemented and based on unclarified assumptions.

These standards are applicable to ALL CHS and ACTHD sites or any work funded by ACTHD (e.g. Calvary, ACTHD provided NGO sites) unless specifically exempt.

All Greenfield Health sites are expected to be fully compliant with all appropriate standards.

Brownfield Health sites undergoing refurbishment should be fully compliant unless an exemption is provided by DSD Infrastructure Hub.

In the event of any design non-compliance issues, a Departures document must be completed and submitted to DSD Infrastructure Hub. These issues should be resolved, in consultation with DSD Infrastructure Hub, as soon as possible within the project process and explicitly prior to site handover.

While some test cases have been cited within these documents as examples, the list is not exhaustive, and all appropriate test procedures shall be formulated, approved prior to testing and testing shall be performed by the client system administrators before full acceptance can be signed off by the Director of ICT Infrastructure Hub.

IMPORTANT:

Any departure from the standard, whether intentional or in error shall require a completed Departures Document to be submitted to DSD infrastructure Hub for approval.

Any non-compliant designs without a pre-approved Departures Document by completion of the project or a nominated milestone or gateway, will require remediation by the Head Contractor at the Head Contractors cost.

Document review high level

(to review detailed document updates Appendix B :)

Version	Summary of Changes	Author	Date
2019.1.0	Approval for release	Mark Moerman Senior Director ICT Infrastructure Hub	1/11/2019
2020.1.1	Updates to the Standards section	Nitin Saxena	13/02/2020

Document references

Document	Version	Location

Document default review cycle

(to be review every 12 months from the release date)

Date	Version	Comments
Feb 2020	2020 1.1	Release date
Feb 2021		(Next review date)

Document Owner

Name	Location
Senior Director, ICT Infrastructure Hub	DSD, Future Capability & Governance, ACT Health

Contents

1. Introduction

1.1. Context and Background

This document forms part of a suite of documents that describe the systems installed in a building for the ACT Government. It details the Vendor System requirements to facilitate the installation of the equipment and support of the nominated system/application.

1.2. Document Audience and Purpose

Once completed, this document will contain the Vendors installation and configuration requirements for the nominated systems for the NameofSite,BuildingorFloor. The purpose for documenting these requirements is to:

- Provide information to allow Digital Solution Division (DSD) Infrastructure Hub to understand the systems that will be installed and provide any underpinning ICT requirements;
- Ensure that the installation of the nominated system will meet the ACT Government's business and ICT requirements;
- Provide information for DSD Infrastructure Hub team to allocate and understand the following for the vendor systems:
    - appropriate amount of data cabinet space for the servers;
    - allocate correct number of switch ports for the servers and other devices;
    - provision appropriate size Uninterruptible Power Supply (UPS) which will provide backup power;
    - provision air conditioning that will include the requirements for the vendor equipment;
    - understand the vendor system remote access requirements to incorporate in the DSD Conceptual Solution Design document; and
    - understand the security features available for the system to obtain approval from the Security team.
- Enable consistency with Solution Designs (for the implemented projects) to be assessed;
- Provide a record of "intended state" so that other systems can be designed, integrated, or interfaced to the system;
- Provide a record of the "intended state" of the above for audit purposes; and
- Provide a baseline for change management activity, in particular, for future upgrades.

Note: It is critical that vendor designs are completed thoroughly and accurately. Partially completed sections are unacceptable. The information provided within this document will be used for the DSD Conceptual Solution Design and during the implementation stage of the project. Anything not included within this document will be out-of-scope for this project. Any changes to the information provided within the document have the potential to delay implementation of the system as DSD will have to undergo a review of the proposed changes.

1.3. Assumed Knowledge and Document Dependencies

An understanding of ACT Government and Shared Services ICT standards. Other relevant documents are mentioned in Appendix A : Reference Documents.

1.4. How to Use This Template

This template is intended to be filled out electronically and saved as a word document.

Do not simply overwrite the customisable fields within the document. Please use File menu, Properties and select Advanced Properties tab. Update the relevant 'values' within Advanced Properties.

The sections below should be filled out with sufficient detail to enable DSD to allocate the ICT resources that will be consumed by the systems. Existing sections should not be removed, if not required then mark as '*not applicable*', stating a reason for the response.

It is extremely important to understand that the information provided within this document will assist in DSD providing the vendor with relevant facilities within the communications rooms.

Although the document appears to be lengthy, a significant component of the document prompts the vendor for information. Text highlighted in yellow is provided as information as to the expected content for the section or instructions to be followed and are to be deleted or overwritten.

Should further information or clarification be required then DSD encourages the vendor to contact the DSD Infrastructure Hub project manager.

2. System NameofTheSystem

Update custom document property “SystemName” to change the reference above.

2.1. System Overview

Do not omit this section. Details are required.

Please provide an **architecture overview** of the system and the set of business requirements or functionality it will support. The architecture overview must provide sufficient information to a person who **does not** know the system. It must answer questions as per the following:

1. What is the component connectivity? For example, the head-end server connects to the concentrators which provide connectivity to the endpoints.
2. What functionality is provided by each component in the solution?
3. Do the components connect over IP network or is proprietary connectivity used?
4. Which component requires ACT Government network connectivity?

Centralised processing models should conform to a "Head End", "Concentrator" and "End points" style configuration. Distributed processing models should follow a logical star topology with autonomous end points and centralised management.

Provide **architecture logical diagram** which explains the solution.

2.2. System Component Summary

Please provide a summary of the system component modules or functions, and how they will interface with other modules within the system and other external systems over the IP network. Diagrams should be included to provide clarity.

2.3. Physical Infrastructure

2.3.1. Cabling Requirements

Please detail and describe any specific cabling requirements needed for your system.

2.3.2. Communications Room Requirements

Detail the location requirements for your system. For example, data cabinet versus wall mounted, proximity to other systems, amount of data cabinet Rack Unit (RU) or wall space required. Please detail any High Availability (HA) configuration proposed/required, including if it can tolerate physical separation and should therefore be installed in dual communications rooms for redundancy; or whether it needs to be installed in close proximity but can be connected to dual switch stacks allowing some redundancy.

Critical Note: To meet DSD standards, hardware located in communications room data cabinets should have **dual independent power supplies** and critical applications must be resilient against significant hardware failure (e.g. physical host failure as opposed to internal disk failure in redundant array). In the event the servers do not support dual power supplies, it must be noted in the document.

2.3.3. Workstations

Detail requirements for workstation software. To avoid proliferation of physical workstations on desks, first preference would be to install onto an **ACTGOV workstation**. Include any pre-requirements for a successful

installation. E.g. CPU, Memory, other applications. Also provide details of software to be installed, including version numbers.

2.3.4. Add Sections for Other Components

Add sections for other component of the system described in this document.

2.4. Configurations

2.4.1. Initial Configuration

Detail the initial configuration and setup of the system. This will provide both the base configuration details for future changes and the start of a run sheet for the initial installation.

2.4.2. Availability

Detail the incorporated levels of availability. Define general failure/outage scenarios and expected impact.

2.4.3. Application Interfaces

Detail how we interact with the application to use, configure and monitor it.

2.4.4. System Integration

Detail expected integration with other systems. See Integration Types for typically available options. Should your target system not be shown, please still add it with the necessary integration detail.

Target system	Type of integration (High/Low level)	Description of the interaction

2.5. Security Considerations

2.5.1. Vendor Access

Please advise the system vendor requirement for local and/or remote access to the system. If so, please detail the access requirements.

2.5.2. Logical Access Control

Please define how access control will be applied and what levels of access (or roles) will be available. This includes access using userid/password etc. See Logical Access Control for more information.

2.6. Capacity, Continuity and Recovery

2.6.1. Backup and Recovery

Please define how the system is to be backed up, who will be backing up the system and the recovery process.

2.6.2. System Monitoring and Alerts

Please define how the system will be monitored and alerts processed. This should include:

- What protocols are being used to monitor the system?
- Under what conditions are the alerts raised? What happens when a component fails?

- Who will monitor the system?
- Who will get the alerts?

2.6.3. System Capacity

Please provide system capacity limitations for the proposed system.

2.6.4. Licensing

Please provide system licensing requirements and who is providing the licenses.

2.6.5. Product Lifecycle

Please detail the hardware, firmware and software as appropriate and their expected lifecycles.

2.7. Network Bandwidth

Please detail the network bandwidth requirements for the system.

For the CCTV cameras, please provide the bandwidth consumed per CCTV camera.

2.8. Protocols used

Provide details of the network protocols that will traverse the ACT Government network between your system components. A security risk assessment will need to be conducted based on the proposed network protocols that will be used by the system.

The information required can have one or several of the components as follows:

Item	Requirement
NTP Requirements	*It is expected that the Directorate's NTP server will be used for time synchronisation. Provide any specific NTP requirements or if the system is unable to use NTP.*
DHCP Requirements	*Provide any DHCP requirements.*
DNS Requirements	*Provide any DNS requirements.*
Active Directory	*Provide any Active Directory or Domain requirements.*
OS Updates	*Is access to the Internet required for OS updates?* *Which protocol and port number will be used to access the updates?*
Application Updates	*Is access to the Internet required for application updates?* *Which protocol and port number will be used to access the updates?*
Anti-virus Updates	*Is access to the Internet required for Anti-virus updates?* *Which protocol and port number will be used to access the updates?*
Direction of Conversation Initiation	*Which system or system component initiates the TCP or UDP conversation?* *Which direction does the information flow?*
Encryption	*Is the application/system traffic encrypted?*
Unicast or Multicast	*Is the network traffic Unicast, Multicast or both?*
Broadcast	*Is the system using broadcast traffic?*

3. Network, Ports and Power Requirements Summary

Please detail the power, rack unit and network requirements.

The table below lists an example of the level of information required.

Note: All comms room equipment must have dual independent power supplies.

Item	Qty	Location			Power source and consumption	Heat (BTU)	Qty Network ports		Qty IP address		Network Bandwidth (if significant)		RU (only if required)		
		Comms Rm1	Comms Rm2	Other			Each and Type e.g. 1000LX, 10GBase-T	SubTotal	Each	SubTotal	Each	SubTotal	Each	SubTotal	
Primary Server	1	Yes			Mains 2xIEC 375w average	1280	3	3	3	3		0	2	2	
Secondary Server	1		Yes		Mains 2xIEC 375w average	1280	3	3	3	3		0	2	2	
Virtual appliance	1	N/a			N/a	N/a	0	0	2	24		0	N/a	0	
End point type A	12			Various, 1 per ward	PoE		1	12	1	12		0	N/a	0	
End point type B	5			Various, in Corridor	PoE		1	5	1	5		0	N/a	0	
Workstation	2			1 per specify location	Mains 1x 10A 250w average	854	1	2	1	2		0	N/a	0	
CCTV (2MP)	9			Various corridor	PoE		1	9	1	9	8Mbps	72	N/a	0	
							Totals:	**34**		**58**		**72**		**4**	

Notes:

The information provided in the table above is used for the following purposes:

1. Location and number of the appliances, in combination with the data cabinet space required, will provide SSICT with information to provision appropriate number of data cabinets within each communications room;
2. The power requirements for each appliance and other components will provide input into the UPS sizing;
3. The heat generated by each appliance will provide input into air condition sizing for each communications room; and
4. Network port and bandwidth requirements will be used for calculating number of network switches required per communications room. Additionally, it will provide input into network capacity planning and provisioning.

It is critical this information is accurate and complete.

Appendix A : Reference Documents

A.1. References

The following DSD Standards and Specifications documents should be referenced for the proposed systems. The version of Standards and Specifications documents are correct at the time of writing the document.

#	Standard/Specification	Version Date
1.	DSD ICT Scope Specification -General 2019	October 2019
2.	St-02 Communications Cabling Infrastructure 2019	October 2019
3.	St-03 Fibre Lead-Ins for Campus and Offsite Buildings 2019	October 2019
4.	St-05 Communications Room Building Infrastructure and ICT requirements 2019	October 2019
5.	St-06 Comms Room and UPS-Batt Layout 2019	October 2019
6.	St-07 Cabinet Physical Layout Cabinet Separation and Governance 2019	October 2019
7.	St-08 Security ICT Standard 2019	October 2019
8.	St-09 BMCS ICT Specifications	November 2019
9.	St-10 Lighting Control System ICT Specification 2019	October 2019
10.	St-11 Fire Systems ICT Specifications 2019	November 2019
11.	St-14 Nurse Call ICT Specification 2020	February 2020

Note: Please consult DSD Infrastructure team for a copy of the latest Standards documents.

Appendix B : Glossary and Amendment Log

Glossary of terms

Abbreviation	Name	Description
BD	Building Distributor	When the term room is absent, refers to the building switch linking the FD's to CN's. A "BD room" will refer to the room housing the BD and this room will by default also be a FD room.
CD	Campus Distributor	When the term room is absent, refers to the switch linking all campus BD switches to the WAN/RN's and DC. A "CD room" will refer to the room housing the CD and this room will by default also be a BD & FD room.
Comms room	Comms room	Generic name used for CD, BD, FD or DC rooms
DC	Data Centre	High end comms room containing servers
ICT	Information and Communications Technology	Covers information technology and various systems such as computers, systems and infrastructure.
FD	Floor Distributor	When the term room is absent, refers to the floor copper access switch linking the FD's to the BD('s). A "FD room" will refer to the room housing the FD
HA	High Availability	Usually provided by redundant physical components or pathways.
RN	Regional Node	Equivalent functionality to the campus distributor CD but in remote sites. RNs form a central Meshed network
Switch Stack	Switch Stack	Individual switches will be linked together using stacking cables to form a single switch entity called a switch stack. The stack shall be connected to the BD switches using fibre trunks and be referenced by a single ID e.g. TCH-B1-L1-SAO1
VLAN	Virtual Local Area Network	A virtual LAN is any broadcast domain that is partitioned and isolated in a network at the data link layer.
VRF	Virtual Routing and Forwarding	IP (Internet Protocol) that allows multiple instances of a routing table to exist in a router and work simultaneously to allow segmentation of network.

Table 1 - Glossary of terms

Note: other terms not listed here can be found in the DSD ICT Glossary of Terms.

Amendment history

Version	Summary of Changes	Author	Date
2019.0.1	Update document and migrate to new DSD template.	Nitin Saxena	31/10/2019
2019.1.0	Finalised fields ready for release	Nitin Saxena	1/11/2019

Table 2 - Amendment History

Appendix C : Expansion of Concepts

A.2. Integration Types

Following is a brief explanation of the type integration between systems.

Low level: Refers to a direct connection. Usually DC in nature, e.g. 12v/0v or relay contacts closed/open.

High level: Refers to a connection where data may be transferred, and the medium used for the connection. May be either a single direction or bidirectional in nature. Connection will conform to a standard bus and data to a standard protocol e.g. RS485 and BACnet.

A.3. Vendor Access

Vendor access may be provisioned as either local physical access (usually supervised) and via remote access using Cisco client-based VPN and two-factor authentication. Local physical access may be supervised or unsupervised depending on the site and the support contract with Health Directorate. Remote access is unsupervised and has several prerequisites including an underpinning support contract and approval from the security teams.

Note: System upgrades and modifications are subject to our change and release management process. The granting of remote vendor access does not exempt the system from change management.

A.4. Logical Access Control

Logical access control is the level of access and control within the system. Broadly, there are 4 levels of access:

- End user: Standard everyday access for the user of the system. Access is limited to basic requirements to perform their everyday duties without impedance;
- Super User: Higher levels of access e.g. create reports and some configuration.
- Application admin: Administrative access to the application e.g. add/remove users. Apply application upgrades.
- Server Admin: Administrative access to the OS and hardware e.g. OS upgrades, RAID additions, cluster and HA configurations.

In all instances, user accounts must have complex passwords applied to comply with ICT Securities requirements.

Last page is left intentionally blank