Digital Solutions Division

ACT Government | ACT Health

St-08 Security ICT Standard

Version 2019.2.0- 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 September 2019. If you are viewing this document after September 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 click here)

Version	Summary of Changes	Author	Date
2019.1.8	Update 'Compliance Requirements' page. Review the document and update as necessary.	Nitin Saxena	04/10/2019
2019.1.8	Sent to the Technology Strategy Committee for approval to release	Mark Moerman	08/10/2019
2019.2.0	CIO Approval for release	Sandra Cook a/g CIO	09/10/2019

Document references

Document	Version	Location

Document default review cycle

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

Date	Version	Comments
Oct 2019	2019 2.0	Original release date
Oct 2020		(Next review date)

Document Owner

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

Contents

1. Document Purpose

1.1. Context and background

This document forms part of a suite of documents that describe ICT specifications for the ACT Health Directorate support systems. It provides the ICT specifications for several Security Systems which are applicable to the green-field and refurbished brown-field sites.

1.2. Assumed knowledge and document dependencies

Relevant documents are mentioned in Appendix A.

1.3. Disclaimer

The following document provides ICT ONLY specifications and requirements for the security systems at the Health Directorate and is by no means intended to cover all the comprehensive business requirements for the system. Additional business and user requirements will be presented in project specific documentation such as Business Requirements, Solution and Detailed designs.

2. Executive summary

The specifications provided in this document are based on enterprise architecture and integration for each security system across all the Health Directorate sites. This architecture will provide the building blocks for a consistent implementation of systems for the Health Directorate. Additionally, it provides the benefit of installations that have standardised installation and configurations within the Directorate, enabling reusable patterns and repeatable system implementation. The consistent architecture will minimise the risks associated with ongoing support for disparate implementations, simplifying the installations whilst reducing the ongoing maintenance costs.

The document provides specifications for all the ICT systems that constitute elements of security at the Health Directorate sites. These include:

- Duress:
  - Fixed;
  - Wireless Fixed location;
- Real Time Location System (RTLS) Mobile Duress;
- Help Points:
  - Consumer Help Point Intercom;
  - After-hours Building Access Intercom;
  - After-hours Ward access;
  - Lift Emergency Intercom;
- Electronic Access Control;
- Intruder Alert;
- Closed Circuit Television (CCTV); and
- Key Management System.

The network infrastructure implemented to support critical systems is in compliance with the Medical Grade Network (MGN) architecture. The MGN architecture can be summarised as modular, Highly Available (HA) and resilient network which minimises the impact of a network component failure on the Health systems. Additionally, the architecture provisions sufficient capacity to allow for growth in the infrastructure requirements for Health systems.

3. Architecture

The architecture presented within this document complies with the architecture principles as follows:

- **AP1**. Control technical diversity to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple systems;
- **AP2.** Maintaining interoperability between systems to conform to defined standards that promote benefit to the business;
- **AP3.** Commissioning systems to a defined level of availability, recognising increasing demand for services to be provided outside of traditional office hours. The system availability also considers the lack of tolerance for system outage over longer periods of time;
- **AP4.** The systems must be manageable remotely and be monitored;
- **AP5.** Use of common systems for head-end and building concentrator layers throughout the Health Directorate is preferred rather than use of separate vendor systems performing identical tasks; and
- **AP6.** The systems must be able to adapt for change and growth. The architecture modularity allows for individual components to be upgraded without replacing the entire system.

The following technology principles are also applicable:

- **TP1.** Interface between head-end and building concentrator shall be IP over Ethernet but under certain circumstances can be a sub protocol such as TCP, BACnet, UDP etc;
- **TP2.** Interface between endpoint devices and the concentrator shall follow known standards, however it can be a mixture of analogue, dry contact, or data protocol compliant cabling (e.g. BACnet over RS485); and
- **TP3.** The systems where the concentrator component of the architecture is in two parts, the interface shall be an approved data bus standard (e.g. BACnet over RS485).

3.1. Three-Tiered Model

The recommended architecture model implemented at the Health Directorate complies with a three-tiered modular approach. The tiered model is based on the principles of hierarchy, modularity, resiliency and flexibility.

3.1.1. Fully Compliant Model

This model consists of three tiers, head-end servers/appliances located in the data centres, building based concentrators/appliances and endpoint devices, which support hierarchical and modular approach. The head-end and building concentrator tiers within this model are intended to provide high levels of resiliency and availability. The model also provides the

flexibility of leveraging existing head-end server infrastructure, where practical, which is expected to be used within various onsite or off-site buildings.

The security systems must be compatible with IP networks and should be able to leverage existing Shared Services ICT layer-3 network that provides connectivity between buildings and the data centre.

The Shared Services ICT network architecture has been provisioned to comply with the MGN architecture which supports the principles outlined previously, providing a robust and resilient network that supports all the security systems mentioned in this document.

The following diagram, Figure 1, illustrates at a conceptual level the proposed three-tiered architecture for each of the systems. The subsequent sections describe each architecture layer mentioned in the three-tiered model.

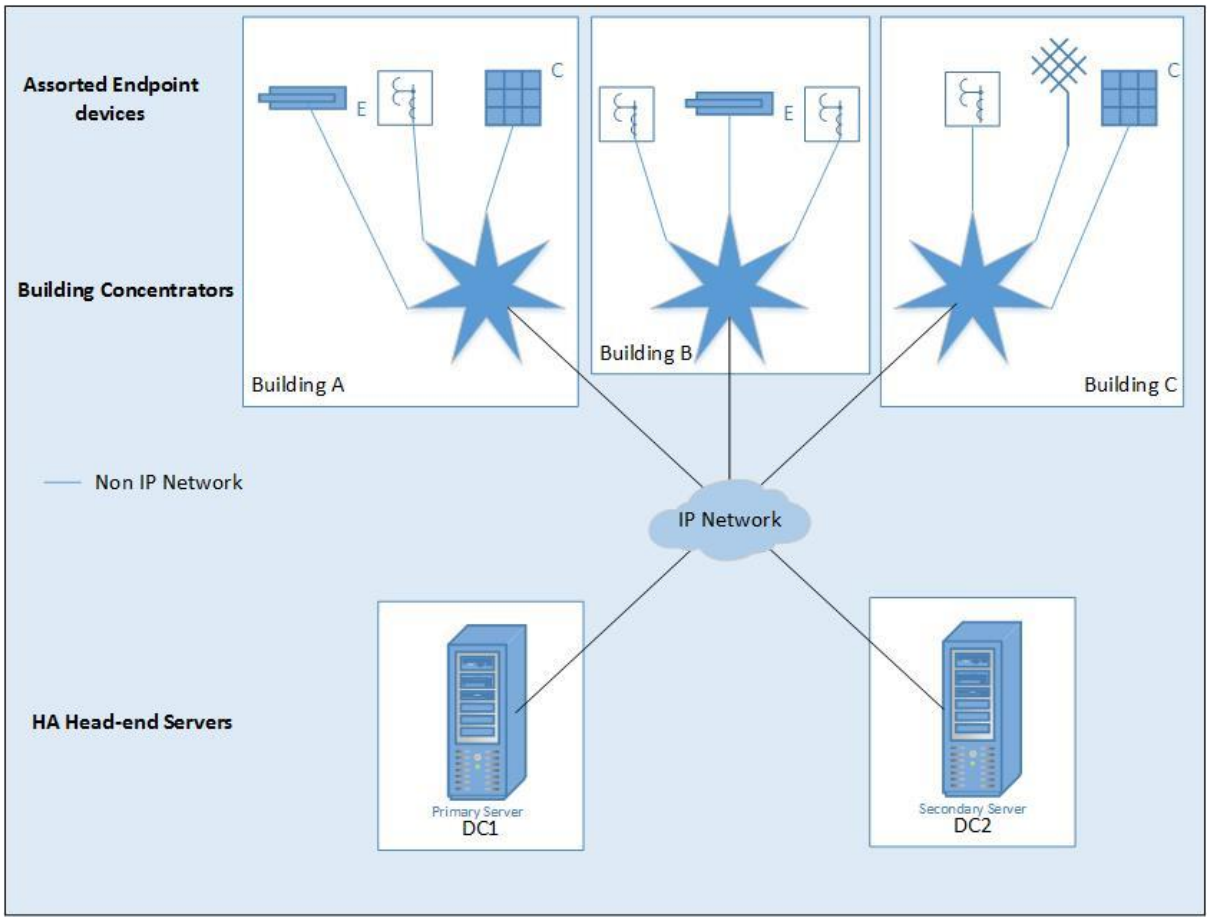

Figure 1 - Generic 3-tiered Architecture of Security Systems

3.1.2. Three-Tiered Model (Variant)

Under certain circumstances, an alternate model that is a variant to the fully compliant Three-Tiered Model is acceptable. However, the systems under this exception will need to be reviewed and approved by DSD Infrastructure solutions architects.

Some systems, such as CCTV, do not have building-based concentrators. The endpoint devices for these systems connect directly to the ACT Government network switches, which

provide connectivity over the network to the head-end infrastructure. The head-end infrastructure is expected to comply with the standards outlined for the three-tiered architecture.

These systems will adhere to the architecture as illustrated in the following diagram, Figure 2.

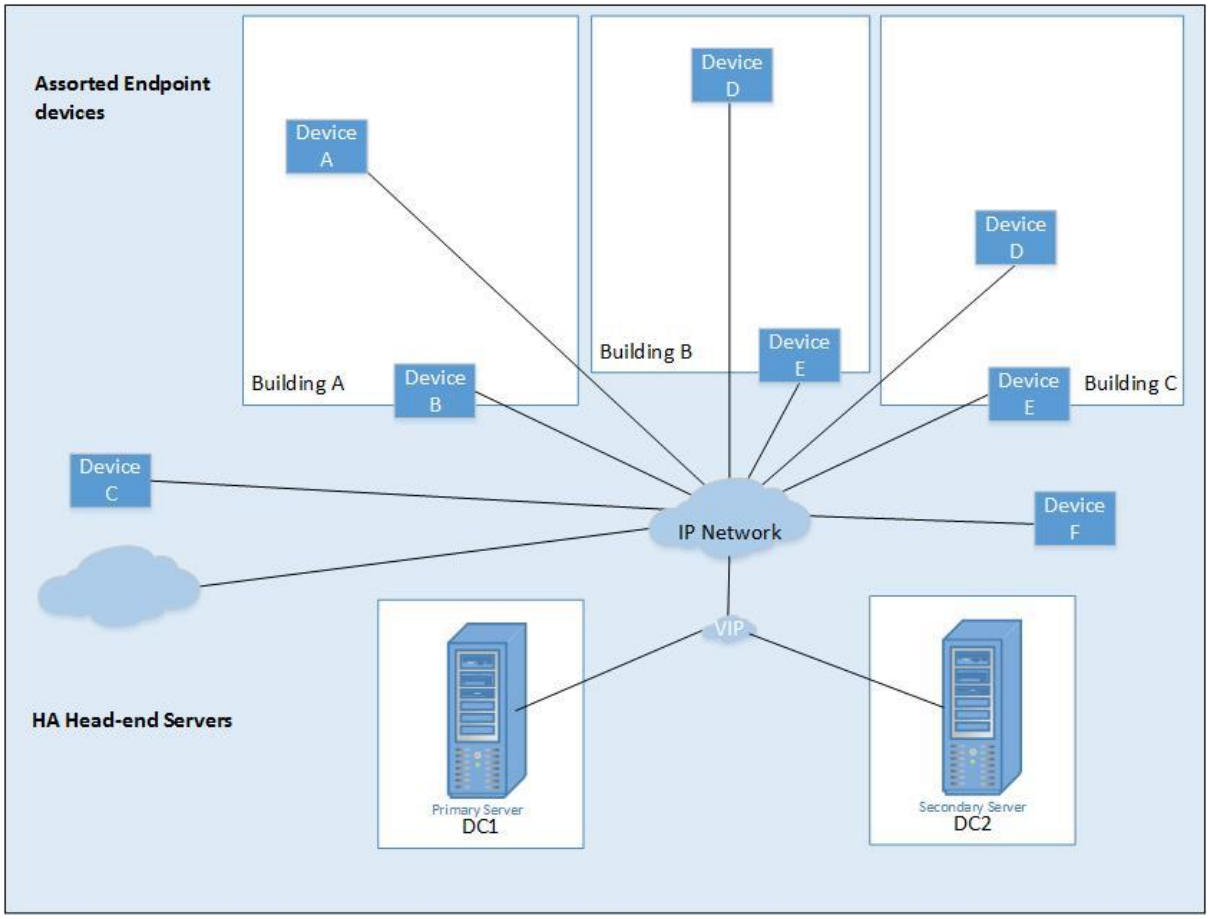

Figure 2 - Architecture for Endpoint Devices supporting direct Ethernet Connectivity

3.2. Head-End Infrastructure

The head-end infrastructure is expected to be deployed in a highly available model, whereby a set of primary and secondary systems will be provisioned. These servers/appliances will support several buildings and must be located in separate data centres in geographically disparate locations.

In the HA configuration, the secondary appliance must be ready to assume the primary role in the event of the failure of the primary appliance. The fail-over is expected to be automatic, in order to minimise the impact on system users.

The primary and the secondary systems must consist of the same model appliances and must operate on the same level of software. It is expected a heartbeat will be maintained between the two systems and failover will take place when the secondary system does not receive a configurable number of heartbeats from the primary.

The primary and secondary systems will present a Virtual IP (VIP) address to the devices accessing the head-end appliances. The individual IP addresses allocated to the appliances will not be exposed to other devices.

The head-end servers/appliances must support the following physical features:

- Support dual Network Interface Cards (NICs); and
- Dual power supplies.

The servers/appliances will support the following capabilities:

- Be capable of location in geographically separates physical locations;
- Automatic failover from primary to secondary system;
- Manual secondary to primary fail-back; and
- System will support Layer-3 IP network.

3.3. Building Infrastructure

Building Concentrators will provide the local building interface between the Shared Services ICT provided IP network and the system-based distribution network (e.g. IP, BACnet, DALI, Zigbee etc). These concentrators will be the conduit between the endpoint devices and the head-end servers located in the data centres.

The concentrators shall access the head-end infrastructure using the VIP address allocated to these devices. Therefore, failure of the primary appliances should not require the concentrators to access a different IP address for the secondary appliances.

In all cases these concentrators shall have an element of autonomous operation capability. In the unlikely event of loss of both the network links, from a site providing connectivity to the data centres, or the loss of the local network interface the concentrators shall support the ongoing operational requirements which include the current stored configuration, receipt and storage of data/logging of the endpoint devices for at least 24 hours.

Concentrators should have:

The building concentrator servers/appliances must support the following physical features:

- Dual power supplies[1]; and
- Dual NICs[2].

The building concentrator servers/appliances must support the following capabilities:

- Support or provide functionality required by the endpoint devices; and

[1] One supply can be a battery, if the system can continue to run with the dead/faulty power supply.
[2] If concentrator can continue to operate with endpoint devices with a faulty/dead NIC then one NIC is acceptable.

- Autonomous operation during periods of network connection outage for example operate user interface devices based on previously stored configuration data. The input data should be maintained locally until network is restored.

3.4. Endpoint Devices

Endpoint devices will provide the required capabilities of the specific system, relaying sensor and/or input device data back to the local building concentrator which will provide operational instruction to other endpoint devices or communicate with the head-end providing information and instructions to activate an endpoint device, for a particular function.

There are two models for endpoint device access to the head-end infrastructure.

3.4.1. Model 1 - Direct Connection to Concentrator

Under the first model, the endpoint devices are expected to be physically connected to the building-based concentrators under three-tiered architecture.

These devices can include duress buttons, annunciators, assurance lights, alarms, locks, input devices, swipe card readers etc. The protocol supported by these devices may include IP, BACnet etc.

3.4.2. Model 2 - Connection to Network Switches

Under the second model, the endpoint devices for some systems may connect directly to the network switching infrastructure. The network switches will provide power to the endpoints via Power over Ethernet Plus (POE+) feature.

The architecture for these systems does not include building concentrators. The endpoint devices access the head-end infrastructure over the ACT Government network.

3.5. Exceptions and Exemptions

Any departure from the above architecture, shall only be accepted when a full assessment of the system has been completed by the DSD Infrastructure solutions architects and has been shown to provide an acceptable alternate architecture model after technical, operational and risk assessments have been satisfied.

A departure document must be completed by the head contractor and provided to the DSD Infrastructure team for assessment prior to proceeding with the implementation of the system at the site.

The existing systems will not be required to undergo an assessment, unless they are not compliant with the architecture principles outlined in this document.

4. Fixed Duress

4.1. Introduction

Fixed Duress will provide a means for Health Directorate staff under personal duress situations to initiate a code BLACK alarm, summoning help from security staff at The Canberra Hospital (TCH) or designated responders at offsite premises.

There are two types of fixed duress system endpoints as per the following:

- Hard-wired buttons; and
- Fixed location wireless endpoints.

4.2. Architecture

The following diagram, Figure 3, illustrates the architecture for the fixed duress system.

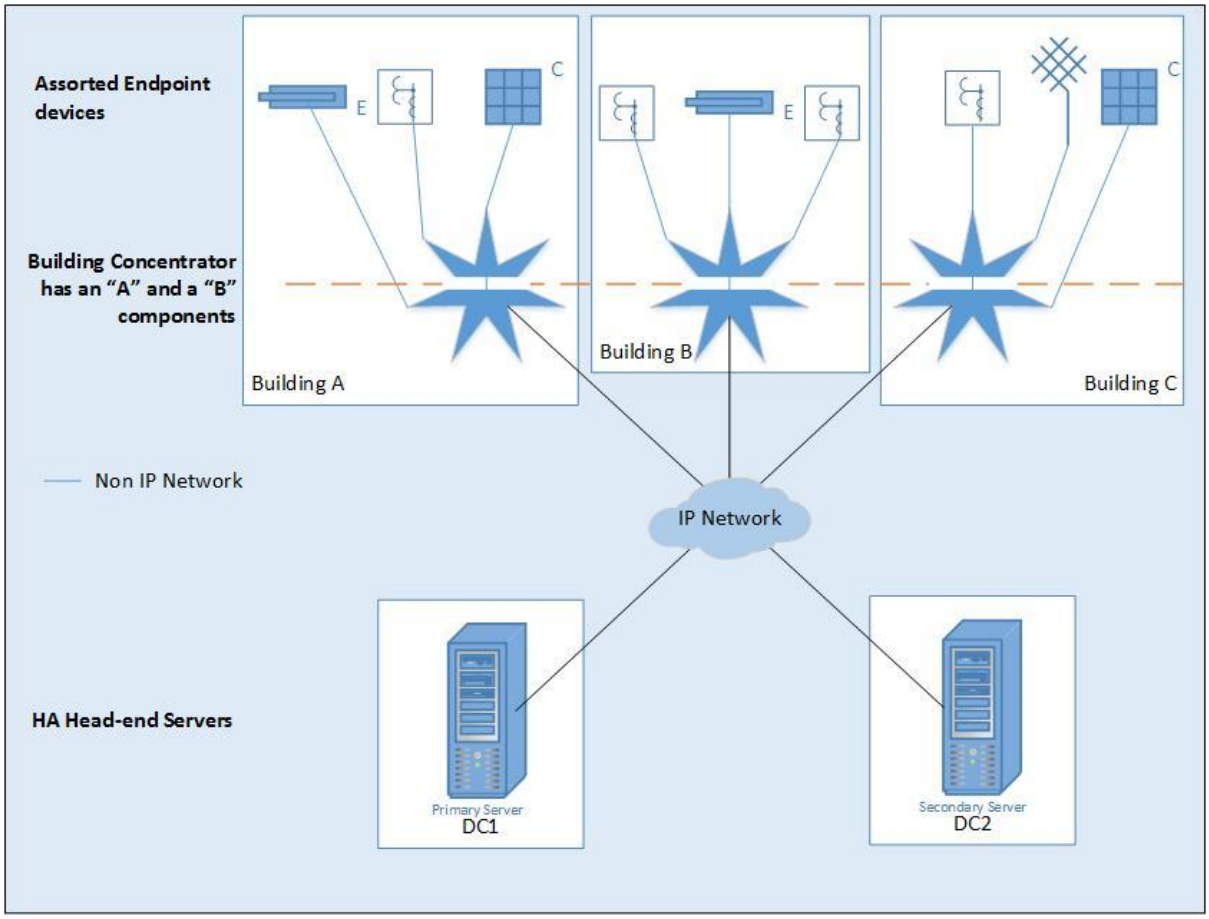

Figure 3 - Fixed Duress Architecture

4.2.1. Head-End Infrastructure

The head-end infrastructure is expected to be deployed in a HA model as per the architecture principles outlined in section 3.2, unless this is technically not feasible. This infrastructure will be located within separate ACT Government data centres that are in geographically disparate locations in Canberra. Connectivity between the data centres has been provisioned over Shared Services ICT layer-3 IP network.

The primary and secondary head-end infrastructure should be able to leverage the ACT Government layer-3 IP network. Shared Services ICT will allocate the public IP addresses used by the system to communicate with other Health systems. In the event the system has a requirement to use private network, this information should be provided to the project team. The primary and secondary servers will present a Virtual IP (VIP) address to the devices accessing the head-end appliances. The individual IP addresses allocated to the appliances will not be exposed to other devices.

The head-end infrastructure will provide the functionality outlined in the following sections.

4.2.1.1. Network

- Support IP connectivity;
- Capable of supporting Virtual Local Area Network (VLAN) to separate duress network traffic from other systems;
- Support layer-3 network connectivity; and
- Capable of supporting a Session Initiation Protocol (SIP) trunk to the ACT Government Unified Communications infrastructure.

4.2.1.2. High Availability

- Support highly available servers operating in primary and secondary configuration;
- Individually, primary and secondary server infrastructure should be able to support the entire Health Directorate duress requirements. Hence, in the event the primary servers are inoperative, the secondary servers should be capable of supporting the functionality and capacity provided by the primary server;
- The failover from the primary to the secondary should be automatic without any intervention. The vendor must state the length of time taken to failover from primary to secondary system;
- The failback from the secondary to the primary should be configurable to be either manual or automatic; and
- The primary and secondary appliances must be capable of synchronising configurations when a change is implemented. The synchronisation should be configurable to be automatic or manual.

4.2.1.3. Monitoring and Alerts

- The system must be able to send alerts to the nominated personnel when the secondary servers assume the role of primary servers;
- Must be able to monitor and report on the status of endpoint devices i.e. support regular polling and/or keep-alive messages. Polling intervals must be configurable from one minute to four hours in one-minute increments; and
- The system shall support Simple Network Management Protocol (SNMP).

4.2.1.4. Logging

- Maintain logs which record system errors and events. Some examples are date and time of configuration changes, synchronisation status with the secondary system, primary system fail over to the secondary system.

4.2.1.5. Integration

- Should be able to integrate with the incumbent Nurse Call infrastructure. The duress system must be able to use a 'heartbeat' or polling mechanism with the Nurse Call system to maintain the integrity of the link between the two systems;
- Should be able to integrate with the existing Vitacom paging system to send messages to the pagers; and
- Should be able to integrate with the Fire Information Panels (FIP).

4.2.1.6. Reporting

- Provide comprehensive reporting features that includes "pre-configured" reports and customisable reports.

4.2.1.7. Time Synchronisation

- Must be able to synchronise time with the Health Directorate Network Time protocol (NTP) server over the ACT Government network.

4.2.2. Building Infrastructure

The building infrastructure can consist of one or both of the components as per the following.

4.2.2.1. Building based servers

The architecture of some systems requires hosting of the head end servers in the data centre and the building. These systems use the architecture of master servers located in the data centre and slave servers located in the buildings.

DSD will consider these servers as the head-end server component, in combination with the data centre located servers, of the Three-Tiered Architecture.

4.2.2.2. Building based concentrators

Building Concentrators will provide the local building interface between the ACT Government IP network and the system-based distribution network. All the endpoint devices will be connected to the concentrators, which will support the functionality provided to the endpoint devices.

The building concentrators will support the functionality outlined in the following section.

4.2.2.3. Network

- Support IP connectivity to the head-end servers located in data centres;
- Capable of supporting VLAN to separate duress network traffic to and from other systems; and
- Support layer-3 network connectivity.

4.2.2.4. High Availability

- Must be able to function in a highly available configuration with primary and secondary concentrators hosted within the building;
- The failover from the primary to the secondary should be automatic without any intervention;
- The failback from the secondary to the primary should be configurable to be either manual or automatic;
- These appliances must be capable of supporting the site functionality locally in the event the network connection between the building-based appliances and the head-end infrastructure is unavailable; and
- The appliances must support physical device hardware resiliency by providing dual power supplies and dual NICs.

4.2.2.5. Monitoring and Alerts

- The system must be able to send an alert to the nominated personnel when the secondary appliances assume the role of primary appliances;
- The system shall be capable of monitoring the endpoint devices for failure and send alerts to the nominated system and personnel. This event shall also be recorded in the log files; and
- The system must support SNMP.

4.2.2.6. Logging

- Maintain logs which record system errors and events. Some examples are date and time of configuration changes, synchronisation status with the secondary system, primary system fail over to the secondary system etc.

4.2.2.7. Reporting

- Provide comprehensive reporting features that includes “pre-configured” reports and customisable reports.

4.2.2.8. Time Synchronisation

- The system must be capable of synchronising time with the Health Directorate NTP server over the ACT Government network.

4.2.3. Endpoint Devices

The endpoint devices, such as hardwired duress buttons and annunciators, will be provisioned in the building based on the requirements provided by the business. These devices will connect to the building-based concentrators either over the ACT Government network or via direct cabling.

The building concentrator / endpoint device interface will support the following functionality in line with AS/NZS 2201.1:2007, Intruder alarm systems, Part 1: Client’s premises—Design, installation, commissioning and maintenance.

Fixed Devices

For fixed devices such as hard-wired buttons, the following functionality is required.

4.2.3.1. Monitoring and Alerts

- The duress system must be able to monitor endpoint devices for failure and send alerts to the nominated personnel. This event should also be recorded in the log files;
- The endpoint devices should be installed with circuit in ‘closed’ state. In the event the system detects the endpoint device in an “open circuit” state, an alarm should be generated, and alerts sent to the nominated personnel;
- The duress system must be able to monitor circuit to endpoint device for impedance change (short circuit), producing an alarm state and send alerts to the nominated personnel;
- Following duress alarm activation, the alarm must be displayed on all specified annunciators within five seconds;
- The annunciators or separate zone sounder speakers must be able to provide an audible notification of a duress alert with appropriate pitch, volume and frequency. These devices must support the following features:

- IP network compatible
- Support Power over Ethernet Plus (POE+)
- Fully programmable
- Provide individual volume control;

- The annunciators must be able to display text uniquely identifying the alarm location.

4.2.3.2. Physical Characteristics

- The endpoint devices must be physically robust to be able to withstand regular and frequent use.

Wireless Devices

For Wireless devices (tags in static location, handsets and pendants), the interface between endpoint device and concentrator is 802.11 wireless network transmission.

4.2.3.3. Monitoring and Alerts

The following four alerts and alarm conditions must be met:

- Lost contact (out of range);
- Tamper alerting;
- Battery alarm (two-week warning for flat battery); and
- Duress Alarm.

4.2.3.4. Batteries

- The batteries used for the wireless duress buttons must support:
  - A minimum of 12 months battery life under normal usage conditions;
  - Support full operation of duress system for a minimum of two hours; and
- The security system must monitor battery life and transmit low battery voltage alarm messages over a High-Level Interface (HLI).

4.3. System Configuration Requirements

4.3.1. Hardware

There is a requirement within the Shared Services ICT to provision all systems, where available, on virtual systems.

The head-end appliances shall be capable of running on virtual platforms as a first preference. However, physical appliances will be acceptable in the event the system cannot be supported on virtual platforms.

There is a potential that multiple endpoint devices are used with the duress system. These devices include but are not limited to the following:

- Duress buttons;
- Annunciators;
- Strobe; and
- Assurance light.

4.3.2. Software and Licensing

The software and licensing must comply with the requirements specified in sections **Error! R eference source not found.** and **Error! Reference source not found.**.

4.3.3. Power

All the critical Health Directorate systems are provisioned with Uninterruptible Power Supply (UPS) support. The backup power for the duress system will be supported by the UPS units.

The power requirements for each of the duress appliances shall be documented in the High-Level Vendor Design (HLVD) and provided to the DSD Infrastructure solutions architects for UPS sizing during the system design stage of the project.

The endpoint devices are powered by the building concentrator via a direct cable Low Level Interface (LLI).

Note: The system vendor shall provide spare batteries for the handsets and battery charging racks.

5. Mobile Wireless Duress

5.1. Introduction

Some Health facilities, such as Mental Health Units, have a requirement to gain visibility into the staff location for security purpose. The consumers have a potential to pose physical threat to the staff working at these sites. It is crucial that staff location can be identified to provide rapid response by security personnel in the event of a physical assault or any other duress situation.

A wireless Real Time Location System (RTLS) has been provisioned for several Health Directorate buildings. This RTLS system is able to track staff location indoors and outdoors with sufficient accuracy to provide staff at the site rapid assistance under emergency situations. The staff members carry a duress handset and potentially a wireless pendant which communicates with the head-end server located in the data centre over the existing ACT Government 802.11 a/g/n wireless network. The system displays staff location using actual floor plans on a console in real-time.

5.2. Architecture

The following diagram,

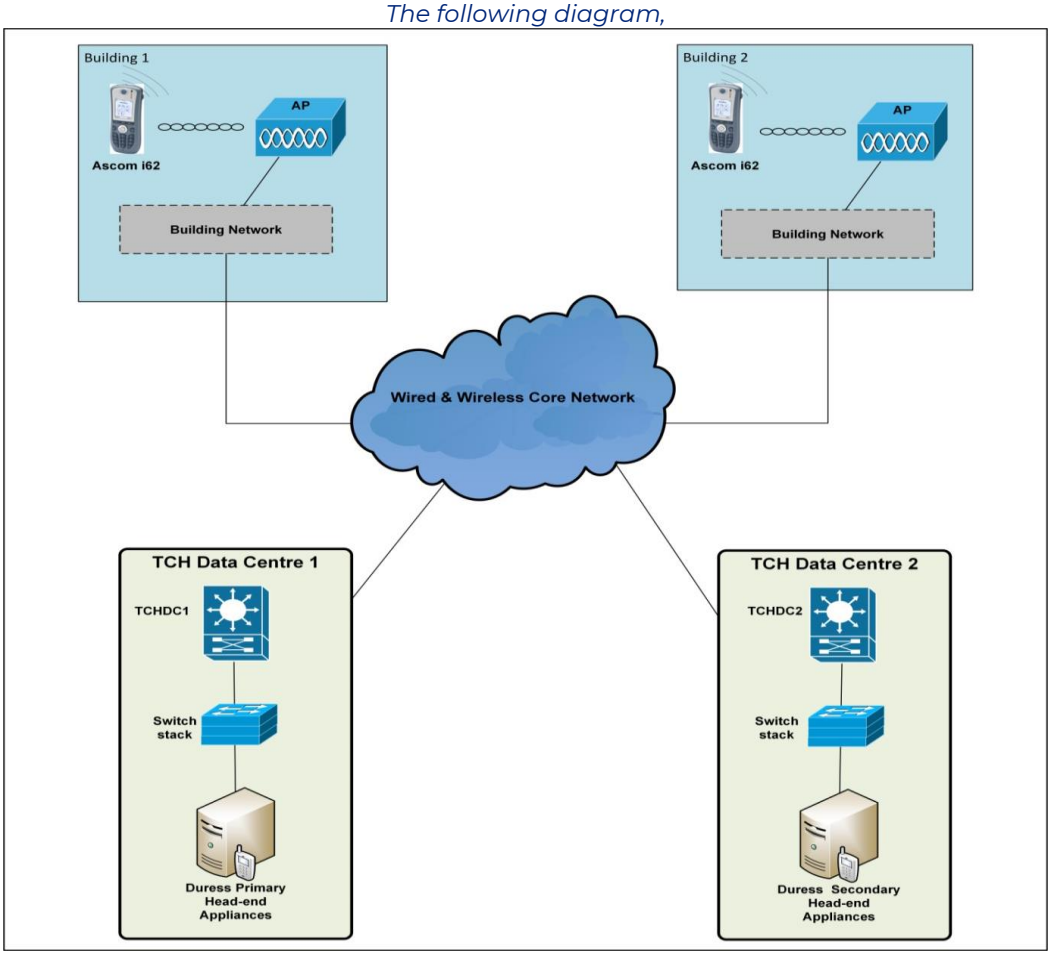

Figure 4, illustrates the preferred architecture for mobile wireless duress.

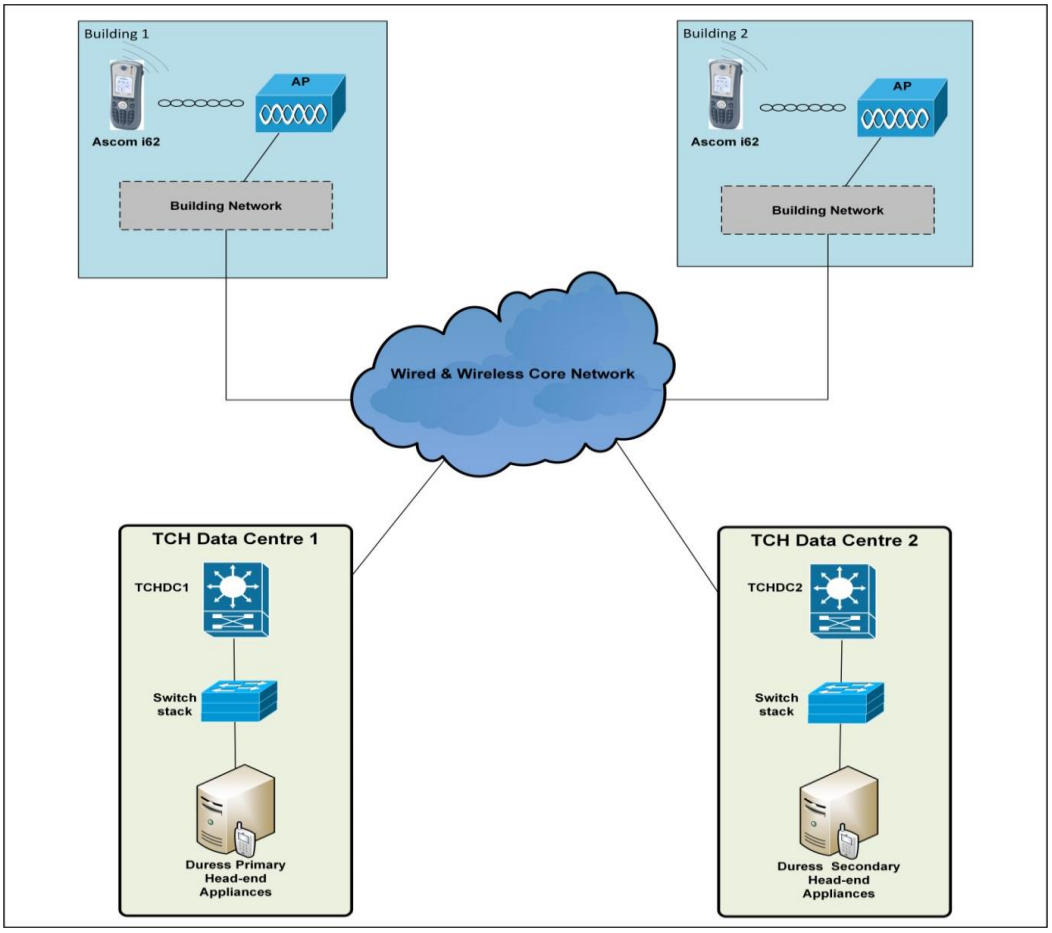

Figure 4 - Mobile Wireless Duress Architecture

5.2.1. Head-End Infrastructure

The head-end infrastructure is expected to be deployed, as outlined in the architecture principles in section 3.2 in the data centre. The appliances will receive location information from the endpoint devices over the existing network infrastructure. This information shall be processed by head-end appliances for location analysis and display. The primary and secondary head-end infrastructure shall be capable of communicating over the ACT Government layer-3 IP network.

The head-end infrastructure will provide the functionality outlined in the following sections.

5.2.1.1. Network

- Support IP connectivity;
- Capable of supporting VLAN to separate duress network traffic from other systems;
- Support Layer-3 network connectivity;
- The system shall leverage 802.11 a/g/n wireless network. The preference is for 802.11n to be used; and
- The wireless frequency must be either 2.4 or 5GHz frequency spectrum. However, technically there is a preference for 5GHz.

5.2.1.2. Location Requirements

- The system shall provide guaranteed location granularity within five[3] metre accuracy or less; and
- The system shall provide location, in real time, on actual floor plans on a designated console.

5.2.1.3. High Availability

- The primary and secondary appliances shall be able to support the entire Health Directorate mobile duress requirements;
- The failover from the primary to the secondary should be automatic without any intervention. The vendor should state the length of time taken to failover from primary to secondary system;
- The failback from the secondary to the primary should be configurable to be either manual or automatic; and
- The primary and secondary appliances must be capable of synchronising configurations when a change is implemented. The synchronisation should be configurable, which can be automatic or manual.

5.2.1.4. Monitoring and Alerts

- The system must be able to send an alert to the nominated personnel when the secondary appliances assume the role of primary servers;
- The system must log the event when primary system fails-over to the secondary system;
- The system shall support SNMP; and
- The system shall highlight an alert on the console. The alert will need to be cleared manually.

5.2.1.5. Logging

- The system must log the location progress of the event until reset;
- The system must log any significant events within the log files; and
- The logs should be recorded locally and to a remote log server.

[3] Although 5m is guaranteed, in reality accuracy down to 1m has often been achieved, but this can vary with changes in solid or absorbing structures nearby.

5.2.1.6. Reports

- Provide comprehensive reporting features that includes “pre-configured” reports and customisable reports.

5.2.1.7. Time Synchronisation

- Must be able to synchronise time with the Health Directorate NTP server over the ACT Government network.

5.2.2. Building Infrastructure

The building infrastructure required to support mobile duress is provided by the Wireless Access Points (WAPs) located at the site. These WAPs form a component of the 802.11 a/g/n wireless network that is provisioned for each site.

It is expected that the mobile wireless duress system and handsets will leverage ACT Government WAPs. The wireless network head-end infrastructure is configured and managed by the Shared Services ICT network team.

5.2.3. Endpoint Devices

The endpoint devices used to support mobile duress primarily consist of a handset carried by staff. This handset shall support features outlined in the following sections.

5.2.3.1. Handset Features

- Support the firmware which facilitates location tracking;
- Support the “Man-down” feature;
- Must be ruggedised and robust to be able to handle being dropped and being handled roughly; (compliance with IEC 60068-2-32 Basic Environment Testing Standard);
- Access to centralised ACT Government phone book;
- Centralised management for upgrades and configuration;
- Capable of supporting an ‘open-channel’ call that enables the response team to silently listen to the duress incident via one-way audio from the initiating handset;
- Capability for staff to log-on to handsets on a shift-by-shift basis;
- Capability for staff to undertake testing of duress functions prior to commencement of shift;
- Capability for messages to include Accept/Reject feature;
- Provide ability to make Voice over WiFi (VoWiFi) phone calls; and
- The duress system shall provide the ability to restrict the handsets to make authorised phone calls only.

5.2.3.2. Monitoring and Alerts

- The handsets must be able to receive alert messages from the mobile duress system, Nurse Call, Electronic Access Control System and paging systems via the central messaging system; and
- Provide an alarm button on the handset which supports local and global duress calls. When the button is pressed a message can be sent to every handset in the designated response group.

5.3. System Configuration Requirements

5.3.1. Hardware

The head-end appliances shall be capable of running on virtual platforms as a first preference. However, physical appliances will be acceptable in the event the system cannot be supported on virtual platforms.

The wireless handsets shall comply with Health standards and must be:

- Infection control compliant;
- Water proof; and
- Shock proof.

The handsets shall be configured to run on 5GHz and final RTLS surveys completed using 5GHz.

5.3.2. Software and Licensing

The software and licensing must comply with the requirements specified in sections 13.14 and 13.15.

5.3.3. Power

The power requirements of the mobile duress infrastructure shall be documented in the HLVD and be provided to DSD Infrastructure solutions architects for UPS sizing during the system design stage of the project.

The handsets will have rechargeable batteries.

Note: The system vendor shall provide spare batteries for the handsets and battery charging racks.

6. Closed Circuit Television

6.1. Introduction

The Closed Circuit Television (CCTV) is one of the security system components that support security requirements for the Health Directorate sites.

The CCTV system records high definition images that can be accessed for forensic analysis or to comply with evidence requirements in the courts.

The current incumbent is the Avigilon system that provides the required infrastructure to support existing requirements.

6.2. Architecture

The CCTV architecture consists of high definition IP cameras, both internal and external as required, IP network infrastructure, Network Video Recorders (NVR) which record and store images captured by the cameras, and CCTV monitors (workstations).

The CCTV System architecture will adhere to the Architecture Concept described in the section 3.1.2.

6.2.1. Head-End Infrastructure

The head-end infrastructure consists of NVR and additional storage expansion units which will meet the storage requirements for the site. The NVR and storage expansion units can be hosted at the data centre or within the communications room at the site where CCTV cameras are installed.

The NVR must provide the functionality outlined in the following sections.

6.2.1.1. Network

- Support IP connectivity to the ACT Government network switch; and
- Capable of supporting VLAN to separate CCTV network traffic from other systems.

6.2.1.2. Storage

- Record data, in a high-quality format, that complies with the evidence requirements for court related matters;
- Capable of storing data on the NVR hard disk or on a Storage Area Network (SAN);
- Capable of storing data on a reliable hard drive in a Redundant Array of Independent Disks (RAID) 5 or 6 configuration; and
- Have adequate capacity to store data compliant with the ACT Government CCTV Code of Practice and/or for the length of time that meets the Health Security team requirements.

6.2.1.3. Recording

The following capabilities must be supported:

- Simultaneous recording of images from multiple cameras;
- Capable of supporting local and remote operator access to view live or recorded images;
- Video Analytics;
- High Level Interface;
- Infra-Red;
- Licence Plate recognition – this is a future requirement; and
- Pan, Tilt Zoom/Fixed Camera.

6.2.1.4. Physical Requirements

- Dual redundant hot swappable power supplies; and
- Hot swappable hard drives.

6.2.1.5. Monitoring and Alerts

- The system shall support SNMP; and
- The system must be able to send an alert to nominated personnel when a component fails.

6.2.1.6. Time Synchronisation

- Must be able to synchronise time with the Health Directorate NTP server over the ACT Government network.

6.2.2. Building Infrastructure

The building network infrastructure required to support CCTV camera connectivity to the NVRs will be provided by the ACT Government IP network.

The network switches will provide power to the CCTV cameras over POE+ feature.

6.2.3. Endpoint Devices

The endpoint devices will consist of IP CCTV cameras that will be installed indoors or outdoors. The location and number of cameras required is unique to each site and is determined during the site planning and design stages of each project in conjunction with the Agency Security Advisor and Security Project Manager.

The CCTV cameras will support the features and requirements outlined in the following sections.

6.2.3.1. Network

- Support IP connectivity;
- Capable of supporting VLAN to separate CCTV network traffic from other systems;
- Capable of directly connecting to the ACT Government IP network switches over structured cabling; and
- Capable of leveraging power from POE+ switch ports. No additional power points shall be required by the cameras.

6.2.3.2. Environmental Considerations

- Capable of operating 24 hours a day, 7 days a week in environments which includes varying temperatures and light conditions in both day and night time settings;
- Outdoor cameras must support heating elements for defrosting due to sub zero temperatures; and
- The cameras will be protected from all known environmental conditions experienced in a particular area where they are installed, by suitable housing and accessories.

6.2.3.3. Camera Requirements

- Each camera must support high definition resolution;
- Internal cameras shall be colour 'fixed view' IP cameras with a minimum of 1080p resolution. The requirement for the camera resolution may vary due to the site requirement for higher level of resolution, therefore the project requirements must be clarified prior to proposing a specific camera model;
- External cameras shall be colour either 'fixed view' or Pan Tilt Zoom (PTZ) IP cameras with a minimum of 1080p resolution. The requirement for the camera resolution may vary due to the site requirement for higher level of resolution, therefore the project requirements must be clarified prior to proposing a specific cameras model;
- External cameras must be Infrared (IR) capable and support video analytics functions.
- All PTZ cameras will be fully controllable from the security office enabling a security officer to remotely zoom and focus on a subject or a "live" incident; and
- Based on site specific requirements, the cameras will be protected by suitable vandal resistant camera housings.

6.2.3.4. CCTV Monitoring System Requirements

- In some areas, as a minimum standard, face recognition must be achievable for any person as per the conditions set out in clause 3.7 of the Australian Standard AS 4806.2-2206 – Closed Circuit Television (CCTV) – Application Guidelines;
- For external cameras, the system must support viewing and recognition of car license plates across a car park; and
- The system must be capable of video analytics to support real-time event detection and "object" verification which are the key requirements for safety and surveillance at the Health Directorate sites.

6.3. System Configuration Requirements

6.3.1. Hardware

The NVR must be enterprise grade system that can be rack mounted in a standard data cabinet. It must support the following physical characteristics:

- Dual power supplies; and
- Dual NICs.

6.3.1. Software and Licensing

The software and licensing must comply with the requirements specified in sections 13.14 and **Error! Reference source not found.**.

The system must include software which facilitates NVR administration and viewing of CCTV recorded and live images.

Based on the project requirements, it must also support video analytics, facial recognition and car number plate identification.

6.3.2. Power

All the critical Health Directorate systems are provisioned with UPS support. The backup power for the NVRs shall be supported by the UPS units.

The power requirements of the CCTV infrastructure shall be documented in the HLVD and be provided to DSD Infrastructure solutions architects for UPS sizing during the system design stage of the project.

The CCTV cameras are provided power via PoE+ from the ACT Government network switches. These switches are supported by UPS backup power.

7. Access Control

7.1. Introduction

Electronic Access Control System (EACS) will provide delineation between perimeter, public and non-public zones within a building. It is used to control personnel movement through zoned environments via clearance groups assigned to proximity cards.

The incumbent access control system is a Tyco/Software House C-Cure 9000 Enterprise System, with iStar and APC field devices and which use a client/server model to permit or deny access to personnel through zoned environments.

7.2. Architecture

The existing system complies with the Health Directorate architecture model. This system consists of proximity card reader, building based i-Star and APC door controllers that perform release actions on each connected door and redundant head-end C-Cure servers located in the TCH data centre.

Each i-Star controller is connected to a network switch port. These controllers have network connectivity to the C-Cure servers over a Layer-3 IP network.

The C-Cure servers provide several features such as monitor events, display dynamic views and monitor system activity from a workstation using a C-Cure client or web client.

7.2.1. Head-End Infrastructure

The incumbent access control head-end infrastructure consists of C-Cure 9000 Master Application Servers (MAS) installed in a highly available configuration. The system configurations are updated on this server and distributed to the building-based Satellite Application Servers (SAS) and i-Star controllers over the ACT Government network to multiple ACT Health facilities across the ACT.

Alarms from multiple buildings can be monitored from multiple workstations connected to the security VLAN.

The head-end servers shall provide the functionality outlined in the following sections.

7.2.1.1. Network

- Support IP connectivity;
- Capable of supporting VLAN to separate Access Control network traffic from other systems;
- Support Layer-3 IP network connectivity; and
- Manage entire Health Directorate requirements across onsite and offsite buildings from the head-end central servers.

7.2.1.2. High Availability

- Support highly available servers operating in primary and secondary configuration;
- The primary and secondary servers, individually should be able to support all the Health Directorate buildings;
- The failover from the primary to the secondary should be automatic without any intervention. The vendor should state the length of time taken to failover from primary to secondary system;
- The failback from secondary to primary should be configurable to either automatic or manual mode; and
- The primary and secondary appliances must be capable of synchronising configurations when a change is implemented. The synchronisation should be configurable, which can be automatic or manual.

7.2.1.3. Monitoring and Alerts

- The system must be able to send an alert to the nominated personnel when the secondary appliances assume the role of primary servers;
- The system must support central monitoring of alarms from multiple sites; and
- The system shall support Simple Network Management Protocol.

7.2.1.4. Logging

- Maintain logs which record system errors and events such as date and time of configuration changes, synchronisation status with the secondary system, primary system fail-over to the secondary system etc; and
- The log files must be protected from unauthorised access.

7.2.1.5. Configurations

- Support access control configurations for all Health Directorate sites; and
- Capable of updating access configurations for the building appliances over the ACT Government IP network.

7.2.1.6. Reporting

- Provide comprehensive reporting features which includes at a minimum the number of incidents, the type of incidents, date and time of the incidents; and
- The system must include “pre-configured” and customisable reports.

7.2.1.7. Time Synchronisation

- Must be able to synchronise time with the Health Directorate NTP server over the ACT Government network,

7.2.2. Building Infrastructure

The building infrastructure can consist of one or both of the components as per the following.

7.2.2.1. Building based servers

The architecture of some systems requires hosting of the head end servers in the data centre and the building. These systems use the architecture of master servers located in the data centre and satellite servers located in off campus buildings.

DSD will consider these servers as the head-end server component, in combination with the data centre located servers, of the Three-Tiered Architecture.

The building-based servers will support the same features as the head-end servers located in the data centre.

7.2.2.2. Building based concentrators

Building Concentrators will provide the local building interface between the ACT Government IP network and the system-based distribution network. All the endpoint devices will be connected to the concentrators, which will support the functionality provided to the endpoint devices.

The building infrastructure required to support access control is provided by i-Star and APC controllers located within the communications rooms at each site.

The building concentrators will support the functionality outlined in the following sections.

7.2.2.3. Network

- Support IP connectivity;
- Capable of supporting VLANs to separate Access Control network traffic from other systems; and
- Should be able to connect to the ACT Government IP network switch ports.

7.2.2.4. Configuration

- Each controller should be able to support several multi format proximity card readers;
- Should have on-board memory to store local configurations on the controller; and
- Should support server backup of configuration stored on the controller.

7.2.2.5. Operational Requirement

- Capable of independent operation in the event of loss of connectivity to the master head-end infrastructure. This will include door control, time scheduling and logging of audit trails.

7.2.3. Endpoint Devices

7.2.3.1. Input devices

The input devices will consist of multi format proximity card readers and access cards, proximity sensors and break glass devices (BGD).

7.2.3.1.1. Card Readers

The card readers will support the following features and requirements:

- Proximity readers should be capable of directly connecting to the building electronic access control concentrators or alternatively connected to the ACT Government POE+ network switch port;
- Proximity card reader must be suitable for indoor and outdoor use; and
- Proximity readers should be capable of reading cards from multiple manufacturers.

7.2.3.1.2. Proximity Cards

The proximity access cards will support the following feature:

- The access cards shall be programmable from TCH security office and other security office locations as required.

7.2.3.1.3. Break Glass Devices

The BGD will provide a means of performing door release mechanisms in an emergency. The BGD shall be capable of:

- Resettable “glass” panel;
- Audible local alarm on activation; and
- Displaying an alarm event on the C-CURE 9000 workstations.

7.2.3.1.4. Exit Buttons

The ‘request to exit’ buttons are to be used on the inside of ward double entry automated doors. Door sensors will be connected to the automatic door opener to avoid door damage.

7.2.3.2. Output devices

The output devices will consist of mainly electronic locks and door openers.

7.2.3.2.1. Electronic Locks

The locks will have the following features:

- Standard electronic style locks that are capable of being set as “fail to open” or “fail to lock”;
- Magnetic lock type for double doors that require rigid centre locking capability; and
- Drop locks for bi-directional doors which may be required to maintain fire egress paths.

7.2.3.2.2. Door Openers

Door openers shall be of type “DORMA” allowing automatic opening and closing of large doors, usually double ward doors with a capacity to integrate with door sensors.

7.3. System Configuration Requirements

7.3.1. Hardware

The door controllers should be installed on the communications room wall.

The door controllers should support rechargeable battery backup. The batteries should provide power for at least 4-hours[4].

7.3.2. Software and Licensing

The software and licensing must comply with the requirements specified in sections 13.14 and **Error! Reference source not found.**.

7.3.3. Power

All the critical Health Directorate systems are provisioned with UPS support. The backup power for the head-end and building infrastructure shall be supported by the ICT building UPS units.

The power requirements of the head-end and building infrastructure shall be documented in the HLVD and be provided to DSD Infrastructure solutions architects for UPS sizing during the system design stage of the project.

The power requirements of the card readers are provided by the i-Star and APC controller units hosted in the communication rooms and mounted on walls.

[4] These batteries will only be required on either failure of the units main power supply or failure of the dual UPS supply which will last a minimum of 30mins in the event of mains and essential power feeds failing.

8. Key Management System

The key management system provides secure access control to the data cabinets/racks and any other physical assets. The electronically 'tagged' keys are locked in the key cabinet until released by an authorised user. The users can only remove the keys from the cabinet that they have been granted access. The system also maintains full audit history of all access to the keys stored in the 'key cabinet'.

The current incumbent at TCH and non-acute facilities is the Traka Key Management System.

8.1. Architecture

The key management system should adhere to the architecture proposed in section 3 of this document. The architecture proposes that head-end infrastructure is installed in the data centre. This head-end infrastructure communicates with the building-based concentrator over the ACT Government IP network.

8.1.1. Head-End Infrastructure

The head-end servers/appliances must be able to manage the Traka cabinets located at various Health Directorate sites. The access rights to the keys should be configurable from the CCURE 9000 Electronic Access control system. The CCURE 9000 system must also support a HLI Interface with the Traka Access Management system head-end servers.

Theses appliances should support the functionality outlined in the following sections:

8.1.1.1. Network

- Support IP connectivity to the ACT Government network; and
- Capable of supporting VLAN to separate Key Management System network traffic from other systems.

8.1.1.2. Operational Requirements

- Seamlessly integrate with Traka cabinets without requiring major changes to the existing Traka cabinets;
- High Level Interface with the CCURE 9000 Access Control System for allocation of keys through the Traka Access Control Integration Software;
- Capable of mapping selected credential for use with the Traka cabinet access;
- A multi format card reader will be installed on the door of the Traka cabinet to support dual factor authentication in conjunction with the number pad;
- Creation and assigning of security groups in Traka as required;
- Capable of disabling Traka access for a user or a group of users;
- Real time updates from the head-end server to Traka key cabinet;

- The Traka cabinet must be capable of sending alerts to nominated personnel if the keys are not returned to the device within the nominated timeframes;
- Capable of supporting and displaying Traka alarms and events in real-time; and
- Manage entire Health Directorate requirements across onsite and offsite buildings from a head-end central server.

8.1.1.3. Configurations

- Capable of updating access configurations for the building appliances over the IP network.

8.1.1.4. High Availability

- Support highly available servers operating in primary and secondary configuration;
- The failover from the primary to the secondary should be automatic without any intervention. The vendor should state the length of time taken to failover from primary to secondary system;
- The failback from secondary to primary should be configurable to either automatic or manual mode; and
- The primary and secondary appliances must be capable of synchronising configurations when a change is implemented. The synchronisation should be configurable, which can be automatic or manual.

8.1.1.5. Monitoring and Alerts

- The system must be able to send an alert to the nominated personnel when the secondary appliances assume the role of primary servers; and
- The system shall support Simple Network Management Protocol.

8.1.1.6. Logging

- Maintain logs which record system errors and events such as date and time when configuration changes were made, synchronisation status with the secondary system etc. Additionally, the system must log the event when primary system fails-over to the secondary system; and
- The logs must be secured against unauthorised access.

8.1.1.7. Reports

- The system must provide standard in-built reports. It must also allow customisation of reports.

8.1.1.8. Time Synchronisation

- Must be able to synchronise time with the Health Directorate NTP server over the ACT Government network.

8.1.1.9. Integration

- Must closely integrate with Access Control Head-end servers to maintain a single source for authorisation information.

8.1.2. Building Infrastructure

The building concentrators will provide key control and management at a site. Each site should host a key management cabinet which will "hold" all the keys.

The concentrators will provide the functionality outlined in the following sections.

8.1.2.1. Network

- Should be able to connect to the ACT Government IP network switch ports; and
- Must support access to the head-end servers/appliances over the ACT Government network.

8.1.2.2. System Capability

- Capable of independent operation in the event of loss of connectivity to the head-end infrastructure; and
- Capable of restricting key access to authorised staff only.

8.1.2.3. Integration

- Integrate with the head-end infrastructure over ACT Government IP network.

8.1.2.4. Configurations

- Should have on-board memory to store local configurations on the controller and the concentrators;
- Capable of setting criteria to determine when an alarm should be raised; and
- Capable of raising an alarm and sending it to the nominated personnel based on pre-determined conditions.

8.1.2.5. Audit Log

- Maintain an audit log of key usage clearly identifying the user accessing the key. The audit log should identify when the key was removed and returned to the cabinet; and
- The audit log should only be accessible by the authorised personnel.

8.1.2.6. Reports

- Capable of producing standard in-built reports from the system. The system should also allow customisation of reports.

8.1.2.7. Time Synchronisation

- Must be able to synchronise time with the Health Directorate NTP server over the ACT Government network.

8.1.3. Endpoint Devices

The key fobs are the endpoint devices for this system. The key fobs must support the following functionality:

- Must be compatible with the Traka cabinet; and
- Key fobs should be capable of recharging when replaced in Key cabinet.

8.2. System Configuration Requirements

8.2.1. Hardware

The key cabinets should be installed on a suitable wall in the vicinity of the building entry that has general access available for all users.

An essential GPO and a data point shall be provisioned by the head contractor.

8.2.2. Software and Licensing

The software and licensing must comply with the requirements specified in sections 13.14 and **Error! Reference source not found.**.

8.2.3. Power

All the critical Health Directorate systems are provisioned with UPS support. The backup power for the head-end infrastructure shall be supported by the UPS units.

The power requirements of the head-end and building infrastructure shall be documented in the HLVD and be provided to Shared Services ICT for UPS sizing during the system design stage of the project.

9. Help Points

9.1. Introduction

The Help Point infrastructure is controlled by a single system however it consists of the following functions:

- Consumer Help Point Intercom;
- Lift Emergency Intercom;
- After-hours Building Access Video-com (including CCTV);
- After-hours Ward access Video-com; and
- Public Address (PA) system.

The intercoms provide a means for consumer and visitors to contact, via two-way audio, the local on-campus or designated offsite contracted security guards in emergency situations such as in car parks, walkways and/or stuck in lifts.

The Video-com is used in several ways as per the following:

- Video and audio feed is provided to an AV work station managed by appropriate personnel. Audio only response is provided back to caller; and
- A means for visitors to obtain after-hours access to a building managed through security personnel or access to an after-hours locked ward which is managed by the ward nurse.

The IP Public Address System can be used for either defined (e.g. waiting room) or pervasive (e.g. campus wide) distribution of general hospital announcements, background music or emergency notifications.

9.2. Architecture

This section specifies briefly the architecture that is the preferred option. The current incumbent system is the Jacques platform. The Jacques platform is a pure IP system which complies with the architecture principles mentioned in section 3. As a result of following the pure IP architecture, this system is easy to implement, particularly when the Head-end is in place in an HA configuration. Due to the requirement to be able to route voice calls with given business rules (e.g. redirection of guard desk phone after 4 rings to a designated mobile phone) this system is linked to the Cisco Unified Communications Manager (CUCM). This capability also provides greater flexibility with Lift emergency phones to make use the opportunity to use local or remote security staff (e.g. dependant on time of day) and removes the requirement for installing dedicated copper services for each building.

As a result of being a pure IP system, no building concentrators are required other than the functionality provided by Shared Services ICT switches. It should be noted that some endpoint devices will interact with other endpoint devices to perform certain functions such as door/gate release at an entrance station.

The following diagram, Figure 5, illustrates the help point architecture.

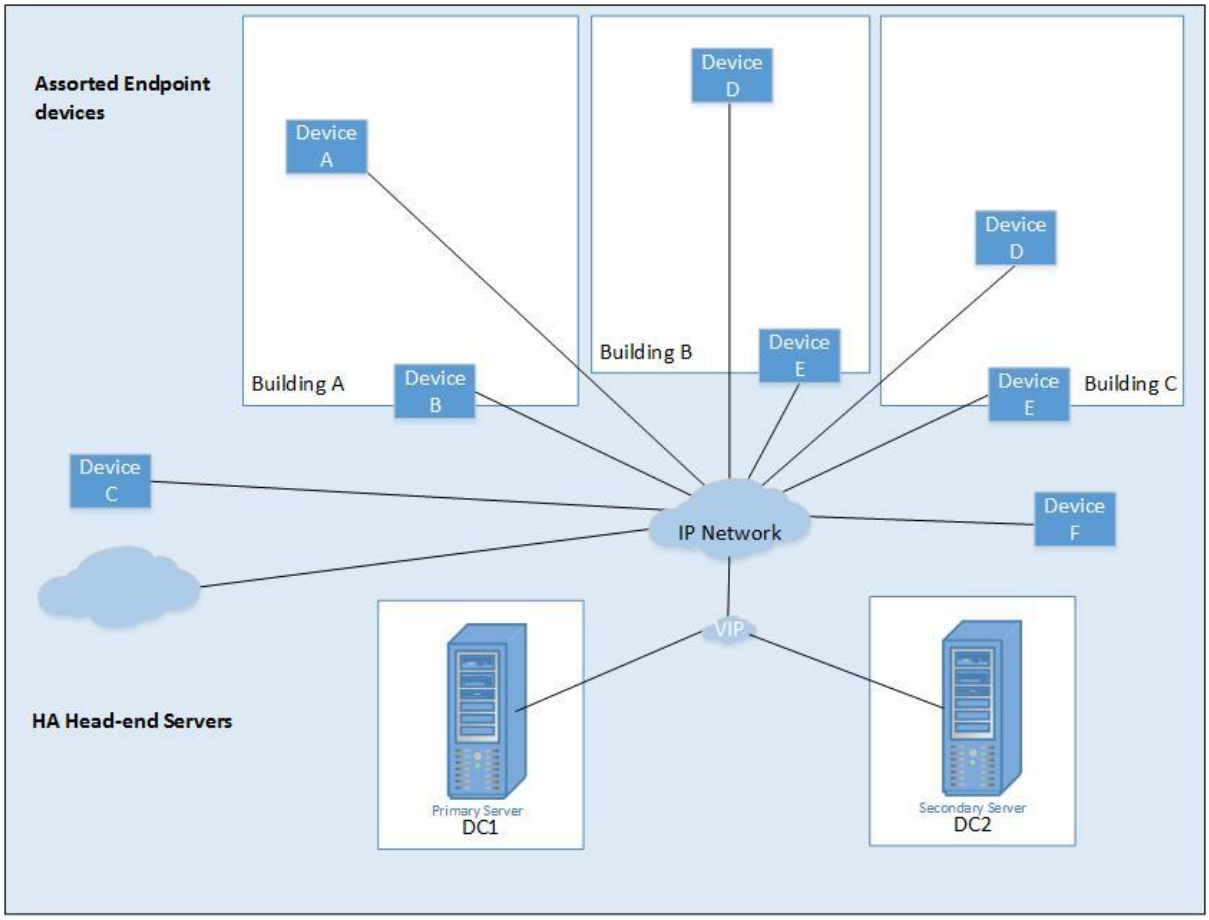

Figure 5 - Help Point Architecture

The following diagram, Figure 6, illustrates various Help Point system components currently used at the Health Directorate and additional component capability.

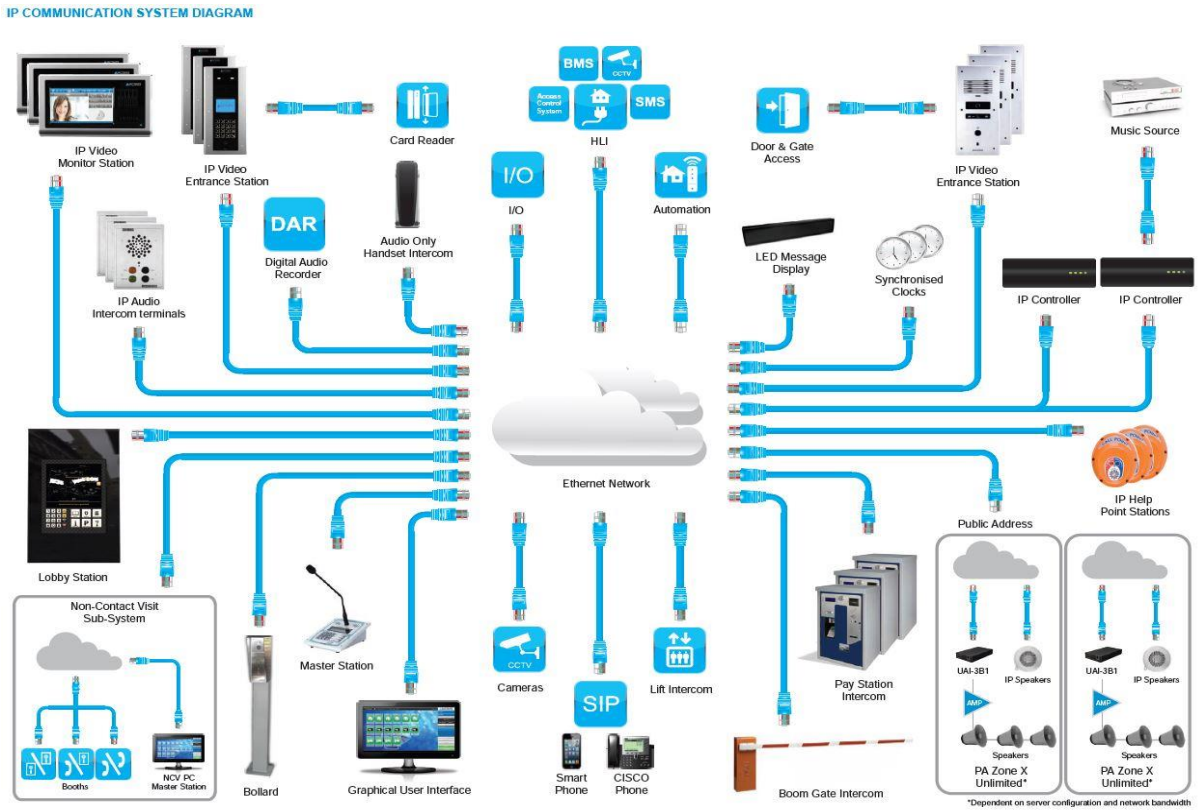

Figure 6 - Help Point system components

9.2.1. Head-End Infrastructure

The head-end infrastructure is expected to be deployed in a HA model as per the architecture principles outlined in section **Error! Reference source not found.**. This i nfrastructure will be located within separate ACT Government data centres that are in geographically disparate locations in Canberra. The data centres have been provisioned with connectivity over Shared Services ICT layer-3 IP network. The primary and secondary head-end infrastructure should be able to communicate over this layer-3 network.

The head-end infrastructure will provide the functionality outlined in the following sections.

9.2.1.1. Network

- Support IP connectivity; and
- Capable of supporting Virtual Local Area Network to separate Help Point network traffic from other systems.

9.2.1.2. High Availability

- The primary and secondary server infrastructure should be able to support the entire Health Directorate requirements. Hence, in the event the primary servers are inoperative, the secondary servers should be capable of supporting the functionality provided by the primary servers;
- The failover from the primary to the secondary should be automatic without any intervention. The vendor should state the length of time taken to failover from primary to secondary system;
- The failback from the secondary to the primary should be configurable to be either manual or automatic;
- The primary and secondary appliances must be capable of synchronising configurations when a change is implemented. The synchronisation should be configurable, which can be automatic or manual; and
- No redundant solution is in place for the Jacques Server.

9.2.1.3. Monitoring and Alerts

- The system must be able to send an alert to the nominated personnel when the secondary appliances assume the role of primary servers; and
- The system shall support Simple Network Management Protocol.

9.2.1.4. Logging

- Maintain logs which record system errors and events such as date and time of configuration changes, synchronisation status with the secondary system, primary system fail-over to the secondary system etc.

9.2.1.5. Reporting

- Capable of producing standard in-built reports from the system. The system should also allow customisation of reports.

9.2.1.6. Time Synchronisation

- Must be able to synchronise time with the Health Directorate NTP server.

9.2.2. Building Concentrators

Building Concentrators are not required in a pure IP network other than the SS-ICT provided IP network switches. All the endpoint devices will be connected to the Floor Distributor network switches, which will support the endpoint devices.

9.2.3. Endpoint Devices

All user endpoint devices will provide two-way full duplex IP voice capabilities between two end devices. Additional capability within the servers which will allow full Session Initiation Integration (SIP) integration with the CUCM to provide further flexibility to reroute calls on no answer or after certain hours.

Some devices will have further capabilities such as one-way video or remote door release functions etc. whereas other non-user endpoint devices will just allow one way audio distribution (e.g. PA).

The endpoint devices can be described under the following four headings.

9.2.3.1. Consumer/Visitor Help Point Intercom

Multiple help points will be located around the premises at strategic points, both internally and external. These will be located as designated by local or consultant safety advisors during the planning stage, for the purpose of providing an instant alert and two-way voice accesses to security personnel.

The system should also provide specific location information of the originating help call, so security personnel can be deployed quickly if required to assist or call back to a station. Points must be continually monitored with IP heart beat by the server to validate operation readiness.

9.2.3.2. Lift Emergency Intercom

The lift solution uses a two-part endpoint device. This is because of the continual movement of the lift and therefore cables over drag chain attachment. The lift intercom is connected via a more robust cable and interfaces to an IP device in the lift machine room. From the IP device the call can be directed to a local Jacques voice station or be (re)directed (via rules e.g. A/H) to an external number via the SIP trunks to the CUCM.

9.2.3.3. After-hours Building Access Video-com (+CCTV)

Each building requiring after-hours access will be provisioned with a single access (i.e. pushing button always connects to a static Video intercom) and a nearby CCTV camera facing the entry door. Consumers or visitors requiring after-hour's access will push a single button that will give them voice access to the security guard on duty. Simultaneously, the device will also enable a high-level instruction to the CCTV system to bring the footage (of the associated CCTV camera) to the forefront of the security offices CCTV viewing PC for comparative reference via a HLI with Jacques and Avigilon CCTV.

The CCTV will alert the security guard of additional persons that may not be visible from the Video-com camera which has a relatively narrow field of view. If the security guard

is confident of a secure entry he can remotely, via high level interface, open the door via a soft key button on the master intercom console.

9.2.3.4. After-hours Ward access Video-com

Each ward area requiring A/H access will be provisioned with a single access (i.e. pushing button always connects to a specific Video intercom) or a multi button intercom with in-built camera. Consumers or visitors requiring after-hour's access will push a button that will give them voice access to the ward CNC or another nominated person on duty. The device will also enable the CNC or the nominated person to release the door remotely via a soft key release button on the master intercom console (requires a relay installation from the designated door from CCURE to Jacques to allow for the high-level system instruction).

9.2.3.5. Public Address System

Each building/ward/public area requiring PA capability will be configured in one of two ways:

- Each location requiring individual speaker addressable audio requirements will be provided with a POE IP speaker. A standard fixed data outlet will be required in the ceiling within 5m of this position; to be patched at ceiling/speaker installation and shall be yellow in colour; and
- Each location requiring only large area addressable audio requirements (i.e. a group of speakers receiving the same audio) multiple speakers will have standard speakers installed in a daisy chain fashion back to an IP/AMP device. (May be possible to leverage from the Fire Speaker systems, for further consideration for campus PA).

This will allow operator audio stations and automated response recordings to selected general (e.g. Campus wide) or specific (e.g. waiting room) PA areas for general and emergency announcements.

9.3. System Configuration Requirements

The system will be configured by the provider who will submit a High-Level Vendor Design for approval by Shared Services ICT. Shared Services ICT will in return, provide the required network configuration detail including IP numbers, VLAN and VRF information. The Help Points/PA being generally an IP system, will operate in the following ways:

- Point to point fixed – single source, single destination (including destination redirection e.g. Help points and A/H building entry Video intercom);
- Point to point selectable – single source, variable single destinations (e.g. A/H Ward entry video intercoms); and

- Point to multi point – single source to multiple destinations (e.g. Operator audio station to selected PA areas.

9.3.1. Hardware

There is a requirement within the Shared Services ICT to provision all systems, where available, on virtual systems.

The appliances shall be capable of running on physical servers or on virtual platforms as a preference.

9.3.2. Software and Licensing

The software and licensing must comply with the requirements specified in sections **Error! R eference source not found.** and **Error! Reference source not found.**.

9.3.3. Power

All the critical Health Directorate systems are provisioned with dual UPS support.

The Help Point central system shall be provided with connectivity to the UPS units. All other endpoint devices will be either POE devices or be provided power from a local essential supply.

10. Intrusion Detection

10.1. Introduction

The Intrusion Detection System (IDS) is used to monitor unauthorised access to premises and restrict access to nominated zones such as Pharmacy, Radiology, Laboratories etc.

A trigger of an alarm is reported back to onsite security centre / personnel and/or can also be reported offsite to a third party contracted licensed security organisation for action that may redirect to the Australian Federal Police (AFP) dependant on established protocols.

10.2. Architecture

The architecture will comply with the three-tiered hierarchical modular approach discussed in section **Error! Reference source not found.**.

The current encumbent system whilst following this approach is a conglomorate of different systems with several systems performing the same functions and therefore is in the process of design consolidation.

Going forward, all new designs will follow the above architecture and consolidate functions at the building concentrator level. Whilst the system may contain components from different manufacturers, it will have a single enterprise architecture implementation to meet system functional requirements.

10.2.1. Head-End Infrastructure

The IDS currently integrates at the endpoint/building concentrator layer with the Access Control head-end infrastructure and therefore this system provides the primary and secondary head-end infrastructure to communicate over the layer-3 network. Refer to the section 7.2.1 Head-End Infrastructure.

10.2.2. Building Concentrators

The IDS will use the access control Building Concentrators (iSTAR) to provide the local building interface between the ACT Government IP network and the system-based distribution network. All the IDS endpoint devices will be connected to the concentrators, which will support the required functionality from the endpoint devices.

The building concentrators will support the following functionality:

- These appliances must be capable of supporting the site functionality locally in the event the network connection between the building-based appliances and the head-end infrastructure fails or is unavailable; and
- The appliances should support physical device hardware resiliency by providing:

- Dual power supplies (either two Power Supply Units (PSUs), one on each UPS feed or one PSU on UPS power and second on an internal battery of 4 hours capacity or greater);
- Dual NICs or alternatively be able, on network failure, to maintain a local database and continue to log all intrusion alerts for a period of 48 hrs until Head-end system communication is restored; and
- Provide a local building alarm (strobe and sound) during network failure.

10.2.3. Endpoint Devices

The endpoint devices, such as hardwired Passive Infrared (PIR) detectors, Seismic sensors and Remote Administration System (RAS) keypads, will be provisioned within the building based on the requirements provided by the business. These devices will connect to the building-based concentrators via direct cabled low-level interfaces.

10.3. System Configuration Requirements

The intrusion detection system shall leverage the Access Control head-end servers.

There is a potential that multiple endpoint devices are used with the Access Control system. These devices include but are not limited to the following:

- PIR (detection of body heat);
- Door reed switch;
- Door break glass point;
- Seismic sensors (detection of vibration-e.g. an attempt or success in breaking glass); and
- RAS keypad (alert on unsuccessful attempts to access via a keypad sequence).

10.3.1. Software and Licensing

The software and licensing must comply with the requirements specified in sections 13.14 and **Error! Reference source not found.**.

10.3.2. Network

The endpoint devices will connect to the building concentrator via direct cabled low-level interfaces.

10.3.3. Power

All the critical Health Directorate systems are provisioned with dual UPS support.

The power requirements of the building-based infrastructure shall be documented in the HLVD by the head contractor and provided to DSD Infrastructure solution architects for UPS sizing during the system design stage of the project.

The endpoint devices will be powered from direct cabled low-level interfaces.

11. Security System Integration

11.1. Introduction

This section outlines the integration of the various security system components. Additionally, it describes integration with the central Messaging platform. The security systems considered are:

- Access Control;
- Intrusion Detection and Alarms;
- Staff Duress Fixed;
- Staff Duress Wireless;
- Help Points and Public Address;
- CCTV; and
- Key safes.

11.2. Architecture

The architecture for the integration of each system above involves the interaction of these systems with the two main head-end systems which are Electronic Access Control System and Help Points. Business rules and requirements should dictate the required interactions of each system. All security systems and subsystems shall be capable of interacting with one another either Low Level Control (LLC) e.g. dry contact or High-Level Control (HLC) e.g. data over RS485 or IP over Ethernet or both.

Electronic Access Control System will provide the general Head-end processing required to process with various events e.g. data validation (e.g. NFC card), reading state changes (e.g. sensor triggering), enabling latching/de-latching (e.g. door release/locking). It will also support the following integration activities:

- LLC relay connection to old paging hardware (incumbent – will be replaced with an IP paging solution); and
- HLC (e.g. send alarm/response location information to the messaging engine to distribute messages to response teams on fixed and/or mobile devices).

Help Point and Public Address system will provide the Head-end processing required to present IP audio, voice and video-coms to selected end devices (e.g. control consoles, PA speakers) for interaction with consumers and visitors A/H. (e.g. external or ward door entry or audio announcements), but will also support the following integration activities:

- HLC from control console performs auto door release (via IP to door endpoint unit), then via LLC to Access Control door endpoint equipment to activate door release/open;

- HLC (trigger state from door intercom activation to enable CCTV system to bring up (Hot zoom window on guard screen) associated CCTV camera monitoring entry door; and
- Access control (smart card reader) at Key safe location (in conjunction with keypad - 2FI) will release key safe door. Future integration will see closer HLC between the access control head-end and the key safe management database to enable single source of truth data.

11.3. Integration of Lift Communication with Various Systems

The Lift Control System will interface and/or integrate with the following systems:

- Access Control - Tyco C-Cure;
- RTLS - Ekahau;
- Nursecall – Austco Tacera;
- Emergency Intercom – Jacques;
- BMCS (Possibly the transient communicator); and
- AGV Control head-end.

An example of potential level of integration required for Code Blue is mentioned below:

- Report each Lift Floor location;
- Receive and act on RTLS instructions to move a lift to a specific floor;
- Advise Access Control to lock lift access at designated level, until a specified ID is swiped, opening doors and releasing lift;
- On release move lift directly (ignoring other requests), to new (emergency) floor as designated by Nursecall; and
- On arrival release lift for general service.

To enable the remote lift access, e.g. (Urgent patient delivery to theatres or AGV lift request):

- Receive and act on RTLS instructions from AGV control to move a lift to a specific floor; and
- Receive notification of handset location from RTLS and move nearest lift to a designated level.

Each lift will also have an emergency intercom that communicates with the lift control room over the highly available ACT Health MGN compliant IP network. The emergency intercoms within the lifts will be managed over IP from the emergency intercom head-end appliances. The head-end system must have rule-based capabilities for diverting the call via the existing VoIP system to several designated end points.

12. Network Requirements

12.1. Wired Network

The Health Directorate has been provisioned with a network architecture that is compliant with the MGN to support Health critical systems. The architecture mitigates against the risk of a single network component failure resulting in the loss of connectivity for these Health systems.

The network has been provisioned with 10 Gbps OM4 multimode (MTP +elite) fibre connections between the access layer Floor Distributor (FD) switches and aggregation layer Building Distributor (BD) switches. Similarly, 10 Gbps OS2 single mode (MTP +elite) fibre connections are provisioned between BD and Campus Core switches.

Each FD switch is connected to both the BD switches using Multi EtherChannel (MEC) feature. Both the links within a MEC are active with traffic traversing across both the links. In the event of a link failure, the network traffic continues to access the Health systems over the remaining active link.

The systems must support the following:

- Capable of connecting to the Ethernet switches over Cat 6_A cabling;
- Capable of leveraging POE+ where applicable; and
- Head end and Building Concentrators shall have components that will support IP network.

12.2. Wireless Network

The wireless head-end infrastructure has been implemented to support wireless services required in various ACT Health buildings. A wireless services block has been created that hosts the head-end wireless network infrastructure in two separate locations, TCH Buildings 1 and10. Each location includes wireless and security components to support the wireless connectivity required from each site.

The head-end infrastructure currently implemented must be leveraged for the wireless network architecture within Health Directorate buildings.

The site based wireless infrastructure will consist of WAPs, which will be provisioned by the Shared Services ICT. A wireless 'Desktop Design' is conducted by Shared Services ICT. This survey outlines the location of WAPs within the building. If RTLS functionality is required, an additional RTLS specific survey is conducted by a company that specialises in wireless surveys to ensure WAPs are located in optimal locations. The Health Security systems that require wireless network access are expected to leverage these WAPs.

13. Vendor Requirements

The following requirements are expected to be supported by each security system mentioned in this document.

13.1. Installation Support

The Health critical systems have an element of complexity that necessitates suitable planning for the installation, configuration, integration with other systems and testing. These systems also include several vendors that need to be coordinated to achieve optimal implementation results and the completion timeframes.

The vendor must identify and document the implementation plan including:

- Installation and configuration processes;
- Rollback process;
- Mechanisms for integration with other systems;
- Tools available to verify the system implementation;
- Tools available to assist in system fault diagnosis;
- Processes to upgrade the system software; and
- Processes to upgrade and/or replace hardware.

13.2. Detailed Design

A detailed design shall be prepared and submitted four weeks prior to installation of the solution. The design should provide and document all system and connectivity details to enable DSD Infrastructure solutions architect to review and incorporate the information in Conceptual design. Additionally, this information should include enough content for WHOG change management approvals.

At the completion of Operational Commissioning, the design document incorporating as-built information must be provided to DSD. All drawings for the system must be provided in both PDF and CAD (if appropriate) format. The documentation must be stored in the Operational Maintenance Manuals (OMM) on completion of the project.

13.3. Training

The Health critical systems are implemented with an objective that these systems will assist staff with the quality of care they provide to consumers. This implies that in addition to installing, customising and testing the systems, it will be necessary to have relevant core processes and procedures in place to achieve the expected results. Therefore, staff will need training in the use of the systems that will be installed at the site.

The vendor must identify and document the following:

- Initial user training requirements to effectively use the system;
- Initial system administrator training requirements to effectively manage the system; and
- The amount of ongoing training for the users and system administrators.

13.4. Backup and Recovery Capability

There is mandatory requirement for having consistent and reliable backups for the systems. The systems shall backup key information for recovery purposes in the event of a catastrophic appliance failure. The scope for the backups includes, but not limited to the following:

- All the folders, files and databases required to recover the system to a state prior to the appliance failure;
- System configuration files;
- System log files; and
- Operating system.

The vendor must identify and document the following:

- The information that must be backed up for system recovery following a catastrophic failure of the system appliance;
- The frequency of the backups;
- Whether full backups or incremental backups will be completed;
- How the system will be recovered from the data that has been backed up; and
- The length of time taken to recover the system from the backup data and for the system to be ready for production.

13.5. Logging Capability

The system must have an automatic logging capability (i.e. recording all data), which complies with the DSD requirements and good governance. At a minimum, the following logging capabilities must be provided by the system:

- The logs must be available for auditing and problem isolation;
- Access to logs must be restricted to authorised personnel. Access should be logged and must be auditable;
- Logs must include a date and timestamp;
- Logs must record various elements and enough detail that explain the event;
- The systems must have adequate storage space for logs; and
- The system must be capable of forwarding logs to a separate central log management server.

13.6. System Monitoring Capacity and Capability

An effective monitoring and event management strategy is crucial to a successful deployment. The existing Health Directorate network infrastructure is monitored by a centralised monitoring system.

The vendor and the Directorate must be able to monitor the systems mentioned in this document. The monitoring strategy must identify and document the following key points:

- Details of how the system will be monitored;
- The components that will be monitored. At a minimum, it is expected the following components will be monitored:
  - Resource utilisation such as CPU and memory utilisation;
  - Disk status including available disk space and other threshold information;
  - Replication activity including status whether replication is running and the state of synchronisation; and
  - Security information including access to the system.
- Monitoring and analysis tools available to monitor the system;
- Any diagnostic tools available to assist with problem isolation and resolution;
- Tools available to support system usage statistics to assist with cost allocation to different business units;
- Triggers that will raise an alarm or an event notification when monitoring the system; and
- The personnel responsible for responding and resolving the problem which raised the alarm including the vendor's escalation process.

13.7. Management Capability

The system management will form a critical aspect for the ongoing optimal operation of the security systems discussed in this document.

The systems must support the following management capabilities:

- Local site management; and
- Remote management from TCH security office or other security office workstations.

In order to plan for the system management, the following requirements must be identified and documented:

- The ongoing resource requirements for effective system management;
- Post implementation system validation requirements whether manual or automated; and
- The frequencies of ongoing system validation to ensure business units maintain a high level of confidence in the system operation and performance.

Key Performance Indicators (KPI) will need to be developed and formally agreed to, ensuring the system is performing in compliance with the expected criteria. These KPIs and associated formulas will be developed collaboratively between Health Directorate and the vendor.

13.8. Capacity Strategy

In order to manage current and future business requirements in a cost-effective manner, capacity management forms a critical component of the system life-cycle. The security systems must provide adequate capacity to meet current anticipated requirements. However, the vendor must identify and document a capacity strategy that provides details of:

- The capacity and scalability of the proposed system including the:
  - Number of concurrent "transactions" supported by the system;
  - Amount of CPU, memory and other system parameter utilisation initially expected from the proposed system;
- Strategies to provide additional capacity as the business requirements increase the requirements for the system; and
- Provide a Total Cost of Ownership (TCO) analysis for a 5-year period.

13.9. System Roadmap

The vendors shall provide a technology roadmap that outlines short-term and long-term direction of the technology solution that is being provided. The information will assist Health Directorate in understanding the technology direction a product is expected to take over a period of time.

The roadmap must identify and document the following:

- The product that will be the focus of the roadmap. Each component in the tiered architecture potentially may have a different product cycle;
- The features that will be addressed by the roadmap; and
- The timelines for any technology changes.

13.10. Network Time Protocol

Network Time Protocol is essential for the systems to maintain consistent time with other devices within an enterprise. The consistent time management with other devices assists with event correlation between different machines.

As various systems are integrated at the Health Directorate, in the event of problem resolution, consistent clock on the appliance/server can be crucial. The Health systems shall support NTP to synchronise appliance/server time with the Shared Services ICT NTP server.

13.11. Maintenance & Support

The vendor shall provide product warranty for the systems.

The Contractor shall maintain a 24-hour emergency service and advise the nominated person of the emergency telephone number.

- The timeframe for the vendor support personnel to arrive onsite for system support will be negotiated between the vendor and the Health Directorate;
- If any required repairs cannot be carried out within 12 hours, the Nominated Authorised Person shall be notified; and
- On completion of a breakdown call out service the technician shall enter details of work performed into the site logbook and provide detailed reports to the building manager and critical incident manager or the delegate.

The Contractor shall provide a 24 hour "Hot Line" Operational Support telephone contact number. Respondents are to confirm the following details:

- Level of after sales service available;
- Qualification of technicians who will service equipment; and
- Availability of spare parts and whether stocks are maintained in the ACT.

The Agency Security Advisor and Agency Security Officer will require operator training and the contractor should allow for equipment location orientation and user training to the security team as requested.

Based on the criticality of the system, a 24 x 7 system vendor support will be required. The support personnel must be based in Canberra. The vendor will identify and document the following:

- The maintenance and support model, including ongoing license costs; and
- Schedule of fees for any other costs that may be applicable.

13.12. System Testing

The Health security systems must undergo extensive testing prior to release into the production environment. The vendor responsible for each system must provide a detailed test and integration plan to the DSD Infrastructure solutions architects for review prior to commencement of testing. The test scenarios must outline the tests that will ensure the system complies with all the functional requirements.

At a high level the test and integration plan must identify and document the following:

- Functionality testing. Provide comprehensive test cases which will verify the functionality provided by the system;
- GUI software testing. In the event the system provides a GUI interface, the test cases must be provided to verify functional aspects of GUI testing;

- Security testing. These test cases must verify compliance with the access restrictions to the system;
- High availability testing. These test cases must verify failover capability of various components of the system;
- Capacity testing. The test cases must outline the capacity testing methodology. Additionally, if any automated tools are available, these must be included in the test cases; and
- Integration testing. These test cases must detail testing that will be conducted to ensure integration with other systems complies with the business requirements.

13.13. Business Unit Validation

In addition to system testing as mentioned in the previous section, there is a requirement for the client to review and validate that the system implementation complies with the business unit's needs.

The validation by the business unit should include the following:

- Develop and document a test plan to validate the business requirements that have been agreed with the users;
- Review the test results from the vendor system testing and provide feedback to the vendor via the Shared Services ICT project manager;
- Conduct functional and non-functional testing to ensure the system complies with the business needs;
- Perform system performance validation; and
- Provide a report of the test results to the Shared Services ICT project manager.

13.14. Software

The operating software needs to be maintained at no greater than n-1 where n is the latest version.

All software updates shall be performed by the contracted company. The updates should be pre-tested in the Shared Services ICT provided TEST environment, where available.

All updates to the live production environment shall be done strictly under the Shared Services ICT approved change control methodology.

13.15. Licensing

An enterprise approach should be followed for any license requirements. Consideration should be given to the annual licensing requirement, allowing for a single purchase of a larger quantity of licences thereby reducing individual license costs.

A centralised enterprise approach will provide an additional benefit of avoiding any licensing issues during commissioning of a system.

The vendors should provide the Health Directorate with the licensing requirements for their systems.

13.16. Certificate of Compliance

Certify on completion that the works comply with the requirements of the Manufacturers Recommendations and any other applicable rules or regulations. The certificate shall be in a form acceptable to the responsible Authority and shall be addressed to them.

Vendors that are non-compliant with these specifications are required to complete the Departures document which identifies deviations from the specifications.

13.17. Remote Vendor Access

The currently deployed infrastructure forms a conduit on which communication with the external parties will traverse. Remote Vendor Access (RVA) relies on the various elements within the network to facilitate the required communications path. This means access policy alterations i.e. firewall changes, will be required at the inbound access point to the network.

RVA is provided on case-by-case basis to the vendor equipment as required by each project in compliance with the remote vendor access policy.

Any vendor with existing remote access to their head-end infrastructure will not require additional access. However, the vendor will need to request any additional access to new infrastructure.

13.18. Model of Care

The Canberra Hospital and Health Services will rely on various information technology-based systems to provide the Model of Care (MoC) to the patients. In order to support the MoC, the business units, in consultation with the vendor, will develop test cases to ensure the system complies with the functionality expected by the user. In addition to the test cases, a compliance checklist must be documented for system vendor compliance.

At a minimum, these test cases should ensure the following criteria are addressed:

- The functional requirements for the system are tested. For example, if a duress button is pressed, what notifications are expected to take place;
- The expected performance of each system is tested. For example, if a duress button is pressed, what is the timeframe for the notifications to be received by the responders; and
- Non-functional requirements are tested.

Appendix A – Document Details

References

Following is a list of Standards applicable at the time of writing this document. However, it is incumbent on the vendors to use the latest Standard in each category prior to system implementation.

- AS 2201 SET:2008 Intruder Alarm Systems;
- AS 3745-2010 Planning for emergencies in facilities;
- AS 4083-2010 Planning for emergencies – Health Care Facilities;
- AS/NZS ISO 31000:2009 Risk Management;
- AS 4421:2011 Guards and patrol security services;
- AS 4485.1 Security for Health Care Facilities General Requirements;
- AS 4485.2 Security for Health Care Facilities Procedures Guide;
- AS 4806 SET:.2008 – Closed Circuit Television (CCTV);
- Any other Australian Standards, not listed above, that are relevant to these systems;
- All installed devices must meet all required Australian standards;
- ACT Government CCTV Code of Practice;
- ACT Government Protective Security Policy Framework; and
- Australasian Healthcare Facility Guidelines.

Abbreviated terms and definitions

Glossary of Term	Definition
ACT	Australian Capital Territory
AFP	Australian Federal Police
BD	Building Distributor
BGD	Break Glass Device
CCTV	Closed Circuit Television
CHS	Canberra Health Services
CUCM	Cisco Unified Communications Manager
DALI	Digital Addressable Lighting Interface
DSD	Digital Solutions Division
FD	Floor Distributor
FIP	Fire Information Panel
Gbps	Gigabits per second
GUI	Graphical User Interface
HA	High Availability
HLC	High Level Control
HLVD	High Level Vendor Design
ICT	Information and Communications Technology

IDS	Intrusion Detection System
IP	Internet Protocol
KPI	Key Performance Indicator
LLC	Low Level Control
MEC	Multi EtherChannel
MGN	Medical Grade Network
MoC	Model of Care
NIC	Network Interface Card
NTP	Network Time Protocol
NVR	Network Video Recorder
OMM	Operational Maintenance Manual
PA	Public Address
PIR	Passive Infrared
POE+	Power over Ethernet Plus
PSU	Power Supply Unit
PTZ	Pan Tilt Zoom
RAID	Redundant Array of Independent Disks
RAS	Remote Administration System
RTLS	Real Time Location System
RVA	Remote Vendor Access
SAN	Storage Area Network
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
TCH	The Canberra Hospital
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VIP	Virtual Internet Protocol
VLAN	Virtual Local Area Network
VoWiFi	Voice over WiFi
WAP	Wireless Access Point

Table 1: Glossary

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

Amendment history

Version	Author	Summary of Changes	Date
0.1	Nitin Saxena & David Richards	Initial draft	19/02/2015
0.2	Nitin Saxena	Inclusions to several section	22/02/2015

0.25	Nitin Saxena	Include Key Management system	24/02/2015
0.26	David Richards	Include Help Point section	25/02/2015
0.27	Nitin Saxena	Review and minor changes to some sections	26/02/2015
0.3	David Richards	Include a section on Integration of systems	26/02/2015
0.4	Nitin Saxena	Updates following peer review	27/02/2015
0.5	Nitin Saxena	Updates following security peer review	02/03/2015
0.6	Nitin Saxena	Include diagram for second type of architecture	03/03/2015
0.7	Nitin Saxena	Updates to include key vendor considerations	01/04/2015
0.8	Nitin Saxena	Updates following feedback from program manager.	07/04/2015
0.9	Nitin Saxena	Further updates to the vendor considerations	10/04/2015
1.0	Nitin Saxena	Final released version	15/04/2015
1.1	Nitin Saxena	The following updates have been applied: Change 'Edge Device' to 'Endpoint Device' based on feedback. Add battery life requirement. Timeframe for Duress alarm display on annunciator. Added a section on Personnel Certification.	08/05/2015
1.2	Nitin Saxena	Incorporate feedback from Security.	12/05/2015
1.3	Nitin Saxena	Incorporate minor feedback from the Program Manager.	25/05/2015
1.4	Nitin Saxena	Update several sections to include the latest information. Update formatting of the document.	08/08/2017
1.5	Raj Mohan	New template update	09/05/2018
1.6	Dario Gomes	Updated sections on Mobile wireless duress, CCTV, Access control, Key management system, Help points and Intrusion detection	01/06/18
1.7	David Richards	Accept changes	02/07/2018

2019.1.8	Nitin Saxena	Update ‘Compliance Requirements’ page. Review the document and update as necessary.	04/10/2019
2019.2.0	CIO to endorse after review and approve for release as 2.0	Sandra Cook a/g CIO	09/10/2019