

Southern Ute Shared Services (SUSS) Network Standards

7. Access Control Systems (ACS)

Preferred Standards (current environment)

- **Controllers:** Mercury-based (Open Options platform) preferred.
- **Management software:** DNA Fusion (existing environment).
- **Readers:** HID multi-technology readers (DESFire capable).
- **Credential standard:** DESFire EV3 with custom encryption (SUIT-managed).

Capability Requirements

- Open, non-proprietary controller hardware supporting multi-vendor reader/credential interoperability (e.g., OSDP).
- Enterprise-class management software supporting licensing for doors, clients, integrations, and software maintenance.
- Encrypted, high-security smart credentials with internally managed keys; migration to DESFire credentials required.
- Support for future multi-factor authentication at controlled locations.
- **Budgetary note:** Credential migration includes a standard of 3 badge printers (~\$130K budgetary).

Controlled Access Locations

- **Exterior doors:** Card reader + keypad (future MFA capability).
- **Interior vestibules:** Standard card reader; must remain secured when exterior doors are scheduled unlocked.
- **IT / MDF / IDF rooms:** Card reader + keypad.
- **Sensitive storage (documents, records):** Card reader + keypad.
- **Department offices:** Standard card reader.
- **Perimeter gates (motorized):** Keypad reader, LPR integration, and long-range reader support.

System Functionality

- First valid badge swipe must disarm the intrusion system; auto-arm on schedule.
- All readers must support HID encryption or SUIT custom encryption.
- All doors must include a Door Position Switch (DPS) and Request-to-Exit (REX), integrated where possible.

Power & Monitoring

- Minimum 4-hour battery backup for controllers and power supplies; 3-year battery replacement cycle.
- Power loss (AC or battery) must generate an alarm and alert the centralized distribution, with recovery notification.

Life Safety & Emergency

- Magnetic locks must release upon fire alarm activation.
- Knox Box access required (24/7); must not expire or require renewal for long-term use.

Lockdown & Maintenance

- **Soft lockdown:** Restricts general access while maintaining controlled movement.
- **Hard lockdown:** Full facility lockdown; access restricted to authorized personnel and first responders only.
- **Annual testing:** Door lock/unlock functionality, sensor performance, and battery health.

8. Video Surveillance Systems (VSS)

Preferred Standards (current environment)

- **VMS:** Milestone (Care+ licensing per camera).
- **Cameras:** Axis, Avigilon, or Bosch.
- **Recording environment:** Windows-based Milestone servers, virtualized (SUSS standard).

Capability Requirements

- Open, ONVIF-compliant cameras and VMS to avoid single-vendor lock-in.
- Enterprise storage (NAS standard) with defined redundancy and capacity for retention targets.
- Virtualized, enterprise-managed recording hosts aligned to server lifecycle.

Lifecycle & Retention

- Camera replacement cycle: 7 years; server/host replacement: 5–7 years.
- Minimum retention 30–90 days based on risk level and site type; critical areas may require extended retention.

Performance Standards

- Interior ≥ 2 MP; exterior ≥ 5 MP; entrances 4K required.
- ONVIF compliance required; multi-lens cameras required (no fisheye).

Coverage Requirements

- All perimeter doors (interior + exterior views); full exterior and parking coverage.
- Interior coverage: IT/server rooms, secured storage, hallways, common areas, elevator lobbies, reception, and public-access spaces.

Advanced Capabilities & Connectivity

- AI/edge analytics where applicable; LPR at all entry/exit points; proactive alerting (notification profiles); monitoring of known problem areas.
- Support for cellular (e.g., T-Mobile) and satellite backup (e.g., Starlink); remote cameras may use SD-card edge storage where needed.

9. Intrusion Detection & Duress Systems

Preferred Standards (current environment)

- **Head-end:** Bosch.
- **Devices:** Bosch or approved equivalent.
- **Wireless:** Inovonics.

Capability Requirements

- Enterprise-monitored intrusion head-end with reliable wireless device support and tamper/supervision reporting.
- Integration with access control for auto-disarm on first valid badge and scheduled auto-arm.

Deployment & Duress

- Motion detection and door contacts at all critical areas; glass-break sensors where risk is elevated; keypads at main entrances.
- Duress/panic required at reception areas and public interaction points.
- Annual testing required for all devices.

10. Fire Alarm Systems

Preferred Standards (current environment)

- **Head-end:** Potter. **Devices:** Potter SLC. **Notification:** Potter or System Sensor. **Communication:** AES required.

Capability & Compliance Requirements

- Systems must meet all applicable codes and Authority Having Jurisdiction (AHJ) requirements.
- Panel replacement lifecycle: 10–15 years.

Detection Requirements

- Sprinkler monitoring; voice evacuation where required by code; pull stations at all exits.
- Smoke detection in common areas, mechanical/electrical/IT rooms, and fire panel locations.
- Heat detection in kitchens/cooking areas; CO detection where fuel-burning appliances exist.
- Duct detection for HVAC > 2000 CFM (supply + return).