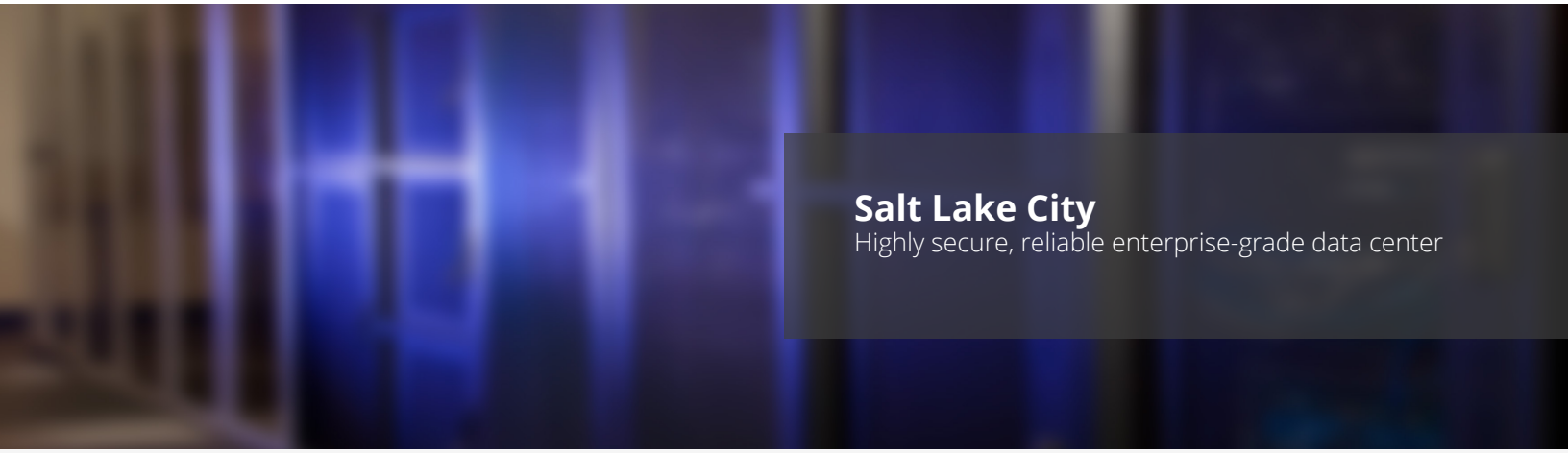
lume



Physical Security Controls

Based on ISO 27001 Standards and Controls

- The data center is physically segregated and requires access privileges based on permission rules and policies.
- Only authorized users can request changes to data center user access listings.
- The facility is outfitted with several strategic man traps throughout the data center.
- Key card/biometric systems are used to control and restrict access to the data center and all sensitive areas. Each user is assigned a card with a unique identification number that is recorded each time the card/biometrics are used.
- To access the raised floor space of the data centers, customers must pass through at least three secure doors, the last of which requiring two-factor authentication.
- Access to all cabinets, cages and network infrastructure are secured through physical locks, card readers and/or biometric scanners and restricted to appropriate personnel.
- All employee key card access is appropriately disabled by Operations personnel upon notification of termination.
- Annual audits of all employee, customer and contractor card access to the data center are performed to validate the ongoing appropriateness of access.
- Visitors are required to check in at the security reception desk with a government issued photo ID and be escorted by data center personnel.
- The delivery/loading zone is isolated from the raised-floor area with secure key card readers. When a scheduled delivery arrives, data center personnel unlock applicable exterior delivery/loading zone gates and/or doors and monitor the personnel involved.
- Security cameras with motion detection are located throughout the facility. Video feeds are displayed and monitored continuously by Operations personnel. A minimum of 30-day archive of video activity is retained.
- Security staff are present 24/7/365 and perform periodic security walkthroughs during each shift.