Critical Infrastructure and Access to SMUD Property

SMUD, as a public power utility, owns and operates facilities that compose part of our national critical infrastructure. In order to ensure the safety of its employees, customers, suppliers and the public and to protect SMUD assets and ability to provide public power, SMUD shall control access to its facilities and infrastructure in compliance with applicable North American Electric Reliability Corporation (NERC) Reliability standards and Nuclear Regulatory Commission (NRC) regulations.

When necessary due to safety or security concerns, Security Operations may restrict access to SMUD grounds and facilities.

Employee Awareness and Behavior

SMUD believes that all employees play a crucial role in SMUD's ability to protect people and energy supply when they support Security Operations in their efforts to maintain a secure environment.

Employees shall behave in accordance with SMUD access control policies and procedures at all times. Employees should remain aware of others in their vicinity, be prepared to respond to verbal directions of security personnel, and report any concerns or suspicious activity to Security Operations.

Local Law Enforcement

When appropriate due to a security threat, Security Operations shall notify and assist local law enforcement in accordance with established procedures and training. All employees must follow instructions of local law enforcement when an incident occurs that involves law enforcement.

Implementation

The Chief Workforce & Technology Officer or designee shall establish controls for employee and public access to SMUD facilities and infrastructure, including procedures and training as deemed necessary to guide security personnel in the performance of their duties.

Related References

NERC Critical Infrastructure Protection Standards
CIP-001 – Sabotage Reporting

Administrative Policies
AP 05.03.02 – Background Investigations
AP 06.02.02 – Emergency Preparedness
AP 06.03.02 – Violence Prevention in the Workplace
AP 08.01.01 – CIP Cyber Security

Management Procedures

MP 06.02.02.100 – Emergency Action Plan
MP 06.03.02.100 – Threat Assessment & Action
MP 06.03.01.100 – Identification Access Badges
MP 08.01.01.100 – CIP Cyber Security
MP 08.01.01.100 – Access to Critical Cyber Assets