Riverside Public Utilities

Physical Security Policy

Prepared By: _____
Rajiv Butala – Senior Electrical Engineer

Approved By: _____
Ed Cortez – Principal Electrical Engineer

Approved By: _____
George Hanson – Assistant General Manager

Approved By: _____
Mujib Lodhi – Assistant General Manager

Approved By: _____
Kevin Milligan – Deputy General Manager

Approved By: _____
Girish Balachandran – Public Utilities General Manager

PURPOSE & SCOPE

The purpose of this Policy is to establish standards for asset protection, physical security, loss prevention, and continuity of operations for the electric and communication system including Fiber Optic Cable network, Computer Network, SONET Multiplexing System, Microwave and Radio systems owned and operated by Riverside Public Utilities. The Policy:

- Establishes the foundation and minimum standards for planning, evaluating, implementing, and sustaining a Physical Security Program for RPU;
- Specifies the duties of personnel specifically responsible for implementing the RPU Physical Security program, and;
- Defines employee actions and behaviors necessary to support the physical security of RPU facilities.

PHYSICAL SECURITY PROGRAM

Physical security is defined as that part of security concerned with active and passive measures for preventing unauthorized access to secured assets and employee work areas. Effective physical security includes safeguarding these secured assets, and employee work areas against harm, sabotage, damage, and theft. Management shall establish, implement and sustain an effective physical security program, which shall include measures for the following:

- **Integration -** Effective integration of physical security into day-to-day RPU operations without disrupting them.
- **Standards & Procedures -** Establishing security standards and procedures, including operating procedures, emergency response procedures, and incident recovery procedures, which specify appropriate actions to be taken by all personnel, but especially those personnel involved with physical security of RPU systems and equipment, and ensuring that these procedures are being complied with and are effective.
- **Controls -** Establishing and implementing appropriate controls for access to critical facilities and restricted areas, including employee identification badges, keys and other access tools.
- **Deterrence –** Employing and maintaining effective physical deterrence measures, including enclosures, barriers, locks, illumination, and signage as appropriate and needed.

- **Electronic Security –** Employing effective electronic security measures, including systems, which deter, detect, report, and monitor unauthorized access to critical facilities. This also includes procedures for communicating and reporting intrusions to appropriate response forces.

- **Force Security –** Employing such force security assets and measures as may be necessary and appropriate, including personnel whose duties may include security oversight, access control, security system operation, surveillance, patrol or response to security incidents.

- **Performance Measurement -** Measurement and regular reviews of security performance to determine whether changes to policies, procedures, systems, equipment or personnel are warranted.

- **Training –** Effective communication of security policies and procedures to employees, contractors, vendors and visitors. Incorporating security into new employee orientation, sustaining security awareness, and providing training where needed.

- **Reporting –** Recording, reporting, and trending security data, especially security incident data, security system maintenance data, and performance measures.

- **Coordination -** Coordination of efforts of all personnel and organizations, which play an active role in physical security of the RPU.

- **Liaison –** Establishing relationships, communications channels and regular contact with local law enforcement officials, private security companies or other organizations on which RPU will rely for response to security incidents and other security matters.

- **Communication –** Establishing communications protocols for quick and effective dissemination of information affecting physical security, such as police intelligence regarding criminal or terrorist activity or threats, FBI or Homeland Security bulletins or threat advisories, and serious security incidents.

- **Compliance –** Compliance with and conformance to applicable federal, state and local codes and requirements, and with City of Riverside policies.

CONTROLLED ACCESS AREAS

Management shall designate those facilities to which access shall be controlled. In general, controlled access facilities shall be designated as *Protected Facilities*, *Restricted Areas*, *Employee Work Areas or Limited Access Areas*.

Protected Facilities are those facilities which house or support systems, equipment and other assets, which, if destroyed, damaged, degraded, lost, or otherwise rendered unavailable for use or service would:

- Seriously degrade RPU's ability to serve a significant portion of its load or significant numbers of its customers;
- Seriously diminish the reliability, availability, stability, or operability of the RPU's electric system;
- Seriously degrade RPU's ability to operate the communication system including Fiber Optic cable network, SONET multiplexing system, Microwave and Radio system that carries voice, data and video signals for internal and external customers
- Have a serious detrimental financial impact on the City of Riverside or the customers depending on RPU's Electric or Communication system
- Compromise confidential information travelling over the RPU communication system including Fiber Optic cable network, SONET multiplexing system, Microwave and Radio system;
- Create a serious risk to the safety or health of employees or the public.

Among those facilities designated as Protected Facilities are:

- Generating plants,
- Electric substations,
- Control facilities,
- Vital communications facilities including Fiber Optic Cable terminating enclosures, and
- Vital operations facilities.

Only authorized employees and other personnel whose work requires access shall be allowed unescorted access to Protected Facilities.

Space within Protected Facilities shall be reserved for the facilities' specific purpose, and shall not be used for storage of non-essential equipment or materials, which may attract thieves, other criminals, or may contribute to fire hazards.

Restricted Areas shall include hazardous materials storage and processing areas, control centers, data centers, computer rooms, telephone closets, switchgear, energized equipment enclosures, fiber optic cable vaults, SONET multiplexing system racks, network router and hub rooms, microwave and radio system shelters, voicemail system rooms, and other such areas containing those facilities, that if damaged, destroyed or tampered with, would disrupt normal RPU's operation and/or endanger personnel.

Only those employees and other personnel whose work requires access to *Protected Facilities* and *Restricted Areas* shall be authorized for unescorted access to these facilities pertaining to their job duties.

Limited Access Areas shall include vital communications facilities including fiber optic cable terminating enclosures, SONET multiplexing system racks, network router and hub rooms, and other such areas containing facilities that are collocated on internal or external customer's premise. If these communications facilities are damaged, destroyed, or tampered with, they could disrupt normal RPU's operation, its internal and external customer's normal operation, or endanger critical information.

RPU will terminate fiber optic cable strands designated for customer's use only at that customer's premise. RPU will not terminate fiber strands used anywhere else in the fiber optic cable system at customer's premise. Use of physically separate fiber strands will ensure cyber and physical security of RPU and customer data.

RPU-owned SONET multiplexing system nodes, network router and hub, and other such systems that are collocated on internal or external customer's premise shall be configured on a separate data pipe terminating on physically separate data port(s).

RPU will maintain enclosure with tamperproof locking mechanisms to secure access to RPU-owned assets.

Customers will be required to enforce Physical Security Policies similar to or better than RPU's Physical Security Policy as a requirement for services. Only those employees and other personnel whose work requires access to *Protected Facilities* and *Restricted Areas* shall be authorized for unescorted access to these facilities pertaining to their job duties.

Employee Work Areas shall include offices, shops, and other non-public areas in which RPU employees and contractors regularly work. Unescorted access to *Employee Work Areas* by persons other than employees shall be limited and controlled.

ACCESS CONTROL

For *Protected Facilities*, *Restricted Areas* and *Limited Access Areas*, unescorted access shall be restricted to those personnel for whom access has been specifically authorized. In general, non-authorized personnel entering *Protected Facilities, Restricted Areas* and *Limited Access Areas* shall be escorted by an employee who holds authorized access to those areas.

Access to *Employee Work Areas* shall be limited to employees and other authorized personnel. For situations in which full-time escort is not practical, unescorted access to *Employee Work Areas* shall require temporary authorization by a supervisor or other employee who is specifically authorized to grant unescorted access. This employee shall be responsible for periodic monitoring of the status and actions of the non-employee during the time such unescorted access is granted.

ACCESS CONTROL & TRACKING MEASURES

Management shall restrict access authority, so that each employee or other authorized person shall have authorized access only to those areas and facilities necessary to perform his or her assigned duties. Each employee's access authorization level shall be recorded, and such records shall be maintained and updated regularly.

Access media (keys, electronic access cards and other access tools) shall be programmed and distributed to authorized users according to the levels of access which are necessary for their assigned duties as determined by management.

Each user's authentication factors shall be unique, and each access terminal (electronic card reader, keypad, etc.) shall be able to identify each user by those factors, verify access authorization, and log user's identity and time of access, such logs to be maintained for future review and reference.

A visitor’s logbook shall be maintained at each facility’s entrance. All visitors and employees not specifically authorized to access the facility must sign in and sign out in the logbook.

As a normal practice, Utilities Dispatch will be informed via telephone or radio when an employee/visitor enters and exits an RPU facility.

SECURITY PROCEDURES

Management shall establish procedures for implementation of the RPU Physical Security Program. Minimum standards for Security Procedures shall provide for:

- Effective deterrence and defeat of intruders and attackers.
- Rapid assessment of alarms received from unattended facilities;
- Dissemination of intruder information to responder forces;
- Rapid deployment of responder force personnel;
- Normal operation which does not disrupt day-to-day RPU operations, and;
- Regular measurement and review of Physical Security Program performance.

PROGRAM OVERSIGHT AND MANAGEMENT

Physical security at Riverside Public Utilities is the responsibility of every employee, but the ultimate responsibility for management and oversight of physical security belongs to the RPU Assistant General Manager, whose responsibility it shall be to:

- **Establish Requirements -** Determine physical security requirements, and make periodic reviews to determine whether requirements have changed;
- **Establish Programs –** Direct the staff to establish physical security programs and procedures which support established policy;
- **Monitor Implementation -** Ensure that those programs and procedures are appropriately and effectively implemented;
- **Measure Performance -** Measure physical security performance and effect changes where performance is not acceptable;

- **Direct Security Operations -** Appoint personnel as needed to execute day-to-day physical security operational duties and support the Assistant General Manager in fulfilling his or her physical security responsibilities.

- **Oversee & Manage -** Provide for overall management and oversight of all activities, expenditures and operations associated with physical security.

Physical Security Coordination – The Assistant General Manager shall appoint a single employee who shall be assigned to execute the Physical Security Program at the Assistant General Manager's direction, monitor the Program's performance, provide regular performance reports and timely incident reports to the Assistant General Manager, and recommend changes or improvements where they the need for them may be indicated. These duties may be a collateral duty and performed in addition to regular duties. This employee shall hereinafter be referred to by the functional title *Senior Manager*. Specific duties, at the direction of the Assistant General Manager, shall include:

- **Coordination –** Oversight and coordination of all day-to-day physical security functions and activities as directed by the Assistant General Manager.

- **Collection, Review & Reporting –** Receiving and reviewing security performance measurements data, incident reports, security system inspection and maintenance reports and other pertinent physical security information, and reporting results to the Assistant General Manager.

- **Coordination & Liaison –** Establishing and sustaining communications with local law enforcement and other outside organizations that play a role in effective Physical Security.

- **Special Assignments –** Execution of special assignments related to physical security as directed by the Assistant General Manager.

Access Control Administration – A single employee shall be assigned to administer RPUs access control program and activities. These duties may be a collateral duty and be performed in addition to regular duties.

Security System Operation – The Senior Manager shall determine the means by which the physical security system will be operated and monitored. The party or parties to whom this responsibility is delegated shall hereinafter be referred to by the functional title of *Security System Operator*, and shall execute the following duties:

- **Alarm Assessment & Communication**
  - Making prompt assessment of security alarms to determine their nature and potential threats to security, and
  - **N**otifying responder forces and other appropriate personnel when a threat is verified.

- **Logging & Reporting**
  - Maintaining a log of physical security system operations, alarms, anomalies, perimeter breaches and suspicious operations,
    - Failures of the system to perform properly and adequately shall also be included in the log and report.
  - Sending the log to the Physical Security Coordinator at midnight each night.

Security Asset Maintenance – Substation maintenance and electronic technician personnel shall, in addition to their regular responsibilities, be responsible for ensuring correct operation of Physical Security systems assets at the substations. Specific duties include:

- **Inspection –** During regular substation and communication facilities inspections, inspect enclosures, barriers, gates, signs, locks and other deterrence measures, and record their conditions and any noted deficiencies.

- **Operability Checks –** During routine substation and communication facilities inspections, verify that Physical Security System components are operational and functioning properly; record results and any noted deficiencies.

- **Maintenance –** As required, test, adjust, calibrate, repair, service, replace and otherwise maintain Physical Security System systems and components to ensure optimal performance.

- **Reporting –** Send copies of physical security system and component test, inspection and maintenance data collected and recorded by Technicians to the Physical Security Coordinator. Ensure that deficiencies are followed up with a Work Order or other similar repair process.

GENERAL REQUIREMENTS FOR EMPLOYEES

All RPU employees/contractors/vendors/visitors, not just those who are directly involved in the implementation of the RPU Physical Security Program, are responsible for supporting and complying with the RPU Physical Security Policy. Following are specific compliance requirements, which apply, to all employees/contractors/vendors and visitors on RPU property and facilities:

- The lending of keys, identification badges, or electronic access media, and/or the sharing of password/PIN information is strictly prohibited.

- The intentional and unauthorized defeat of any Physical Security asset or alarm function, including fences, gates, locks, access control devices and other assets, is specifically prohibited.

- Employees shall challenge any unescorted persons within the boundaries of a *Protected Facility, Restricted Area* or *Employee Work Site* who does not display proper identification. Employees shall ask unauthorized, unescorted personnel to leave the work site and shall immediately notify supervision when such persons refuse to comply.

- Employees shall not take unauthorized personnel or non-employees into a *Protected Facility, Restricted Area*, or *Employee Work Area* without either obtaining proper authorization or identification for the person or, when authorization and identification procedures are impractical, obtaining supervisory approval.