Security Access Policy

Tier I - Organizational

Revision Date: 5 / 15 / 2020 Effective Date: / /

Scope:

Tier	Affected Divisions / Departments
Tier I	x All (EWEB)
Tier II	☐ Multiple Divisions and/or Departments, or within a Division or Department

All operational policies are organizationally supported, governed, and enforced; see the Operational Policy for additional details.

Revision History

Revision	Author / Editor	Date	Description
00	Lisa Krentz	5/15/2020	Policy Origination

Description *(Roles & Responsibilities, Requirements or Standards, References, Process Descriptions, Impacts)*

As a publicly owned utility, the Eugene Water & Electric Board (EWEB) is committed to ensuring the continued delivery of safe and reliable power and water to our community. The safety, security, and efficient operations of our facilities provides the foundation for the workforce to meet our responsibility to our customers and community at large. The utility holds employees accountable to enterprise-wide policies and procedures that impact all employees, contractors, visitors, and guests.

These rules were adopted to establish guidelines for all applicable persons accessing and using EWEB facilities at the Roosevelt Operations Center (ROC) and the Headquarters (HQ) building, including offices, common areas, outbuildings, storage yards, and other workspaces. All EWEB employees, contractors, vendors, and visitors will acknowledge their understanding and commitment to uphold this policy prior to working in or around EWEB facilities.

Roles and Responsibilities:

A. The Executive Team (ET) shall establish strategic goals for operational policies, advise Managers/Supervisors on developing/implementing procedures, and set enforcement guidelines. The ET shall provide final approval for all Operational Policies prior to them taking effect and shall approve any change.
B. Managers shall have the responsibility for ensuring continuity of this policy between all divisions and for providing guidance to their personnel regarding exceptions due to documented emergent needs or circumstances, and for enforcement action for policy violations.

C. Supervisors shall have the responsibility of communicating and enforcing the policy provisions within their workgroups, including addressing witnessed or reported policy violations.
D. Security department personnel shall have the responsibility of immediate enforcement of this policy and for reporting violations of the policy to appropriate supervisors and managers. Security will conduct initial training on access control requirements during the badging process, and will provide a copy of this policy to all persons receiving an electronic access ID badge. Security will remain a resource for questions or concerns regarding access control requirements and will conduct retraining or deliver appropriate messaging when substantive modifications to the policy are made.
E. Gatekeepers are specified EWEB employees who maintain access control authority for sensitive and regulated workspaces. Gatekeepers must be consulted prior to any person obtaining access permission and subsequent access levels added to their electronic access ID badge. Gatekeepers may deny access to any person who lack a legitimate business need, or persons who have had access revoked for any reason.
F. All employees shall be required to strictly adhere to this policy and to promote the positive attributes of a safe and secure working environment. Employees may choose to assist others by respectfully pointing out actions or conditions violating the principles or spirit and intent of this policy, or they should use their chain of command to report egregious or repetitive violations.
G. Contractors and visitors must abide by all EWEB policies and procedures when working at or visiting EWEB facilities. Contract administrators, site contacts, and EWEB employees hosting visitors are responsible for ensuring the understanding of and compliance with EWEB policies. Concerns or questions should be routed through their Contract Administrator or site contact.

Facility Access and Security

EWEB is committed to providing safe and secure buildings, workspaces, and common areas for business purposes, which requires reasonable provisions for access control and responsible use of the facilities. Security and personal safety is the responsibility of every individual. By adhering to security requirements you are contributing to protecting yourself, your co-workers, property, and the critical infrastructure we support for our community. The following procedures must be followed by all who use the facilities:

A. All employees, contractors, and authorized visitors must display their EWEB issued electronic access ID badge or visitor sticker at all times.
    a. If performing a function where wearing the badge will create an unsafe condition or hazard, the badge may be temporarily removed. When the safety-sensitive situation has been resolved, the badge must again be displayed.
B. Electronic access ID badges are issued at the ROC Operations Building, room 135, by appointment only. Instructions for completing an electronic Physical Access Request (PAR) form can found on the EWEB Security SharePoint Page at: https://ewshare.ewebnetwork.net/es/physsec/SitePages/Access_Control.aspx. The PAR must be routed through one's department supervisor or contract administrator to review access requirements and permissions. Security will create an individual cardholder account and arrange for a badging appointment within two business days of receiving the completed PAR form.
C. All employees and credentialed contractors or visitors must use their electronic access ID badge when entering the ROC Operations Building, Warehouse Building, and Fleet Building; and when entering the HQ South or North Buildings.

D. General access includes only common areas and certain exterior doors. Additional access permissions must be requested through one's department supervisor and be granted by the workspace gatekeeper.
E. Every person entering a space with an electronically controlled door lock must present their badge each time they enter the door. Escorted visitors may be signed in as required.
F. Employees who have been authorized by their supervisor to access the ROC yard in their personal vehicle must present their badge at the card reader for access.
G. No *tailgating* is allowed – each person must use their own badge at the appropriate card reader.
H. No person shall share or loan their electronic access ID badge.
I. Employees who forget their badge shall contact Security at **541-685-7911** to arrange access and be issued a temporary badge, if warranted.
J. If an electronic access ID badge is lost or stolen, Security must immediately be notified by telephone at **541-685-7911** and via email at **Security@EWEB.org** to deactivate the badge and arrange for replacement. Replacement badge requests must be routed through an individual's department supervisor or contract administrator. For a broken or non-functional badge, please call Security to arrange for replacement. Replacement badge appointments will occur within two business days, based upon Security activity levels and other responsibilities.
K. Any person discovered circumventing or avoiding access control measures will be reported to supervisors and managers for their prompt and appropriate corrective action.

Exterior doors shall remain secure and electronically locked at all times except when entering/exiting or loading/unloading materials. Propping or blocking open exterior doors disrupts the critical air handling systems of the facility and can cause poor air quality within the building or damage air handling equipment. Roll up shop bay doors may not be left open unless employees are working in the immediate area. Windows may be opened while employees are working inside, but must be closed and locked at the end of the workday.

Propping or blocking open of any door with a card reader is prohibited without notifying Security in advance. Card reader equipped doors are alarmed and nuisance alarms caused by propping doors can disrupt the Security team from their duties. Doors should be propped only when necessary to facilitate moving materials in or out of the building. Once the propped door is closed, notify Security so they can resume normal alarm monitoring for that point.

Use of Parking Lots and Yard

The ROC yard is a dynamic area with frequent vehicle and apparatus traffic at all hours. Accessing the yard requires awareness and adherence to additional safety protocols to ensure security and safety of our personnel, equipment, and materials. Each EWEB vehicle is equipped with a device that will automatically open the ROC yard drive through gate. The gate can also be accessed by employees in non-EWEB vehicles by presenting their EWEB electronic access ID badge at the card reader. Employees requiring access to the yard in non-EWEB vehicles must be authorized by their supervisor as having a business need for accessing the yard. Employees shall work, park, and utilize their assigned departmental areas of the yard. When employees who accessed the yard in their personal vehicle transfer to an EWEB vehicle, the personal vehicle should be parked in the vacated spot to minimize crowding in the yard.

No vehicles, trailers, or drop boxes may be parked or left in hash-marked areas or fire lanes. Immediate drop off and pick up of large or bulky materials is permitted adjacent to the buildings, but the vehicle must be immediately relocated when the activity is complete. Any variance to this policy must be authorized by the Facilities Maintenance Team.

Employee and Visitor parking lots at the ROC and HQ facilities are controlled and limited to those personnel who are on duty or otherwise on EWEB business. All employees, interns, and contract staff must display a valid EWEB parking permit when using EWEB parking lots. Permits are assigned based upon the vehicle's federal fuel efficiency rating. Blue permits are issued for standard vehicles and trucks, Green permits for fuel efficient rated vehicles, and Red permits for Compact vehicles. Only vehicles with Green permits may be parked in Fuel Efficient spaces; only vehicles with Red permits may park in Compact spaces. If an employee changes vehicles, they must update their vehicle permit information with Security. Carpool/Vanpool spaces should not be used for any other purposes. Employees shall not park in Visitor spots, to ensure our guests have adequate parking near the building. No personal trailers shall be parked or stored in parking lots or in the yard.

For the security and safety of personal vehicles, overnight parking is discouraged in the employee parking areas. EWEB is not responsible for damage, theft, or loss to any personal vehicles or property left in any EWEB parking area. Arrangements for overnight parking for those with a business need can be made by notifying Security ahead of time. Employees with a business need, such as traveling, standing duty as a First Responder, or an overnight shift may arrange to leave their personal vehicle in the designated Overnight Parking stalls in the ROC yard, or in the secure yard at HQ.

No materials, vehicles, or rubbish may be staged or stored within six feet of the perimeter fence. Security personnel and Facilities Maintenance staff require unhindered access to the fence to deter, detect, and investigate breaches to the security fence and criminal activity.

Accessing Facilities outside Normal Work Hours

The security of our employees, protection of customer's confidential information, and protection of the physical assets of the Utility are strengthened by a robust access control and monitoring system. Beyond normal staffing hours, there are departments with 24/7 operations that use certain portions of the ROC and HQ buildings. To provide for the safety of employees working 24/7 functions, access to EWEB buildings outside normal working hours will be controlled. Employees shall adhere to their departmental scheduling for use of the facilities. If you have a valid business need to enter the facility between 9:00pm and 4:00am, notify Security. Department functions or scheduled activities outside of normal working hours must be communicated to Security by a department Lead, Supervisor, or Manager, so they can arrange appropriate access to those employees. Emergency call-outs and trouble-shooting functions are exceptions, though a courtesy call to Security is requested.

NERC-CIP/ RSAP Access Protocols

Only approved and cleared employees and specified contractors may access Restricted Security Access Portal (RSAP) and North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) spaces. Special background screening and permission from the workspace Gatekeeper are required before such access levels will be added to an electronic access ID badge. Any visitor or contractor with a business need may be granted temporary access to those spaces and must be escorted by a qualified EWEB employee. An access control logbook located inside the RSAP or NERC-CIP portal must be filled out by the escorting EWEB employee and will clearly indicate the name of the escorted individual, the purpose of the visit, and in/out times. Certain Contractors who have a business need, have undergone additional background checks, and completed the required NERC-CIP training, may be granted unescorted access by the Gatekeeper for that space. Under no circumstances may a Contractor escort any person into an RSAP or NERC-CIP space.

Contractors/Vendors/Visitors

Contractors, vendors, and visitors are valued guests in our EWEB facilities, but appropriate security access and facility use controls must be followed to protect employees, customer information, and physical assets. Contractors who have received EWEB Contractor ID Badges will be allowed access only to specific portions of the facilities. Any access needs outside their contract scope must be approved by their EWEB Contract Administrator and those changes must be communicated to Security. Under no circumstances may a Contractor escort any person into an RSAP or NERC-CIP space.

Departments Leads and Supervisors hosting Contractors must notify Security of any required access to the ROC yard. The Contractor shall press the intercom button at the ROC yard visitor pedestal and await authorization from the Duty Security Officer to enter the vehicle gates. No tailgating or gate sensor bypassing is allowed.

Regularly scheduled Contractors and Vendors who require access into buildings may be granted named electronic access ID badge accounts with their access controls programmed to their badge. Hosting department Supervisors must complete a Physical Access Request form for their contractor or vendor and submit the form to Security for processing.

Visitors to the ROC Operations Building must be received by their EWEB host at the entry doors before access into the buildings. The EWEB host shall ensure the visitor first signs in through the Lobby Guard system for a temporary visitor sticker. Training in use of the Lobby Guard system is available from Security. Visitors to ROC or HQ facilities must be escorted and monitored by their EWEB host. EWEB departments hosting large groups or conferences should contact Security at least 48-hours in advance for special access and visitor logging arrangements.

Visitors to the HQ building shall enter the main lobby and use the Lobby Guard system to request access. Their EWEB host will meet them in the lobby to escort them through the facility.

Policy Revisions/Adherence

The aforementioned procedures are subject to modification as required for operational needs. In most cases, employees will follow the policies and self-correct any time they fall out of these policies. On occasion, employees may be approached by other employees or Supervisors to remind them to follow the Security Access Policy. Failure to comply with this policy will be treated as a policy violation, in accordance with EWEB's Standards of Conduct (200.40) and Discipline and Discharge policies (200.05).

Approval

I agree to support and enforce the policy, procedure, standard, and/or method described herein.

DocuSigned by:
Frank Lawson
Frank Lawson – General Manager

DocuSigned by:
Susan Ackerman
Susan Ackerman – Chief Energy Officer

DocuSigned by:
Deborah Hart
Deborah Hart – Chief Financial Officer

DocuSigned by:
Lena Kostopulos
Lena Kostopulos – Chief HR Officer

DocuSigned by:
Julie McGaughey
Julie McGaughey – Chief Customer Officer

DocuSigned by:
Rod Price
Rod Price – Chief Engineering & Operations Officer

Special Instructions *(Communications, implantation, notes)*