HUMAN RESOURCES
POLICIES AND PROCEDURES

Policy:	Computing Policy	
Date: November 2, 2017	**Revision Date:**	**Approved by:** Human Resources

I. PURPOSE AND SCOPE

This policy governs District technology and network use. It applies to all workers (full-time, contractor, temporary, etc.) who access technology or network resources provided by Eastern Municipal Water District. Violation of this policy may lead to revocation of system privileges and/or disciplinary action. The scope of this policy does not limit employees' rights to engage in legitimate concerted labor related activities as defined by law.

II. POLICY STATEMENTS

Eligible employees may be issued a computer or mobile device(s) if the nature of the work and/or the need to maintain contact with the District and effectively complete assigned work is best accomplished through the use of technology. Eligibility will be determined by the employee's department head or Executive Management.

III. SECURITY

Users are the District's most important security safeguard.

- Never share any computer or system passwords or leave an unlocked computer unattended.
- Never open suspicious files, e-mail messages, or web links.
  If in doubt, call the helpdesk for guidance or contact the originating user by phone to validate the authenticity of the communication.

The following must be reported in-person or via phone to the Information Systems helpdesk and your direct supervisor or manager as soon as you are aware of:

- Lost, stolen, or compromised device
- Lost or stolen sensitive customer, employee, or District information
- Inadvertent disclosure of privileged information to unauthorized parties
- Unauthorized system or network access

Specifics of computer or network security issues should be only discussed with Information Systems or Risk Management, since disclosure could result in a serious breach.

IV. SOFTWARE AND CLOUD SERVICES

Staff shall not engage or commit the District to any software or cloud service without first seeking a review and receiving approval from Information Systems and the Purchasing and Contracts Department; to include proof-of-concept or trial installations.

Software license tracking is provided by Information Systems. Software not managed or tracked by Information Systems may be removed during regular software compliance audits.

V. LIMITATIONS OF USE

Users shall abide by all applicable laws and adhere to the District's Ethics and Harassment Policies at all times.

District-issued technology (e.g., telephones, cellular devices, computers, laptops, tablets) are intended to be used for business purposes (e.g., checking District e-mails, capturing field notes, etc.).

- District issued e-mail addresses are to be used for District business only and should not be used for registration to websites or services for personal use.
- Non-exempt employees should not check, read, send, or respond to work-related e-mails outside their normal work schedule unless specifically authorized based on job duties or management direction.
- Modifying, disabling, or tampering with any settings or systems that could present a security risk to the District is strictly prohibited.
- Accessing District systems or information not directly related to a user's work is strictly prohibited. Unauthorized review, dissemination of files or passwords, damage to systems or software, removal of files or programs, or improper use of information contained in any system may be grounds for disciplinary and/or legal action.
- Personal use of the Internet is authorized as long as it is not excessive or inappropriate and occurs during personal time (e.g., meal periods, breaks) provided it does not present a security risk, incur any cost or burden on the District, disrupt District operations, or violate any District policy. Other than "Open Internet" Wi-Fi, personal devices (e.g., cellular devices, computers, laptops, tablets) are not permitted on any District network and these devices may not be used to remotely access or control any District system.
- District technology may never be used for personal gain or an employee's personal, religious, political, commercial ventures, or any activity that would cause an obstruction or disruption to District work.
- ***Use of technology, even personal devices used for District business, may be subject to discovery under the California Public Records Act.***

VI. SPECIAL ACCESS REQUESTS

Authorization must be obtained from Information Systems before any contractor or visitor device may be connected to any District network. Notice must be given to the Information Systems helpdesk in advance of the planned engagement.

Remote access to District systems must be granted by a Department Director. No District computers or networks may be remotely accessed by users who have not received prior authorization.

Use of hosted document sharing platforms (e.g. Box, Dropbox, Google Drive, etc.) must be granted by a Director-level employee and receive further approval by Information Systems. No District computers or networks may be configured for real-time document synchronization to these platforms.

VII. PRIVACY

The District reserves the right to examine any information transmitted or stored on District technology. Such examination may occur at any time, and may or may not include advance notification to the employee. If examination is performed as part of an investigation, it will be coordinated with the employee's department head and the Human Resources department.

Privacy of personal communications using District technology cannot be expected. District-related communication via personal technology may also be examined in the course of an investigation, a Public Records Act request, or other litigation.

The District may wipe devices or erase any data stored on District-issued technology.

VIII. RECORDS MANAGEMENT/RETENTION

All stored or transmitted data is the property of the District.

Records related to ongoing or potential litigation or any investigation must be retained and cannot be disposed of, even if the retention period has been met, except as advised by legal counsel. Please refer to the District's Records Retention Policy and current Memorandum of Understanding for details.

Employees should contact their supervisor or Records Management for further assistance.

IX. USE OF TECHNOLOGY WHILE DRIVING

Employees shall comply with all applicable laws and regulations regarding the use of mobile technology while operating a motor vehicle.

Please refer to the District's Vehicle Use Policy for further guidance.

X. TERMINATION OF USE

The District may revoke access to District technology at any time. All District-issued devices must be returned in working order prior to separation from District employment.

ACCESS REQUEST FOR EMPLOYEES

I have read and agree to the requirements and expectations of the Computing and Network Resources Policy for the Eastern Municipal Water District. I have received a copy of the policy and agree to abide by the policy and guidelines as a condition of my employment and my continuing employment at the Eastern Municipal Water District.

I understand that if I have questions, any time, regarding this policy, I will consult with my immediate supervisor or Human Resources Department.

_____ _____

Name (please print clearly) Signature

_____ _____

Employee Number Date

ACCESS REQUEST FOR NON-EMPLOYEES

Please complete and forward the following form to the Information Systems Department to receive access to EMWD's technology and network resources. Only original documents with wet signatures will be accepted. PLEASE PRINT CLEARLY.

<table>
<tr><td>DATE:</td><td>FIRST (please print):</td><td>LAST (please print):</td></tr>
<tr><td colspan="3">MY SIGNATURE BELOW INDICATES THAT I HAVE READ AND UNDERSTAND THE DISTRICT'S COMPUTING POLICY AND THAT I AGREE TO THE CONDITIONS OF THIS POLICY:</td></tr>
<tr><td colspan="3">SIGNATURE:</td></tr>
<tr><td>EMWD EXT. OR PHONE #:</td><td colspan="2">COMPANY NAME:

EMAIL ADDRESS:</td></tr>
<tr><td colspan="3">DISTRICT CONTACT RELATED TO BUSINESS BEING PERFORMED

NAME:

DEPT: EXT:</td></tr>
</table>