Policy:	Computing Policy	
Date: November 2, 2017	**Revision Date:** April 8, 2022	**Approved by:** Human Resources

I. PURPOSE AND SCOPE

The purpose of this policy is to establish standards of acceptable use of electronic equipment, data processing, and communications resources used to conduct Eastern Municipal Water District (EMWD or District) business, even when non-District equipment is used for technology, data, or network access.

This policy governs EMWD technology, network use, and data confidentiality. It applies to all full-time, part-time and temporary staff as well as contractors and visitors using or accessing technology, data, or network resources provided by EMWD. Violation of this policy may lead to revocation of system privileges, legal action, corrective action or discipline, up to and including termination of employment. 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 using technology. Eligibility will be determined by the employee's department Executive Management.

Prior to using or accessing any EMWD technology, data, or network resources, all users must sign the appropriate Computing Policy Acknowledgement at the end of this document affirming that they have read, understand, and will comply with this policy at all times.

III. SECURITY

Users are the District's most important security safeguard.

- Never share any computer or system passwords or leave an unlocked device unattended.
- Always lock the screen or log out when away from a system, whether working remotely or in the office.
- 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 as soon as you are aware of:

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

Specifics of computer or network security issues should be discussed only with Information Systems or Safety, Risk and Emergency 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. Non-compliant software may be removed during regular software compliance audits without notice.

V. LIMITATIONS OF USE

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

District-issued technology (e.g., telephones, cellular devices, computers, laptops, tablets) is 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 are not required to 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. This does not preclude staff from configuring District email on a well-maintained personal device.
- Modifying, disabling, or tampering with any settings or systems that could present a security risk to the District is strictly prohibited.
- Intentional introduction of malicious or infected files onto District systems is strictly prohibited and grounds for disciplinary and/or legal action.
- 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 if 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.
- A personal device may only be used to remotely access District resources if it meets and is maintained according to in accordance with the minimum specifications as defined in the EMWD Telecommuting Policy, distributed with a work-from-home authorization.
- Enabling or configuring a personal wireless (e.g. Wi-Fi, Bluetooth) hotspot for any purpose other than personal, non-District business use within a District-controlled facility is prohibited.
- Accessing, installing, or using any materials that infringe on one or more active copyrights is prohibited.
- Acquisition, storage, or dissemination of data which is illegal, pornographic, or which negatively depicts race, sex, creed or other protected classes is specifically prohibited.
- 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.***

District data, sensitive documentation, or intellectual property shall be shared and used only in connection with District business. District data may not be used for any other purpose, in an aggregated or disaggregated manner, without explicit authorization from the District's designated representative. District data, credentials, documentation, and intellectual property shall be stored and managed securely and within the United States at all times. If a contractor operates or stores data outside the United States, any exceptions must be clearly defined and negotiated as an addendum to a contractor's agreement.

VI. LIABILITY

District contractors and any associated third parties that expose District technology or data to harm, misuse, or theft may be held legally and financially responsible for actions resulting from the violation.

VII. 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 or file 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 file sharing platforms.

VIII. PRIVACY

The District reserves the right to examine any information transmitted or stored on District technology. Such examinations 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.

Secure (SSL) traffic from EMWD computing devices to the Internet is scanned and filtered except for sites categorized as: finance and banking, health and wellness, or personal privacy. You can look up a site's assigned category on FortiGuard Labs website at https://www.fortiguard.com/webfilter.

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

Any and all internal communication(s) by and between the officers, agents and attorneys of any and all labor organizations which have been recognized or certified as the exclusive agent for bargaining over wages and conditions of employment for any group(s) of District employees (hereinafter "Labor Organization") – whether originated on, stored on or transited through the District's information systems -- shall be deemed private and confidential. Additionally, any and all data or information stored on or transited through the District's information systems by any and all Labor Organizations shall be deemed private and confidential. Hereinafter, references to Labor Organization confidential communications and private data shall be collectively referred to as "Confidential Information." Information

Systems and Records Management employees who through the normal course of performing assigned job duties (e.g. restoring files, maintaining systems, supporting users), inadvertently access Confidential Information in the course of legitimate work-related tasks, are not in violation of this Policy. Notwithstanding the above, the District urges any representatives of labor organizations to engage in internal communications without using District technology and/or equipment.

The District shall hold and treat Confidential Information, and shall not copy, read, view or in any other way access Confidential Information without the express written approval from the applicable Labor Organization. The protection afforded to Confidential Information by this Computing Policy does not supersede the District's obligation to produce documents in response to a California Public Records Act ("CPRA") request, civil discovery request, subpoena and/or court order, and other obligations imposed by federal or state law

In such circumstances, the District will notify the applicable Labor Organization that: (1) the District is in receipt of a CPRA request, civil discovery request, subpoena and/or court order; and (2) that it could potentially cause the District to access Confidential Information within the meaning of this Computing Policy. The District will then provide the Labor Organization with a copy of the CPRA request, civil discovery request, subpoena, and/or court order. The Labor Organization shall then have 10 days from receipt of the District's notification to respond in one of the three following ways:

(1) The Labor Organization does not object to the District accessing Confidential Information, and producing documents containing Confidential Information in response to a CPRA request, civil discovery request, subpoena, and/or court order;

(2) The Labor Organization intends to cooperate with the District so that potentially responsive documents can be accessed, reviewed, and redacted to the extent they contain Confidential Information, prior to production in response to a CPRA request, civil discovery request, subpoena and/or court order. The District will provide the Labor Organization the initial opportunity to review responsive documents and recommend redactions. This cooperative process shall last no longer than 30 calendar days, at which time the District may proceed with production of responsive documents.

(3) The Labor Organization will file an objection, motion to quash, and/or other pleading within ten (10) days seeking judicial intervention to halt the underlying obligation and prevent the production of documentation containing Confidential Information.

In the event the District does not receive a response from the Labor Organization within ten (10) days, the District shall proceed with producing documents containing Confidential Information in response to a CPRA request, civil discovery request, subpoena, and/or court order.

Subject to the foregoing, in the event of the production of dissemination of Confidential Information by a District employee/agent -- the District shall immediately notify the impacted Labor Organization and take all appropriate and legally mandated actions to ensure the future confidentially of the affected Confidential Information.

IX. RECORDS MANAGEMENT/RETENTION

All stored or transmitted data is the property of the District and shall not be shared with other parties without permission from the department's respective Executive Management. Exporting or saving District records to removable media as a means of circumventing District records management policies is prohibited.

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 for details.

Employees and contractors affirm that any copies of District data will be permanently deleted when no longer required under an active District project, retention policy, or agreement.

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

X. 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.

XI. 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.

XII. FURTHER GUIDANCE

The Information Systems helpdesk is always available to assist with questions or clarification on specific technical aspects of this policy.

EMPLOYEE ACKNOWLEDGEMENT

I have read and agree to the requirements and expectations of the Eastern Municipal Water District's Computing Policy. I have received a copy of the Computing Policy and agree to abide by its guidelines as a condition of my employment and understand that violation of this policy may lead to revocation of system privileges, legal action, and subject to corrective action or discipline, up to and including termination of employment.

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

_____	_____
Name (please print clearly)	Signature
_____	_____
Employee Number	Date

CONTRACTOR/NON-EMPLOYEE ACKNOWLEDGEMENT

Please complete and forward the following form to the Information Systems Department to receive access to EMWD's technology, data, or network resources. Only hand-written 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. I AGREE TO THE CONDITIONS OF THE COMPUTING POLICY AND CAN BE HELD LEGALLY LIABLE FOR VIOLATIONS OF THIS POLICY:</td></tr>
<tr><td colspan="3">SIGNATURE:</td></tr>
<tr><td>CELLULAR 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>