NORTH MARIN WATER DISTRICT

**BOARD POLICY: COMPUTER USE AND CYBERSECURITY**
**BOARD POLICY NUMBER: 40**

**Original Date: May 1, 2007**
**Last Reviewed: June 2024**
**Last Revised: October 2024**

## I. PURPOSE

This policy governs the use of computers by North Marin Water District (NMWD or District) employees to ensure appropriate use and District compliance with all legal requirements pertaining to computer use, acquisition and installation. The policy serves as a cybersecurity policy to enforce standards and procedures to protect the District's water and wastewater systems, prevent security breaches, and safeguard networks.

## II. SCOPE

This policy applies to computers and all documents and data contained in or recoverable either electronically or in hard copy from such tools used by NMWD. This policy applies to all computers provided by NMWD and includes computers, computer accessories, software, laptops, tablets, smart phones, storage media, electronic mail (e-mail), voice mail, text messages, internet access, online information services, and any other type of computerized electronic equipment, as well as computers used on NMWD's property for NMWD's business purposes. The term computer is used throughout this policy and shall have the meaning of any of the electronic devices, equipment, software and services described above.

The following individuals are identified as cybersecurity leads for the District, serving as centralized point of contact responsible for overseeing and managing the planning, resourcing, and execution of cyber activities for information technology (IT) and operational technology (OT) systems:

| Position | Title | Contact |
|---|---|---|
| IT Cybersecurity Lead | IT Consultant (CORE Utilities, Inc.) | IT@nmwd.com; (415) 761-8915 |
| OT Cybersecurity Lead | Distribution & Treatment Supervisor | (415) 761-8902 |

## III. GENERAL POLICY

NMWD's computers may only be used for its business purposes, except for incidental use during an employee's unpaid lunch period and before or after work as set forth below. It is the policy of NMWD to provide computers to District employees as necessary to adequately perform their assigned duties. It is also policy to provide tablets to the Board of Directors (considered employees for purposes of this policy) to adequately perform their duties including official communications via District emails and conducting Board meetings. District-issued computers to the Board of Directors is also

covered in Board Policy No. 46. During work hours, except during an employee's unpaid lunch period, these computers may not be used for personal purposes or any other purposes unrelated to NMWD's business. Personal use of District computers during the regular work day is prohibited. Employees may make incidental use of their District computer for personal reasons before or after their regular work day. Employees shall have no expectation that the information they convey, create, file or store on NMWD computers, whether during or outside of work hours, will be confidential or private. At no time shall NMWD property including computers be used for commercial purposes outside the scope of NMWD business.

NMWD reserves the right to monitor, copy and/or retrieve the computer files, e-mail, voice mail, or any type of electronic file of any employee, without notice, for purposes, including, but not limited to; obtaining business-related information; investigating violations of this or any other NMWD policy, including, theft, disclosure of confidential business or proprietary information, using the system for personal reasons during work hours, or for monitoring work flow or productivity.

Activity reports will be generated from time to time and will include detailed information concerning computer use by NMWD employees.

## IV. USE OF COMPUTERS

A. Computer Software

All software installation on the file server or District Computer hard drives will be coordinated through the Department Head, Information Technology (IT) staff and the Auditor-Controller (A-C), if the cost is not covered by existing subscriptions or licenses. No District software will be copied for use outside of the District, unless it is legal to do so, and coordinated through IT staff. All software that resides on any of NMWD's computers must be licensed to NMWD. Employees understand that data, files, messages and information on NMWD's computers, servers, or voice mail may be subject to disclosure, either as "public records" or pursuant to discovery in litigation.

B. Online Information Service Use

Use of online information services, such as the Internet, shall be accessed on NMWD computers only through the internet service provided by NMWD. Personal access to online information is permitted on a limited and incidental basis only during an employee's unpaid lunch period and before or after an employee's regular work day. Personal access to any internet content of a sexual nature is strictly prohibited. All software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading or modifying any such software without the permission of their Department Head, IT staff. and the copyright holder. External connections to NMWD's internal network are not permitted unless expressly authorized by the Department Head and IT Staff.

C. E-mail

Electronic mail addressed to, generated by, or received on NMWD's computers or servers is the property of the NMWD. When using District e-mail, the employee is acting as a representative of NMWD, and should act accordingly so as not to damage the reputation of The District. Confidential financial or customer data should not be sent via e-mail except under unique circumstances as determined by the Auditor-Controller or General Manager. Sending employee medical, personal, or financial information by email or storage media should be avoided unless delivered via a fully encrypted e-mail system or storage media. Incidental personal use of the District's email system is permitted but should be kept to a minimum, comply with all other provisions of this policy and not include any personal broadcast emails such as emails sent to "all staff" or other email address group about a non-District matter such as a personal request, function or event. The standard for a minimal amount of messages will be established at the discretion of the Department Head or supervisor.

The District e-mail system and all messages, attachments, and images are the sole property of the District. This includes any and all messages, attachments, and images of any kind sent during regular work hours, an employee's break, or after-hours. E-mail messages may constitute a District record subject to NMWD Board Policy No. 28 Public Records Policy, and subject to potential disclosure under the California Public Records Act. Electronic records, including but not limited to e-mail messages, may be disclosed by the District to outside parties in connection with litigation, investigations, audits, requests for public records under the California Public Records Act, or by any other law or policy. The District will comply and will not be liable or responsible for the disclosure of any electronic record or part thereof.

D. Information Retrieval or Delivery

Information or files deleted by an end-user from electronic media may not be permanently deleted from the system. Employees understand that it is possible to recover end user deleted computer files, deleted e-mail, deleted voice mail messages, or any other deleted digital data at any time.

Use of web-based file transfer services (such as Dropbox) or third-party remote access programs (such as TeamViewer or Splashtop) are not permitted unless expressly authorized by the IT Staff. Any vendor or consultant who has been given access to the District's systems is not permitted to transfer files to or from their systems unless specifically authorized by the IT Staff. This includes VPN connections and any third-party remote software programs that provide file transfer functions.

E. Virus Protection

NMWD computers have virus protection software installed; however, no virus protection software package will detect every possible virus. Employees should assume that any media from

outside the District (flash drives or other storage devices, e-mail attachments, files downloaded from the internet, etc.) could contain a virus. Do not open any file with which you have any concern or suspicion or were unsolicited. Report immediately to IT staff and the Department Head any detected virus or abnormal computer activity after receiving any suspicious media from outside the District.

F. Passwords

The District requires passwords to access computer-based systems. These passwords, with a login ID, represent a specific individual to the system for security purposes. No employee should attempt to login as another individual. Passwords should be complex enough so that they cannot be easily duplicated. A combination of numbers, letters, and characters is recommended. Passwords must not be shared or compromised. If you suspect your password has been compromised, contact IT staff for instructions on how to change your password immediately. For login to industry associations or memberships (e.g. AWWA, ACWA) on behalf of the District, establishing a group login and password can be established where allowed.

G. Use During Public Meetings

During District Board meetings or public committee meetings the computers will be used solely to access the District meeting materials for the current or previous meetings. The use of technology hardware, including cell phones, smart phones, tablets, computers, and other similar devices including accessing the internet for email, social media, blogs or other communication platforms, or to receive or send phone calls, texts, emails or other types of electronic communication, by a Director or District staff for the purposes of communicating directly with another Director, multiple Directors or Staff regarding an action item on the Agenda during a public meeting is not permitted pursuant to the Ralph M. Brown Act. However, use of similar technology and communication methods during a public meeting, is permitted for purpose of coordinating or communicating the logistics or actions of an invited consultant or other third party participating in the meeting (remotely or in-person) or for confirming a fact, data, or reference related to an Agenda item.

H. Use of Artificial Intelligence (AI)

Available applications driven by Generative Artificial Intelligence (GenAI), such as chatbots (e.g., ChatGPT) or image generators (DALL- E 2, Midjourney) are exciting new innovations that may appear to offer opportunities to increase workplace efficiency. Use of this new technology also brings significant risks related to confidentiality, accuracy, and security. GenAI applications are subject to providing false answers or information, or information that is out-of-date. As such, employees must carefully and thoroughly verify that any response from a GenAI tool upon which they intend to rely, or use is accurate, appropriate, and ethical; is not a breach of confidentiality; and does not violate any District policy or law.

Information provided to a GenAI tool may become publicly available, regardless of any assurances to the contrary. As such, no confidential, proprietary, or sensitive information should be provided to a GenAI tool. For example, employees must not upload or input: passwords or other credentials; confidential health records or other personnel or personally identifiable information; or any other confidential District information. If an employee does use a GenAI tool to help perform a work task, they must inform their supervisor of that fact, preferably in advance of such use, in writing.

Employees are not permitted to represent any work generated by GenAI as their own original work. Employees must ensure that, if any of their work uses AI-generated information or assistance, they should include a clear statement of that fact on the work product. Employees shall not integrate any GenAI tool into District software, without advance written authorization from the IT Staff.

I. Mobile Devices

District employees use mobile communications devices (personal and District-issued) to conduct District business and serve the public. The District may provide an eligible employee a District-issued Cellular Phone to conduct District business. The District reserves the right to refuse the ability to connect personal mobile devices to District messaging and the District computer network. The District will engage in such action if the mobile device security has been compromised or has been used in a way that puts the District systems, data, and staff at risk.

Only incidental personal use of District-issued mobile devices is allowed. Employees shall not use mobile devices that violate state or local laws regarding the use of cell phones or wireless devices while driving. Incidental personal use of communications wireless devices must not adversely affect the performance of employee's official duties or the organization's work performance, must not be disruptive of co-workers, must be of limited duration and frequency and should be restricted to matters that cannot be addressed during non-duty hours. The incidental personal use of District communication wireless devices shall be kept to an absolute minimum. The District reserves the right to monitor wireless device use periodically for abuses.

Any District-related Electronic Communication, or information stored on a wireless communication device may constitute a record subject to disclosure under the California Public Records Act (CPRA), the California Code of Civil Procedure, the Federal Rules of Civil Procedure, or other applicable statutes, regulations, or legal authorities.

## V. ALLOWABLE USES OF COMPUTERS

Allowable uses of computers for NMWD's business purposes include the following:

A. Facilitating performance of job functions;

B. Facilitating communication of information within NMWD;

C. Coordinating meetings of individuals, locations and resources of the NMWD;

D. Communicating with outside organizations as required in order to perform assigned job duties;

E. Communicating with a District-owned equipment or device equipped with a computer, when authorized;

F. Communicating with computer-based or network enabled device, equipment, or system associated with building or facility operational function, when authorized;

G. Computer use by Board Directors as described in Board Policy Number 46.

## VI. PROHIBITED USES OF NMWD's COMPUTERS

Prohibited uses of NMWD computers include, but are not limited to, the following:

A. Using the computer systems for any unlawful purpose, such as in violation of copyright or patent rights or for criminal purposes;

B. Transmitting confidential financial or customer data or confidential personnel or medical information concerning other NMWD employees except as allowed in Section IV. C above;

C. Displaying, downloading or transmitting material, images, messages or cartoons that are sexually explicit or that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs;

D. Displaying, downloading or transmitting messages or images that are threatening, derogatory, defamatory, obscene or otherwise inappropriate;

E. Soliciting others for commercial or personal financial gain (including chain letters, sale of personal property, etc.), political or religious lobbying, outside organizations, or other not job-related matters;

F. Intentionally disrupting network traffic or crashing the network and connected systems (for example, sabotaging, intentionally introducing a computer virus);

G. Accessing or attempting to access others' accounts or files without authorization and with no substantial business purpose;

H. Vandalizing the data of another user;

I. Forging, spoofing or phishing email messages;

J. Wasting system resources (for example, downloading unneeded files or images, "spamming" e-mail, and storing unneeded files);

K. Using computers inappropriately, in a way deemed by NMWD to violate the intended purpose of this computer use policy.

## VII. STAFF TRAINING

As a water systems entity, the NMWD runs both operational technology (OT) and information

technology (IT) systems that are often vulnerable to cyberattacks. Conducting cybersecurity awareness training to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks is an important part of each NMWD staff member's training plan. As part of this policy, cybersecurity awareness training should be conducted on an annual basis for all staff that use computers with a signed acknowledgment that they have completed training. This signed acknowledgment will be retained in the employees personnel file.

## VIII. REMOTE ACCESS POLICY

Approved District staff can remotely access District resources in two different situations. The first situation is for regular District employees to connect to the main office network via a secure VPN and then be able to access their assigned workstation. This allows for the employee to have a secure virtual connection to their individualized workstation only. In this situation, the above policies remain in effect and the employee is to treat the connection as if they were at the District office. The second situation is to allow remote access for District System Distribution staff to the District's SCADA systems. This is provided via a secure VPN connection and then a direct remote access to the SCADA servers at the Yard and Stafford Treatment Plant. Only authorized Operations staff are allowed this ability.

## IX. ACCESS CONTROL POLICY

The District utilizes a combination of Discretionary Access Control (DAC) and Role-based Access Control (RBAC) throughout it systems. All employees are provided with a username and password that is required to log onto a District workstation. Permissions are set by the administrator for the employee based on their role with the District. This provides basic access to the workstation, e-mail, server public folders, their working folder, and specific shared drive locations on the servers. In addition, there are specialty programs for billing, accounting, HR, engineering, SCADA, etc. that also require a separate login with permissions. Those separate permissions are based on the individual employee. Individual workstations are customized for each employee's access by IT staff and are not allowed to log on using other workstations unless specifically set up by IT staff. Mobile devices such as cell phones, tablets and laptops all have specific VPN credentials installed for each and can be enabled or disabled individually. Employees should not try and access areas of the network where they are not authorized.

## X. DATA PROTECTION POLICY

The District follows a strict data protection policy (DPP) to standardize the use, monitoring, and management of data. The District collects and stores billing, accounting, water/sewer system, employee, and customer information on its servers. The District's water and sewer system information can include as-built drawings, developer, construction and operational information. Employee

information includes job descriptions, performance reviews, payroll, banking, and other employee information such as healthcare. Customer information including service information, billing information, transactions, balances, payments, and usage history. The District protects this data through effective use of the Access Control Policy and a robust backup system. Backups are conducted with weekly snapshots on secure drives in addition to daily full backups rotated on removable media and stored securely.

Employees must constantly be on alert for attempted theft of District data. The most common attempt to gain access to secured District data is through an e-mail scam. An employee might receive an e-mail that looks like it came from a supervisor, management, or a Board Director asking for information. While the District has safeguards in place to try and filter out these attempts, automated software applications that performs repetitive tasks over a network (known as bots) and AI are constantly improving their attempts to gain access. It is imperative that employees verify requests for sensitive data like usernames, passwords, social security number, banking information, wire transfers, etc. are actually coming from other District staff. If employees receive such e-mails, they should immediately engage IT staff to verify the e-mail or verify in person the request. Other attempts come through websites that look legitimate but are not. Employees should always stop and verify the legitimacy of what is being asked and not provide sensitive information without being certain.

Confidential information should never be provided outside the District without first verifying it is required. If it is to be provided, it should only be provided via encrypted e-mail, encrypted websites or encrypted files via removable media. If there is ever any doubt, employees should discuss the transfer of critical information with their supervisor, management or IT staff.

**XI. VIOLATIONS OF POLICY**

Violations of this policy will be reviewed on a case-by-case basis and may result in disciplinary action (up to and including termination), pursuant to the District's personnel policies.

## NMWD Computer Use Policy Acknowledgment

I acknowledge that I have received a copy of the NMWD Computer Use and Cybersecurity Policy.

I agree to abide by the conditions set forth therein.

_____

Employee Signature / Date

Revised: 06/13, 10/24