TITLE:
Electronic Resources Policy
ADOPTED BY BOARD OF HARBOR COMMISSIONERS:
11-15-2021
EFFECTIVE DATE:
Upon approval from the Board of Harbor Commissioners.
SUPERSESSION:
This Administrative Policy supersedes policies #513 and #513.1, adopted June 21, 2021.
PURPOSE:
The Oxnard Harbor District provides various Electronic Resources and postal communication resources to authorized employees and to members of the Board of Harbor Commissioners to assist them in performing their duties for the District. Each individual who is provided with District Electronic Resources has a responsibility to use the District's Electronic Resources in a manner that increases productivity, enhances the District's public image, and is respectful of others. The purpose of this policy is to establish guidelines for the use of the District's Electronic Resources. Failure to follow the District's policies regarding Electronic Resources may lead to disciplinary measures, up to and including termination of employment, and/or loss of the right to use District Electronic Resources.
POLICY:
1. Applicability. This Policy is applicable to all exempt and non-exempt employees of the Oxnard Harbor District, as indicated within the policy, as well as the Board of Harbor Commissioners to the extent that Board Members are issued and/or use District Electronic Resources. 2. Definition of Electronic Resources. Electronic Resources consist of all electronic media and storage devices, software, and means of electronic communication including any of the following: personal computers and workstations; laptop computers; mini and mainframe computers; tablets; computer hardware such as disk drives, tape drives, external hard drives and flash/thumb drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet or cloud storage accounts; electronic mail; telephones;

cell phones; personal organizers and other handheld devices; pagers; voicemail systems; and instant messaging systems.

3. Ownership. The District shall be considered the owner of all Electronic Resources paid for by the District.

4. General Rules. Users of Electronic Resources must:

- Operate Electronic Resources in accord with all applicable District policies.
- Operate Electronic Resources or related equipment in a safe manner.
- Maintain the privacy of all passwords. There must be no unauthorized obtaining, sharing or use of passwords.
- Use appropriate greetings and communicate in a courteous, professional and conscientious manner.
- Not remove from District premises or fail to return upon request any District owned Electronic Resources, without prior written permission of the CEO/Port Director or designee.

5. Prohibited Uses. Electronic Resources are prohibited from being used in the following manners:

- For any illegal purpose, violation of any District policy, for pecuniary gain, or in any way that discloses trade secrets or other confidential or proprietary information of the District, business partners, vendors, or customers.
- To create, modify, execute, or re-transmit any data, images, recordings, computer programs or instructions intended to gain unauthorized access to, or make unauthorized use of, any of the District's Electronic Resources.
- To copy, retrieve, forward, or send copyrighted materials unless the employee has the author's permission or is accessing a single copy only for the employee's reference.
- With the intent to compromise any other systems, computers, or networks or to commit crimes or other unethical acts.
- For political activity, including campaigning.

- To engage in online activities that are connected with any type of outside work, commercial activities, or for-profit activities, including trading.

- To initiate or propagate non-work related electronic chain letters, photos, videos, recordings, images, blogs, unauthorized mass mailings or using e-mail or personal web pages for political or personal commercial purposes that are outside the scope of District's purposes.

- To transmit, receive, download, or store any information that is discriminatory, harassing, defamatory, obscene, indecent, threatening, or that otherwise could adversely affect any individual, group, or entity (e.g., sexually explicit, or racial messages, slurs, jokes, or cartoons). As set forth more fully in the District's Harassment, Discrimination and Retaliation Prevention policy in the Employee Handbook and the Anti-Harassment, Discrimination, and Retaliation Policy # 503.1, the District does not tolerate discrimination or harassment based on gender, pregnancy, childbirth (or related medical conditions), race, color, religion, national origin, ancestry, age, physical disability, mental disability, medical condition, marital status, sexual orientation, family care or medical leave status, military status, veteran status, or any other status protected by state and federal laws.

- For personal use, or in a manner which is excessive or uneconomical. Telephones are provided to conduct District business and should not be used for non-emergency personal use. Personal calls must be kept brief and shall only be of an immediately important or emergency nature. Receipt of personal calls shall not interfere with District business. The District reserves the right to seek reimbursement for any telephone charges resulting from personal / non-emergency use of the telephone. Use of District purchased postage stamps and postage meters for any purpose other than conducting District business is prohibited.

- To discuss confidential or sensitive information (particular applicable to cell phones) unless it is determined that the manner of communication is secure.

- For gambling.

- To store, operate or in any manner use non-work related data.

- To improperly or inaccurately convey or imply the District's support, opposition, sponsorship, or endorsement.

- To release or fail to protect confidential District or employee information or to violate any privacy rights.

- In violation of any other District policies or in any manner that violates local, state or federal laws or regulations.

6. Preclusion from Using Personal Accounts. Except as expressly provided herein, all District employees are prohibited from using personal accounts or personal electronic devices for the creation, transmission, or storage of electronic communications regarding District business or in any way conducting District-related business. Additionally, all employees are prohibited from using District-provided Electronic Resources for personal use except as otherwise specifically provided herein.

7. District Property and No Right of Privacy. All messages sent and received, including personal messages, and all data and information stored on the District's Electronic Resources (including on its electronic mail system, voicemail system, or computer systems) are District property regardless of the content, and regardless of whether it is a union-related communication sent during non-work hours. As such, the District reserves the right to access all of its Electronic Resources including its computers, voicemail, and electronic mail systems, at any time, in its sole discretion. No employee, other than the CEO/Port Director or designee, has authority to waive, vary or amend the District's right to access its Electronic Resources.

8. Passwords and Login Credentials. Certain of the District's Electronic Resources can be accessed only by entering a password or using login credentials. Passwords and login credentials are intended to prevent unauthorized access to information. Passwords and login credentials do not confer any right of privacy upon any employee of the District. Thus, even though employees may maintain passwords or be provided with login credentials for accessing Electronic Resources, employees must not expect that any information maintained on Electronic Resources, including electronic mail and voicemail messages, are private. Employees are expected to maintain their passwords and login credentials as confidential. Employees must not share passwords, or forward login credentials unless authorized by the CEO/Port Director or designee thereof and must not access coworkers' systems without express authorization.

9. Non-Exempt Employee Usage of District Electronic Resources Outside of Work Hours. Non-exempt employees are prohibited from using District provided Electronic Resources outside of working hours. This includes, but is not limited to, tablets and cell phones. As used in this policy, "working hours" includes all time during which a non-exempt employee is performing services or work for the

District; it does not include rest break periods, meal periods, or periods in which a non-exempt employee is not performing services or work for the District.

10. Issuance/Use of Electronic Resources by Commissioners and Exempt Employees. The District may issue and pay for employee-enabled cellular phones, tablets, and wireless cards (hereafter "Device(s)") consistent with this Policy to Commissioners and exempt employees (collectively, "Participants") who submit a request to the District IT Department.

- Activation: Upon submission of a request, approval thereof, and being issued a Device by the District, Participants may opt to use their own personal Apple ID, and/or the District assigned Apple ID.

- Expenses – Covered: Participants will be issued a District-owned Device on a District-provided plan ("Plan"). Monthly business-related voice and data charges will be covered by the Plan. The District's Plan includes unlimited data and wireless, and Participants will not be charged for business-related data or wireless charges. Additionally, the Plan will cover incidental usage of the District-owned device, including personal voice and data charges provided there is no additional cost to the District. The District will not cover the cost of any expenses incurred by Participants that are not directly related to the District's business

- Expenses – Not Covered: Participants may use District devices for personal use provided there is no additional cost to the District. The Plan does not cover, and Participants will be responsible for, the following expenses incurred on a District-owned Device ("Participant Charges"):

  (a) Any charges not included in the Plan (e.g., directory assistance calls, international roaming charges, Talena, games, ring tones, etc.);

  (b) Additional memory, portable power supply, or upgrading to a larger device, unless the memory or upgrade is directly related to the Participant's job duties within the District;

  (c) Additional device accessories (e.g., higher quality headphone, etc.) or charges incurred for downloading games, ring tones, or any other non-District-related features

- International Travel: International Plans must be activated in advance of travel to avoid excessive roaming charges and to ensure the availability of data services. The participant must provide the IT Department with sufficient advance notice of plans to

travel abroad to allow time for an International Plan to be added during your scheduled travel date(s). The participant is required to contact the IT Department in advance of traveling outside of the country with a District-issued Device so that International services can be activated.

11. Electronic Resources Management Policy. The District shall use a Mobile Device Management (MDM) software system that allows the IT Department administrative control over District-issued Electronic Resources. This system allows for management of passwords, remote connection settings, increased device security, control of allowed applications, and location of lost or stolen devices. This software may not be removed or tampered with.

- Download of applications may be restricted, or applications may be removed, if those applications are considered inappropriate, unrelated to District business, or they are considered a threat or significant risk to the District's network environment.

- From time to time, users may be asked to present their device to the IT Department for a software update or receive instructions on how to download and update themselves. Users must promptly comply with these requests.

- Devices are used as convenience and productivity enhancing tools. Due to their somewhat volatile nature, the data on these devices is considered as transient, convenience copies. However, if there is a record on the District-owned device that needs to be retained, users are required to retain the record on a District-file system pursuant to the District's Records Management Policy.

12. Security Requirements. All users of District Electronic Resources, to the extent possible depending on the Electronic Resource, must comply with the following security procedures:

- Electronic Resources must be password protected;

- Electronic Resources must lock after five incorrect password attempts; and

- Electronic Resources must "time out" and require a password after a fifteen-minute period of inactivity.

13. Loss or Theft. In the event of a loss or theft of District Electronic Resources, users must immediately notify the District IT Department. The District retains the right to correct any such incident in order to protect the integrity of District's

systems and data. The District reserves the right to perform a remote reset/wipe of any District-owned Electronic Resource at any time.

14. Use of Electronic Resources While Driving. Employees who drive on District business must abide by all state and local laws prohibiting or limiting Electronic Resources (for example, cell phone or personal digital assistant) use while driving. Further, even if usage is permitted, employees may choose to refrain from using any Electronic Resources while driving. "Use" includes, but is not limited to, talking, or listening to another person or sending an electronic or text message via Electronic Resources. Regardless of the circumstances, including slow or stopped traffic, employees should proceed to a safe location off the road and safely stop the vehicle before placing or accepting a call. If acceptance of a call is absolutely necessary while the employee is driving, and permitted by law, the employee must use a hands-free option and advise the caller that they are unable to speak at that time and will return the call shortly. Under no circumstances should employees feel that they need to place themselves at risk to fulfill business needs. Since this Policy does not require any employee to use a cell phone while driving, employees who are charged with traffic violations resulting from the use of their Electronic Resources while driving will be solely responsible for all liabilities that result from such actions. District employees and representatives are expressly prohibited from checking, sending or receiving emails or text messages while driving. These requirements apply at all times when driving a District issued vehicle and at any time when driving on District business, even if the representative or employee uses their own vehicle. Failure to adhere to this provision is grounds for discipline, up to and including termination.

15. Accounting Controls: Copies of all reviewed Device bills shall be maintained by the District's Finance Department. Additional audits of these bills shall be carried out on a periodic basis by Finance Department staff to ensure adherence to this Policy.

16. Discontinued Use. Upon separation of employment or upon a user no longer qualifying to receive District-owned Electronic Resources, the Electronic Resources must be returned to the District. With approval of CEO & Port Director, users may purchase discontinued electronic Resources at current documented market value.

17. Potential Disciplinary Action or Restrictions on Future Use: Any District employee who violates this Policy may be disciplined, up to and including termination as appropriate, in accordance with this Policy. Further, any violation of this Policy may be punishable by an individual's loss of the right to use any District-owned Electronic Resources as described herein. In addition, violations of this Policy may be referred for criminal prosecution, if appropriate.

RELATED POLICIES:

OPERATIONS POLICY 208.1 District Driving Policy

DEFINITIONS:
Electronic Resources consist of all electronic media and storage devices, software, and means of electronic communication including any of the following: personal computers and workstations; laptop computers; mini and mainframe computers; tablets; computer hardware such as disk drives, tape drives, external hard drives and flash/thumb drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet or cloud storage accounts; electronic mail; telephones; cell phones; personal organizers and other handheld devices; pagers; voicemail systems; and instant messaging systems.