STAFF REPORT

FAIR OAKS RECREATION & PARK DISTRICT

Meeting Date:	**March 15, 2023**
To:	**Board of Directors**
From:	**Michael J. Aho, District Administrator**
Subject:	**Approval of Policy Updates: Diversity, Equity and Inclusion Policy, Technology Asset Management Policy, and Cybersecurity Policy.**
Prepared By:	**Jennifer Larkin, Administrative Services Manager**

I. Recommendation

Approve the Diversity, Equity and Inclusion (DEI) Policy, Technology Asset Management Policy, and Cybersecurity Policy as recommended by the Policy Review Committee.

II. Background

The Policy Review committee met on March 7, 2023 to review several new policies, including the DEI Policy, Technology Asset Management Policy, and Cybersecurity Policy.

The DEI Policy memorializes the District's commitment to maintaining a diverse and culturally respectful workplace environment. All specific information on legally protected classes of employees as well as processes to be followed can be found in the District's Personnel Policy Manual and are updated as often as legally required.

The Technology Asset Management Policy is a companion to the District's Asset Management Policy and outlines the District's process for tracking and effectively managing the District's electronic devices.

Finally, the Cybersecurity Policy outlines the District's program to prevent, detect, respond to and recover from cybersecurity threats. The District has a separate Social Media Policy that outlines proper protocols for utilizing social media on District devices.

III. Problem /Situation/ Request

Staff requests that the Board approve the policies to be included in the Fair Oaks Policy Manual.

IV. Financial Analysis

There is no financial impact to the District.

Respectfully Submitted,

Michael J. Aho
District Administrator

Attachment A: Draft DEI Policy
Attachment B: Draft Technology Asset Management Policy
Attachment C: Draft Cybersecurity Policy

DIVERSITY EQUITY AND INCLUSION POLICY

OVERVIEW

The Fair Oaks Recreation & Park District (FORPD) is committed to fostering, cultivating and advancing a culture of diversity, equity and inclusion (DEI) which is central to its mission and vision.

SCOPE

FORPD diversity initiatives are applicable to all levels of leadership, employees, partners and the community. The District is committed to being an inclusive organization through its practices and policies on staff recruitment and selection; compensation and benefits; professional development and training; promotions; transfers, layoffs and terminations along with the development and delivery of social and recreational programs in the community,

DIVERSITY EQUITY AND INCLUSION POLICY

I. The District embraces diverse and inclusive teams knowing they provide a positive impact on work through innovative approaches that help to better serve the community. The collective sum of the individual differences represents a significant part of enhancing not only the Fair Oaks community but inspires a healthier reputation and strengthen the District's achievements.

II. FORPD is committed to an ongoing development of a work environment that encourages and enforces:

   a. Respectful communication and cooperation between all management and employees, whether temporary, part-time, or full-time.

   b. Teamwork and employee participation, permitting the representation of all groups and employee perspectives.

   c. Discussion and respect of individual's boundaries

   d. Speaking up when experiencing or noticing disrespectful behavior;

   e. Championing diversity, equity and inclusion through all aspects of work with partners, customers and the community.

III. All employees of FORPD have a responsibility to treat others with dignity and respect at all times. All employees are expected to exhibit conduct that reflects inclusion during work, at work functions on or off the work site, and at all other company-sponsored and participative events.

IV. All employees are also required to attend and complete periodic diversity awareness training to enhance their knowledge to fulfill this responsibility.

Any employee found to have exhibited any inappropriate conduct or behavior against others may be subject to disciplinary action.

Employees who believe they have been subjected to any kind of discrimination that conflicts FORPD's Personnel Policy should seek assistance from a supervisor or a Human Resources representative.

Approved By:

Administrative Services Manager	Date
District Administrator	Date

Jennifer Larkin, District Clerk	Filing Date

TECHNOLOGY ASSET MANAGEMENT POLICY

OVERVIEW

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

PURPOSE

This policy provides procedures and protocols supporting effective organizational asset management specifically focused on electronic devices.

SCOPE

This policy applies to all FORPD staff and Board Members, and all devices owned by the District.

POLICY

I. Asset Types

a. The following minimal asset classes are subject to tracking and asset tagging:

i. Desktop workstations

ii. Laptop mobile computers

iii. Tablet devices

iv. Printers, copiers, fax machines, and multifunction print devices

v. Handheld devices

vi. Scanners

vii. Servers

viii. Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)

ix. Private Branch Exchange (PBX) and Voice over Internet Protocol (VOIP) Telephony Systems and Components

x. Internet Protocol (IP) Enabled Video and Security Devices

xi. Memory devices

II. Asset Value

a. Assets which cost less than $500 shall not be tracked, including computer components such as smaller peripheral devices, video cards, or keyboards, or mice. However, assets, which store data regardless of cost, shall be tracked either as part of a computing device or as a part of network attached storage. These assets include:

ii. Network Attached Storage (NAS), Storage Area Network (SAN) or other computer data storage
iii. High Capacity temporary storage drives (except USB thumb drives)
iv. Tape or optical media with data stored on them including system backup data

III. Asset Tracking Requirements

a. The following procedures and protocols apply to asset management activities:

b. All assets must have an internal FORPD asset number assigned and mapped to the device's serial number.

c. An asset-tracking database shall be created to track assets. It shall minimally include purchase and device information including:

i. Date of purchase
ii. Make, model, and descriptor
iii. Serial Number (if present)
iv. Location
v. Type of asset
vi. Assigned to
vii. Department
viii. Where it was purchased

d. Prior to deployment, Admin staff shall assign an ID to the asset and enter its information in the asset tracking database, Productive Parks. All assets maintained in the asset tracking database inventory shall have an assigned owner.

IV. Asset Disposal And Repurposing

a. Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus.

b. When disposing of any asset, sensitive data must be removed prior to disposal. Admin support staff shall determine what type of data destruction protocol should be used for erasure. Minimally, data shall be removed using low level formatting. For media storing confidential that is not being repurposed, disks shall be physically destroyed prior to disposal.

V. Audit Controls And Management

a. On-demand documented procedures and evidence of practice should be in place for this operational policy as part of FORPD. Satisfactory examples of evidence and compliance include:

b. Current and historical asset management system checks for asset records.

c. Spot checks of record input and accuracy against tracking database.

d. Evidence of internal process and procedure supporting this policy for compliance with general workstation computing policies.

VI. ENFORCEMENT

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

Approved By:

Administrative Services Manager	Date
District Administrator	Date
Jennifer Larkin, District Clerk	Filing Date

CYBERSECURITY POLICY

OVERVIEW

This policy was developed and based upon the best practices and guidelines set by the National Institute of Standards and Technology (NIST).

PURPOSE

The main purpose of the District's Cybersecurity Program is to help prevent, detect, respond to, and recover from cyber security threats.

CYBERSECURITY POLICY

I. Cybersecurity Program

a. Routine Asset Inventories:

i. Maintain log of approved physical electronic devices, cloud systems, data storage, virtual connections, smart devices, etc.

ii. If inventory identifies unauthorized asset(s), a threat assessment shall be performed and unauthorized asset removed from the District's network infrastructure.

b. Assess Risks.

i. Perform an internal risk assessment, at a minimum, annually.

ii. On a tri-annual basis hire a third party to perform the risk assessment.

c. Minimize Control System Exposure.

i. Eliminate all non-secure communication access paths.

ii. Segment networks to limit exposure.

iii. Maintain role-based security clearance.

iv. Encrypt communication when possible.

v. "Lock down" the network to only be accessed by approved devices.

d. Enforce User Access Controls.

i. Use role-based access control to limit the ability of individual users.

ii. Use the principle of limiting the access to network information to the minimum required for the specific users to perform their job.

iii. Ensure default passwords are not used.

iv. Implement multi-factor authentication where possible.

v. Secure remote access through the use of firewalls, virtual private networks, etc.

vi. Deactivate user accounts immediately upon separation from the District.

e. Safeguard from Unauthorized Physical Access.

i. All locations with network, electronic devices, etc. shall be locked at all times and monitored by alarms (motion, door latch, camera, etc.) when office is not in use.

ii. Hardware is to be stored in a lock facility or to be locked in place.

iii. Secure documents with IT configuration information and passwords should be physically stored and locked. Electronic versions shall be password protected.

f. Embrace Vulnerability Management.

i. Create a culture of vulnerability awareness and action.

ii. Once the vulnerability is identified implement the solution as soon as possible.

iii. Attend trainings and conferences to stay current on the best cyber-hygiene practice.

iv. Annual staff trainings on cybersecurity.

v. The District Manager shall commit to continuous improvement and enforcement of cybersecurity.

g. Plan for Incidents, Emergencies and Disasters.

i. Maintain cybersecurity insurance.

ii. Create a disaster response plan for all cyber and electrical components.

Approved By:

Administrative Services Manager	Date
District Administrator	Date

Jennifer Larkin, District Clerk	Filing Date

8.3 Discussion and Possible Action on Approval of Policy Updates

Final Audit Report 2023-03-10

Created:	2023-03-10
By:	Jennifer Larkin (jlarkin@forpd.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAJv4Wg9L4_9xjYv9NinDCVeGclh24Rbpz

"8.3 Discussion and Possible Action on Approval of Policy Updates" History

Document created by Jennifer Larkin (jlarkin@forpd.org)
2023-03-10 - 10:19:57 PM GMT

Document emailed to maho@forpd.org for signature
2023-03-10 - 10:20:09 PM GMT

Email viewed by maho@forpd.org
2023-03-10 - 10:21:11 PM GMT

Signer maho@forpd.org entered name at signing as Michael J. Aho
2023-03-10 - 10:22:09 PM GMT

Document e-signed by Michael J. Aho (maho@forpd.org)
Signature Date: 2023-03-10 - 10:22:11 PM GMT - Time Source: server

Agreement completed.
2023-03-10 - 10:22:11 PM GMT