RANCHO MURIETA COMMUNITY SERVICES DISTRICT

Category:	Personnel	**Policy #**2026-03
Title:	Cybersecurity & Information Security Policy	

1. PURPOSE

The purpose of this Cybersecurity & Information Security Policy is to safeguard the Agency's information systems, operational technology, financial systems, and data against unauthorized access, disruption, fraud, and cyber threats.
This policy supports safe, reliable operations and compliance with applicable federal, state, and local regulations.

2. SCOPE

This policy applies to:

- All employees, contractors, consultants, volunteers, and Board members
- All Agency-owned devices, systems, networks, and cloud services
- Operational technology (OT), including fleet systems, dispatch, CAD/AVL, SCADA and facilities controls
- Financial and administrative systems
- Any third-party vendors with access to Agency systems or data

3. GOVERNANCE & RESPONSIBILITIES

- **Board of Directors:** Provides oversight and approves cybersecurity policy updates.
- **General Manager:** Responsible for implementation and enforcement.
- **IT Manager:** Oversees cybersecurity strategy, risk management, and incident response.
- **Department Directors:** Ensure compliance within their divisions.
- **All Users:** Must comply with this policy and report suspected incidents immediately.

SECTION A: CONTROLS / PROTECTIONS IN PLACE

4. ACCESS CONTROL & AUTHENTICATION

- All users shall have unique credentials.
- Multi-factor authentication (MFA) shall be required for:
  - Remote access
  - Administrative accounts
  - Financial and payroll systems
- Access shall be granted based on the principle of least privilege.
- Access rights shall be reviewed periodically and removed promptly upon separation.

5. NETWORK & SYSTEM SECURITY

- Firewalls, intrusion detection/prevention systems, and endpoint protection software shall be maintained.
- Systems shall receive regular security patches and updates.
- Agency networks shall be segmented separately:
    - Administrative systems
    - Payment systems
    - Operational technology (OT)
    - Public Wi-Fi networks
- Public Wi-Fi shall not have access to internal systems.

6. OPERATIONAL TECHNOLOGY (OT) SECURITY

- Fleet management, dispatch, vehicle communications, collection systems, industrial controls and SCADA shall be secured against unauthorized access.
- Remote access to OT systems must be restricted and logged.
- Changes to operational systems shall follow a documented change management process.
- Backup and recovery plans shall be maintained for critical systems.

7. DATA PROTECTION

- Sensitive data, including employee records, payroll, and payment information, shall be encrypted in transit and at rest where feasible.
- Regular data backups shall be performed and stored securely.
- Confidential information shall not be transmitted via unsecured channels.
- Retention and disposal of records shall follow applicable records management policies.

8. FINANCIAL & PAYMENT SECURITY

- Segregation of duties shall be maintained for financial transactions.
- Changes to vendor payment information must be verified independently.
- Electronic funds transfers (EFT), ACH, and wire transfers require documented approval.
- Revenue reconciliation shall occur regularly.
- Bank accounts and financial reports shall be reviewed monthly by management.

9. VENDOR & THIRD-PARTY SECURITY

- Vendors with system access must comply with Agency cybersecurity standards.
- Contracts shall include data protection and breach notification requirements.
- Third-party remote access shall be restricted, monitored, and disabled when not in use.

SECTION B: TRAINING & MONITORING

10. CYBERSECURITY TRAINING

- All employees shall receive cybersecurity awareness training at hire and periodically thereafter.
- Training topics shall include:
    - Phishing and social engineering
    - Password security
    - Protection of employee data
    - Reporting suspicious activity
- Employees with elevated access shall receive additional role-based training.

11. MONITORING & RISK MANAGEMENT

- Network activity and system logs shall be monitored for suspicious activity.
- Periodic risk assessments shall be conducted.
- Internal controls and cybersecurity practices shall be reviewed annually.
- Vulnerability scans or security assessments shall be conducted as resources allow.

SECTION C: INCIDENT RESPONSE

12. INCIDENT REPORTING

All employees and contractors must immediately report:

- Suspected Phishing or Ransomware
- Unauthorized system access
- Data breaches
- Lost or stolen devices containing Agency data
- Disruption to operational or fare systems

Reports shall be made to IT and the appropriate supervisor without delay.

13. INCIDENT RESPONSE PROCEDURES

Upon identification of a cybersecurity incident:

1. Affected systems shall be isolated to prevent further compromise.
2. The IT Manager (or designee) shall assess scope and impact.
3. Passwords and credentials shall be reset as needed.
4. The General Manager and Board leadership shall be notified.
5. Law enforcement and regulatory agencies shall be notified when required.
6. Service continuity plans shall be activated if transit operations are impacted.
7. A post-incident review shall be conducted, and corrective actions implemented.

14. BUSINESS CONTINUITY & DISASTER RECOVERY

- The Agency shall maintain a Business Continuity Plan (BCP).
- Critical operational systems shall have documented recovery procedures.
- Backup restoration processes shall be periodically tested.

15. ENFORCEMENT

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

Approved by Rancho Murieta Community Services District Board of Directors	Adopted