Rivergrove Water District
Cybersecurity Policy

Policy Brief & Purpose

This cybersecurity policy outlines the Rivergrove Water District's guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks, and system malfunctions could cause severe operational and financial damage to our District.

The District recognizes there are unique protection measures for different system architects. To mitigate cyber threats and ensure the integrity of our information, this policy implements security measures to lessen the impact of a cyberattack and provides instructions to reduce certain security risks.

Scope

This policy applies to all employees, volunteers, and anyone who has permanent or temporary access to the systems and hardware of the District.

For the purpose of defining District systems and hardware, this includes:

- SCADA (Supervisory Control & Data Acquisition)
- CUSI (Utility Billing System)
- QuickBooks (Accounting Software)
- Electronic files (Email and other official digital information)

Policy Elements

- **Confidential data**

Confidential data is considered secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers, vendors, employees, and volunteers
- Patents, formulas, or new technologies
- Customer lists (existing and prospective)

All employees are obligated to protect confidential data and avoid security breaches by following District policies.

- **Protect personal and company devices**

When employees use their digital devices to access District emails or accounts, they introduce security risks to our data. Employees are required to keep both their personal and company-issued computer, tablet, and cell phone secure by following these protocols:

- Keep all devices password protected.
- Upgrade antivirus software as directed.
- Do not leave devices exposed or unattended.
- Install security updates on browsers and systems as soon as updates are available.
- Log into District accounts and systems through secure and private networks only.

Employees will avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new District employees receive company-issued equipment, they will receive instructions for establishing:

- Login and password management tool setup.
- Other guidance intended to protect the device(s).

- **Keep emails safe**

Email communication can often host scams and malicious software (e.g., worms.) To avoid virus infection or data theft, employees will:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g., offering prizes, advice).
- Check email and names of people they receive messages from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks).

If an employee is not completely sure that an email they receive is safe, they should immediately contact the District's IT Support Contractor: Pacific Office Automation, 1-888-770-0498.

- **Manage passwords properly**

Password leaks are dangerous since they can compromise the District's entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, employees will:

- Choose passwords with at least eight characters (including capital and lowercase letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays).
- Remember passwords instead of writing them down. If an employee needs to write down their passwords, they are obligated to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when necessary. If credentials cannot be exchanged in person, employees should use the phone instead of email, and only if they personally recognize the person they are talking to.
- Change passwords every two months.

Remembering numerous passwords can be daunting. Try the following tips to create strong passwords:

1. Do not use letters and numbers in sequence.
2. Combine letters, numbers, and symbols that have at least eight characters.
3. Refrain from using your name and never use your birthdate.
4. Do not use related information and steer clear of using family members' names and birthdays, pet names, addresses, or hobbies.
5. Avoid using common passwords.
6. Stop reusing your passwords. Every time you create a new password, do not use previously used or similar passwords from other accounts.
7. Stronger passwords can also be a long passphrase where you combine multiple words into a long string of at least 15 characters. Example: Picklesgrowhair
8. Refrain from changing just one digit whenever you update your password every 60-90 days. Example: MyG@laxyPassw0rd01, MyG@laxyPassw0rd02

Compromised passwords are responsible for 81% of hacking-related breaches according to the Verizon Data Breach Investigations Report. Password choices are your first line of defense against hacks and cyberattacks. A strong password is your best defense in safeguarding data.

- **Transfer data securely**

Transferring data introduces security risks. Employees will:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless necessary. When mass transfer of data is needed, employees will notify the General Manager **before** any transfer is made. The General Manager will authorize approval or consult with Pacific Office Automation if deemed appropriate.

- Share confidential data over the company network/system and **not** over public Wi-Fi or private connection.
- Ensure the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches, and hacking attempts.

Pacific Office Automation, 1-888-770-0498, will be immediately notified of any scams, breaches, or malware so they can better protect our infrastructure. Employees will report perceived attacks, suspicious emails, or phishing attempts as soon as possible. Pacific Office Automation will investigate all concerns promptly, resolve the issue, and send a District-wide alert when necessary.

Pacific Office Automation is responsible for advising District employees on how to detect scam emails. Employees will contact Pacific Office Automation with questions or concerns.

- **Additional measures**

To reduce the likelihood of security breaches, employees will:

- Not visit social media sites at work.
- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to the General Manager.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Pacific Office Automation serves as the District's security specialist and network administrator. They will:

- Install firewalls and anti-malware software, and access authentication systems.
- Arrange security training for all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Thoroughly investigate security breaches.
- Follow District policy provisions as employees do.

- **Remote employees**

When authorized by the General Manager to work remotely, District employees will follow this policy in its entirety. Since remote work entails accessing the District's accounts and systems from a distance, employees are required to follow all data encryption, protection standards and settings, and ensure their private network is secure. Pacific Office Automation will be consulted for additional advice and instructions.

- **Disciplinary Action**

The District expects all employees to follow this policy. Any employee that fails to comply, to include those who cause security breaches, may face the following disciplinary action:

- First-time, unintentional, small-scale security breach: The employee will receive a verbal warning and security training.
- Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): The employee will receive more severe disciplinary action up to and including termination.

The District will examine each security incident on a case-by-case basis. Any employee who is observed disregarding these security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

- **Take security seriously**

Cybersecurity is as important as technology. Everyone…from our customers and partners to our employees and contractors…should feel that their data is safe. The advancement of technology has left many people vulnerable to cybercriminal activities, such as hacking, data theft and damage, and industrial espionage. It is our responsibility to be proactive and protect our systems and databases. We can do this by staying vigilant and keeping cybersecurity a top priority.

Janine Casey
General Manager
Rivergrove Water District