EL DORADO COUNTY FIRE PROTECTION DISTRICT

STANDARD OPERATING GUIDELINE

ARTICLE 2: ADMINISTRATIVE POLICIES	**EFFECTIVE DATE: 03-18-2021**
SECTION 34: DISTRICT EMAIL USAGE	**REVISED:**

2.34.1 **PURPOSE:** Our District email usage Standard Operating Guideline helps authorized users manage their District email addresses appropriately. Email is essential to our everyday jobs. We want to ensure that our staff understands the limitations of using their District email accounts.

Our goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

2.34.2 **SCOPE:** This policy applies to all staff, firefighters, board members, vendors and partners who are assigned (or given access to) a District email. This email may be assigned to an individual (e.g., name@eldofire.com) or department/role (e.g., info@eldofire.com.) For this policy, "staff" will refer to District administrative staff, firefighters, board members, vendors and partners utilizing the district email system.

2.34.3 **SOG ELEMENTS:** District emails are powerful tools that help staff in their jobs. Staff should use their District email primarily for work-related purposes. However, we want to provide staff with some freedom to use their emails for personal reasons. We will define what constitutes appropriate and inappropriate use.

2.34.4 **Inappropriate use of District email:**

Our staff represent our District whenever they use their District email address. They must not:

- Sign up for illegal, unreliable, disreputable, or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.
- Use a District email address to send confidential information without authorization.
- Send offensive or inappropriate emails to the public, colleagues, or business partners.
- Use a District email for an illegal activity.

2.34.5 **Appropriate use of District email:**

Staff must be mindful of their obligations to preserve confidentiality and the privacy of individuals assisted by the District and other employees.

Staff is allowed to use their District email for work-related purposes without limitations. For example, staff can use their email to:

- Communicate with fire departments, district related vendors and job-related resources.
- Log in to software and websites for district training, resources, and job-related items.
- Give their email address to people they meet at conferences, board meetings, or other District events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

2.34.6 Personal use:

Staff is allowed to use their District email for some personal reasons. For example, staff can use their District email to:

- Register for classes or meetups.
- Send emails to friends and family as long as they do not spam or disclose confidential information.
- Download eBooks, guides, and other content for their personal use as long as it is safe and appropriate.

Staff must adhere to this policy at all times.

2.34.7 No expectation of privacy in use of District email:

Staff should have no expectation of privacy in their use of District email, even if the District email is used for personal reasons. The District may monitor and archive District email without prior notice. Additionally, many emails or portions of emails may constitute "public records" subject to public disclosure if they fall within the scope of a request for public records.

All Board of Director emails, xxxx@eldofire.com, shall reside on District email servers. In the event of a public records request or other scenarios that may require access to current or previous Board Members email accounts, the Fire Chief shall notify the Board Chair or Vice Chair of the nature of the request and/or need to access these emails. The Board Chair or Vice Chair may elect to notify the involved Board Member(s) of the inquiry.

2.34.8 Email Security:

Email is often the medium of hacker attacks, confidentiality breaches, viruses, and other malware. These issues can compromise our reputation, legality, and security of our equipment.

Staff must:

- Select strong passwords with at least ten characters (capital and lower-case letters, symbols, and numbers) without using personal information (e.g. birthdays.) or other terms that may be inappropriate for use as a password.
- Remember passwords instead of writing them down and keep them secret.
- Change their email password immediately any time you feel it has been compromised in any way.

Also, staff should always be vigilant to catch emails that carry malware or phishing attempts. We instruct staff to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g., "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If any staff isn't sure that an email, they received is safe, they can ask our IT Team at RTS.

We remind our members to be mindful of their anti-malware programs, and alert IT if you suspect it is disabled or in some way not working.

2.34.9 Email Signature:

All District email users should use an email signature that exudes professionalism and represents our District well. Senior personnel who represent our District to the public should pay special attention to how they close emails.

If members are unsure how to set up an email signature, they can ask for help from our Administrative or IT personnel.