MEETING DATE: February 5, 2025

AGENDA ITEM: 8. Beckwourth Peak FPD - Policies - Review and Possible Approval of 7 Policies

FROM: Cary Curtis

RE: Beckwourth Peak FPD - Policies - Review and Possible Approval of 7 Policies

---

BACKGROUND:

The Policy Committee has 7 policies to present to the Board for their review and possible approval. These policies are designed to ensure the District is in compliance with CA Code and Law and District direction and processes.

EXECUTIVE SUMMARY:

The Policy Committee has worked up the following policies for the board's review and possible approval. We have provided a synopsis of each of the policies -

Conflict of Interest Policy 1035 - We need a standard conflict of interest policy that supports the Conflict-of-Interest Code the board passed by the attached Resolution 2024.06 dated July 3, 2024, and to ensure we are continually compliant with filing requirements. The COI Code is required to be updated every two years and submitted to Plumas County. The COI Code is the basis for our Form 700 filing.

Purchase Order Policy 2142 - This policy is needed to ensure consistency with when a PO is required and outlines steps to follow to execute one. There is a CSDA policy that is not as comprehensive and clear as this draft. Nothing exists in the Lexipol policies.

Bill Pay - Invoice Processing and Payment Requirements 2141 - This policy is needed to ensure consistency with the flow of tracking and approving invoices for payment. There is not a comparable policy in CSDA or Lexipol. This policy includes processing procedures that can easily be followed by the Administrative Assistant or anyone else who needs to step in to cover.

Information Technology 2205 - This policy was first presented to the Board at the November 6, 2024, meeting for a first reading where the Board provided direction to the Committee to obtain legal counsel review and input. The District's legal counsel BBK has reviewed and edited the policy that is now presented for a second reading. This policy is needed to comply with CA cyber security laws, to establish prudent responsibilities for how IT resources are used, and it provides guidance to protect the District from cyber-attacks. The

final draft with legal edits is included.

Social Media Policy 2415 - At our January 2025 meeting, the Board discussed setting up a BPFPD Facebook site and to do so, we need a policy to set the standards and requirements for how that site is used. CSDA has a template policy that has been used. However, to ensure there was no overlap with CSDA and Lexipol policies, the Committee reviewed 5 Lexipol policies that are on the books and 3 possible non-booked CSDA policies. This policy is comprehensive and provides great guidance. CSDA policy templates have peer and legal review completed.

CA Request for Public Records Act 2425 and Request Form - This is a required policy and must be followed to be in compliance with CA code and law. The Committee used the CSDA template to create this policy. Lexipol has a policy however it is not specific to CA code. This brings us into compliance and the policy outlines the steps to follow and timing of communications. Also attached a standard request form that supports complying with the request.

Types of Board Meetings 4235 - This policy was originally adopted on July 3, 2024. This is a modification to the Policy due to the Board's action to change our regular meeting calendar to bi-monthly, starting April 2, 2025. The new meeting schedule beginning in April will be the first Wednesday at 6pm during the months of February, April, June, August, October and December.

RECOMMENDATION:

Review, discuss and provide feedback and direction for the seven policies presented. Consider adopting some or all policies as presented by the Policy Committee.

FISCAL IMPACT:

Adopting appropriate policies has a positive impact to the District as it allows for adhering to compliance requirements and potentially reduces exposure to losses.

ATTACHMENTS:

A. 1035 CONFLICT OF INTEREST POLICY DRAFT 2.5.25
B. BPFPD CONFLICT OF INTEREST RESOLUTION 2024.06

C. 2141 BILL PAY INVOICE PROCESSING AND PAYMENT REQUIREMENTS 2.5.25 DRAFT
D. 2142 PURCHASE ORDER POLICY 2.5.25 DRAFT
E. 2205 INFORMATION TECHNOLOGY POLICY 2.5.25 DRAFT
F. 2415 SOCIAL MEDIA 2.5.25.DRAFT
G. 2425 CA. REQUEST FOR PUBLIC RECORDS ACT 2.5.25 DRAFT
H. 2425 CA. REQUEST FOR PUBLIC RECORDS ACT REQUEST FORM 2.5.25 DRAFT
I. 4235 TYPES OF BOARD MEETINGS REVISED 2.5.25

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: Conflict of Interest

POLICY NUMBER: 1035

1035 – Conflict of Interest

1035.1 The Political Reform Act, Government Code §81000, et seq., requires state and local government agencies to adopt and promulgate conflict-of-interest codes. The Fair Political Practices Commission ("FPPC") has adopted a regulation (2 Cal. Code of Regs. §18730) which contains the terms of a standard conflict of interest code. It can be incorporated by reference and may be amended by the FPPC after public notice and hearings to conform to amendments in the Political Reform Act.

1035.2 Therefore, the terms of 2 Cal. Code of Regs. §18730 and any amendments to it duly adopted by the FPPC are hereby incorporated by reference and, along with the attached Resolution #2024.06 adopted by the Beckwourth Peak Fire Protection District Board of Directors and updated bi-annually, and in which members of the Board of Directors and employees designated, and in which disclosure categories are set forth, constitute the conflict-of-interest code of the Beckwourth Peak Fire Protection District.

1035.2 The District Clerk shall file and retain statements of economic interests in the District office.

Adopted:

Phone: Station 1 (530) 832-1008
Fax: (530) 832-5828
fireprotectplumas@gmail.com
180 Main St. Beckwourth, CA 96129

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

RESOLUTION NO. 2024.06

RESOLUTION OF THE BOARD OF DIRECTORS OF THE BECKWOURTH PEAK FIRE PROTECTION DISTRICT TO ADOPT A CONFLICT OF INTEREST CODE PURSUANT TO THE POLITICAL REFORM ACT OF 1974

WHEREAS, the State of California enacted the Political Reform Act of 1974, Government Code Section 81000 et seq. (the "Act"), which contains provisions relating to conflicts of interest which potentially affect all officers, employees and consultants of the Beckwourth Peak Fire Protection District (the "District") and requires all public agencies to adopt and promulgate a Conflict of Interest Code; and

WHEREAS, the potential penalties for violation of the provisions of the Act are substantial and may include criminal and civil liability, as well as equitable relief which could result in the District being restrained or prevented from acting in cases where the provisions of the Act may have been violated; and

WHEREAS, notice of the time and place of a public meeting on **July 3, 2024**, and of consideration by the Board of Directors of the District, the proposed Conflict of Interest Code was provided to each designated employee and publicly posted by the District for review; and

WHEREAS, a public meeting was held upon the proposed Conflict of Interest Code at a regular meeting of the Board of Directors in **July 3, 2024**, at which all present were given an opportunity to be heard on the proposed Conflict of Interest Code.

NOW, THEREFORE, BE IT RESOLVED by the Board of Directors of the Beckwourth Peak Fire Protection District does hereby adopt the proposed Conflict of Interest Code, a copy of which is attached hereto and shall be on file with the Administrative Officer and available to the public for inspection and copying during regular business hours;

BE IS FURTHER RESOLVED that the said Conflict of Interest Code shall be submitted to the Plumas County Board of Supervisors for approval and said Code shall

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: Bill Pay – Invoice Processing and Payment Requirements

POLICY NUMBER: 2141

2141 Bill Pay – Invoice Processing and Payment Requirements

Purpose:

The purpose of this policy is to establish clear procedures for the timely and accurate payment of invoices, ensuring that all payments are authorized, and supported by necessary documentation.

Policy:

2141.1 To ensure transparency, accountability, and proper recordkeeping, the following procedures must be followed for entering invoices and processing payments:

2141.2 Invoice Entry Requirements
Invoices must be submitted with the following information before processing:

- Vendor Information: Correct vendor name, address, and contact details.
- Invoice Number: A unique invoice number to help track and verify payments.
- Invoice Date: The date the invoice was issued by the vendor.
- Description of Goods/Services: Clear and detailed description of the goods or services provided.
- Amount Due: The exact amount due for payment, including taxes, shipping, and other fees if applicable.
- Payment Terms: The due date and any discounts for early payment or penalties for late payment.
- PO Request Number: If applicable, the invoice should reference the associated Purchase Order Request (PO).
- Approved Signature: The invoice must be approved by the Fire Chief or his designee before submission for payment.

2141.3 Documentation Required for Payment:
For an invoice to be processed for payment, the following supporting documentation must be provided:

- Valid Invoice: As outlined above.
- Purchase Order Request (PO): Required for all payments. The PO must match the invoice amount and be signed by the authorized requester.
- Approval Signatures: The invoice must have the proper approval signatures

POLICY TITLE: Bill Pay – Invoice Processing and Payment Requirements

POLICY NUMBER: 2141

from the Fire Chief or his designee.

- Receiving Report (if applicable): A signed receiving report that confirms the goods/services have been delivered or rendered in accordance with the terms of the purchase.
- Contract/Agreement (if applicable): If the payment is based on a contract, a copy of the relevant contract or agreement should be attached to the invoice.

2141.4 Invoice Submission and Payment Process

- Invoice Submission: Invoices should be submitted to the District Administrative Assistant.
- Invoice Review: Administrative Assistant will verify the invoice details, including matching with the PO, receiving reports, and approval signatures.
- Discrepancies: Any discrepancies between the invoice and supporting documents (e.g., incorrect amounts, missing signatures, or unapproved POs) must be resolved before processing the payment.
- Payment Processing: Once the invoice is verified, the Administrative Assistant will process the invoice for payment.
- Payments will be made via check, ACH transfer, or other authorized payment methods.

2141.5 Late Payments and Penalties

- Late Payments: Invoices must be submitted on time to ensure payments are processed within the vendor's required timeframe. If an invoice is submitted late or without the necessary supporting documentation, the payment may be delayed.
- Penalty for Non-Compliance: If invoices are not submitted with the proper backup documentation, they may be delayed until all requirements are met.
- Repeated failure to comply with the invoice entry requirements could result in additional scrutiny or process delays.

2141.6 Payment Approval Workflow

- Initial Review: The Administrative Assistant will conduct an initial review to ensure the invoice matches the PO and that all documentation is attached.
- District Approval: The Fire Chief or his designee must sign off on invoices before payment of the invoice.
- Final Payment Approval: The final approval for payment will be given by the Fire Chief.

POLICY TITLE: Bill Pay – Invoice Processing and Payment Requirements

POLICY NUMBER: 2141

- Authorization: Beckwourth Peak FPD requires all checks for payment of invoices are signed by two authorized signers as captured on the Plumas Bank signature card.

2141.7 Exceptions

In certain cases, exceptions to this policy may be granted with prior approval from the Fire Chief. Any exceptions must be documented and kept on record.

Adopted:

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: Purchase Order Policy Requirements

POLICY NUMBER: 2142

2142 Purchase Order Policy Requirements

Purpose:
2142.1 This policy outlines the procedures for initiating and approving purchase orders (POs) to ensure responsible fiscal management and compliance with budgetary constraints.

Policy:
2142.2 All purchases must be made using a purchase order when the total cost of items exceeds $500.00. This ensures proper approval, documentation, and budget tracking. Routine invoices and bills are exempt from this policy and include, but are not limited to, utility billings, routine facility expenses, subscriptions, fuel and any regular or routine purchase made.

In contrast, a PO is required and includes, but is not limited to Capital Fund expenses, Grant disbursement expenses, equipment orders and vehicle orders.

The Fire Chief is to be consulted whenever there is a question related to when a PO is required.

2142.3 Procedures for Purchase Order Request

- Threshold: A purchase order request must be initiated for any single item or cumulative items totaling over $500.00.
- Request Form: Complete a Purchase Order Request Form, including description of items or services needed:
    1. Justification for the purchase
    2. Estimated total cost
    3. Fire Chief approval

2142.4 Submission Process

- Submit the completed Purchase Order Request Form to the Administrative Officer.
- Ensure that all required documentation (quotes, specifications) is attached.

2142.5 Approval Process

- The Fire Chief will review the request for compliance with budgetary constraints and appropriateness of the purchase.

POLICY TITLE: Purchase Order Policy Requirements

POLICY NUMBER: 2142

2142.6 Issuance of Purchase Order

- Upon approval, the Administrative Assistant will issue a purchase order number. The purchase order will be sent to the vendor, along with any necessary terms and conditions.

2142.7 Payment Process

- Once verification is complete, submit the invoice to the Administrative Assistant for payment processing, referencing the purchase order number.

2142.8 Receiving Goods/Services

- Upon receipt of the goods or services, the department must verify that they match the purchase order.
- Report any discrepancies to the Administrative Assistant or Fire Chief immediately.

2142.9 Record Keeping

- Maintain copies of purchase orders, invoices, and any related documentation for auditing purposes.

2142.10 Exceptions

- Emergency purchases that exceed $500.00 may be made without a purchase order but must receive the approval of the Fire Chief and documented.

2142.11 Review and Amendments

- This policy may be amended as necessary to reflect changes in district needs or regulatory requirements.

Adopted:

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: Information Technology Security Policy

POLICY NUMBER: 2205

2205.1 Policy Purpose:

The purpose of this Beckwourth Peak Fire Protection District ("BPFPD" or "District") Information Technology Security Policy "("Policy") is to establish standard operating procedures, guidelines, and boundaries for the use of the District's network and to ensure that BPFPD personnel use computing technology in a responsible, efficient, ethical, and legal manner. This Policy also prevents the unauthorized access to or disclosure of sensitive information prepared, owned, used, or retained by the District.

The more we rely on technology to collect, store and manage information, the more vulnerable the District becomes to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage to the District and community and may jeopardize the District's reputation and the public's trust. For this reason, this Policy implements a number of security measures and provides instructions that mitigate security risks.

Effective implementation and adherence to this Policy will help protect the integrity of the District's network and minimize unauthorized access to the District's computing resources.

2205.2 Scope:

Effective information technology security is a team effort involving the participation and support of all employees, contractors, consultants, volunteers and other workers at BPFPD and any affiliate who deals with District information or information systems. This Policy applies to all District employees, contractors, consultant, volunteers, and anyone also has been granted by the District permanent or temporary access to District systems and hardware (collectively, "Users").

2205.3 Other District Policies:

Complimentary policies may exist that address areas of information security including policies on Internet use, Email, vendor-contractor access, and portable computing. All District policies shall be abided by at all times. In the case of any conflict between this Policy and another, whichever provides greater protection of District systems shall guide.

2205.4 District Technology Assets:

This Policy applies to the use of all District electronic devices, including, but not limited to - computers, laptops, printers, fax machines, telephones, other mobile devices, removable devices including USB flash drives, hard drives, and software, as well as all District information and communication systems such as internet, email, and voicemail (collectively, “Devices”). These Devices are the property of the District and must be used in accordance with all District policies, standards, and guidelines, including this Policy.

2205.5 User Responsibility and Acceptable Use:

Users are prohibited from accessing or using District Devices in a manner that risks exposing the District to virus attacks, security breaches, or other compromises of District systems and services.

Acceptable and prohibited uses of District Devices are discussed below. This is not an exhaustive list of acceptable and prohibited uses but instead, attempts to provide a framework to encourage Users to employ common sense and good judgment. Any question about Device use should be discussed with the Fire Chief prior to executing the use.

2205.5.1 Privacy of Personal Data:

For legal and liability reasons, all data and electronic messages on District Devices, including information accessed via the internet and sent or received through electronic mail (email) systems, are the property of the District.

a) All Users are aware that all data and information on District Devices is the property of the District. This may include data and information on personal devices connected, linked, or otherwise used in conjunction with District Devices.
b) All records on District Devices or related to District matters, whether paper or electronic, may be subject to public disclosure under the California Public Records Act, Government Code section 7920.000 et seq., or discovery in a court of law.
c) When Users use their personal digital devices to access District emails or accounts, they introduce security risk to the District’s data. The District strongly encourages Users to keep both their personal and District-issued Device(s) secure and separate.

2205.5.2 *Manage Passwords Properly:*

Password leaks can compromise District infrastructure by giving negligent or nefarious hackers the ability to tamper with or disable District information and services. Passwords on District Devices should be complex, in line with the below requirements, and be kept secret.

a) Passwords shall be (1) at least eight characters, (2) include at least one capital letter, one lowercase letter, one number, and one symbol, and (3) avoid information that can be easily guessed (e.g., birthdays).
b) Passwords shall not be written down, except when stored in a secure password manager (e.g. Bitwarden, password-protected document).
c) Passwords shall be changed at least every two (2) months.
d) Passwords or other credentials shall not be shared, except when approved by the Fire Chief and for a specific amount of time. At the conclusion of the designated time, the original User shall promptly change their password.

2205.5.3 *Keep Devices Secure:*

Losing a Device or compromising a Device's security is a serious risk to the District. Users shall comply with the following to keep Devices secure.

a) A Device shall only be used by the person it is individually issued to, unless expressly authorized by the Fire Chief. Users are responsible for managing and protecting any information used on or stored in their Device.
b) Devices shall be kept password-protected and locked at any time not in use.
c) Devices shall not be left unattended. Permanently-fixed Devices shall be locked or turned off any time the User leaves or is not using the Device.
d) Immediately report stolen or damaged Devices to the Fire Chief. Immediately change all District account passwords on a stolen Device.
e) Devices shall be maintained with all anti-virus software recommended by the District. Additional anti-virus may also be installed, with the Fire Chief's permission.
f) District Devices shall only be accessed through secure and private networks.
g) Users shall not download any unauthorized software on District Devices.
h) Users shall not open or download webpages, emails, links, documents, or other information from an unrecognized source or unsolicited project (e.g., the subject is not relevant to District work). If a User is suspicious, always double check with an email sender by calling them.
i) Users shall be immediately suspicious of any unsolicited emails. Users shall also check email and names of people who send messages to ensure they are legitimate. (e.g., Outlook shows "Jane Doe", a known consultant, but the email card shows it came from "j@ned0w1234@hotmail" is suspicious).
j) Users shall be suspicious of clickbait titles (e.g., offering prizes, unsolicited advice) and inconsistencies or giveaways (e.g., grammar mistakes, odd phrasing, capital letters, excessive number of exclamation marks).
k) Immediately report any suspicious webpages, emails, links, documents, or other information received or on District Devices to the Fire Chief.

l) Users shall comply with all District social media and internet usage policies, and other policies applicable to Device use.
m) The Fire Chief, at his or her discretion, may permit exceptions to these rules on a case-by-case basis.

2205.5.4 *Transfer Data Securely:*

Transferring data can be a security risk to the District and general public. Users shall comply with the following to keep data secure.

a) Transferring personal data is prohibited, except when within the scope of the User's work, the recipient has been verified, and the transfer is absolutely necessary (e.g., human resources consultant transferring personnel records to the Fire Chief, finance director transferring customer information to a customer who verified themselves). In the case of more than one person's data is to be transferred or the situation is unique for other reasons, Users are required to confer with the Fire Chief for direction.
b) Verify that the recipient of the data is an authorized person or organizations and has adequate security policies.
c) Transfer data in a manner and format that maximizes the District's security (e.g., download and send a PDF with metadata scrubbed rather than a Word document)
d) Report scams, privacy breaches and hacking attempts to the Fire Chief.
e) Manage passwords in accordance with this Policy and change them frequently.

2205.5.5 *Electronic Document, Software and Mail Storage:*

Improper management of documents and email can compromise the District. Users shall comply with the following regarding electronic documents, software, and emailing.

a) All documents and other data created or maintained by the User should be saved on the "C" Drive, or District-approved cloud storage, rather than local drives, unless directed by the Fire Chief, or designee.
b) Email should only be used for conducting District business and transmitting District information. Using District email for personal reasons is strictly prohibited.
c) Email should not be used for preserving information for future reference. Communications, attachments, documents, and other information in email or other temporary source and needed for future reference should be downloaded and electronically filed on the "C" Drive, or other electronic archive designated by the Fire Chief, or printed and physically filed.
d) Users shall use the District signature block when emailing within the scope of their work for the District. The signature block shall be at the end of all messages. The block must be in a format, type, and color approved by the Fire Chief, or designee. Generally, the

block should include the sender's name, title, the District's name, direct telephone number, fax number, and District website address.

2205.6 Prohibited Activities and Uses of Information Technology:

The following activities are prohibited on District Devices, except when expressly authorized by the Fire Chief in advance and necessary for the User's District job function.

a) Creating security breaches including, but not limited to, unauthorized access, alteration, destruction, removal or disclosure of data, information, equipment, software, or systems (e.g., sharing passwords or Devices).
b) Installing software on the District's Devices not authorized by the Fire Chief (e.g., freeware, specialized editing software).
c) Adding to, or using with, any District Devices any unauthorized hardware devices (e.g., connecting to personal tablets, smartphones or wireless access points).
d) Downloading, installing, or running any programs or services that provide ongoing communications with the Internet which have not been approved by the Fire Chief, including but not limited to instant messaging, screen savers, peer to peer communications, and all streaming media (e.g., using a VPN, streaming Netflix).
e) Using Devices and District resources for non-District purposes (e.g., commercial purposes, personal gain, political campaigns, religious or political causes, chain letters). Note this is expressly prohibited by law as a gift of public funds.
f) Sending unencrypted confidential documents via the Internet without direction of the Fire Chief.
g) Disclosing, or requesting disclosure of, passwords, personal identification information, account information, device access, or similar sensitive information without the approval of the Fire Chief, or designee (e.g., customer data, HR records).
h) Speaking on behalf of the District unless authorized to do so, via electronic communication or otherwise.
i) Any Device uses that violate Local, State, or Federal laws or regulations.

2205.7 Fire Chief Responsibilities:

It is the responsibility of the Fire Chief to ensure computing systems are secure and to mitigate the opportunity and threat of data theft and breaches. Due to the rapidly changing nature of technology and its impact on the workplace the District's Fire Chief or designee will:

a) Review this Policy annually and recommend any necessary changes to the Board President.
b) Establish and authorize a standard signature block for users.
c) Ensure firewalls, anti-malware software, and access authentication systems are installed and maintained.

d) Ensure Users back-up District databases daily, weekly, monthly, quarterly and annually for archival and retrieval purposes by sending out regular reminders to do so.
e) Annually, provide this Policy and Information Technology security training to all District Users, and within 30 days of start to all new Users.
f) Inform Users regularly about new scam emails or viruses and ways to combat them.
g) Ensure remote Users have authorization to work remotely and that they must follow this policy and instructions.
h) Engage with the District's IT consultant to assist in evaluating District functional needs and recommend appropriate options for improvement of District technology resources.
i) Partner with IT consultants to provide any necessary on-site training and consulting advice on approved software and make recommendations as appropriate.
j) Ensure IT consultants set up and assist with maintaining an on-site office automation library of proven and reliable software and hardware requiring minimal technical support that is easy to use, enhances District productivity, and is compatible with District technology systems.
k) All requests for deviation from this Policy must be stated in writing that an exception waiver has been approved by the Fire Chief or their designee, and that the written approval includes a statement of how the risk has been mitigated.
l) The Fire Chief or designee is responsible for maintaining documentation of all variances to this policy and reporting variances to the Board President annually.
m) Investigate security breaches thoroughly.
n) Engage with the District's IT consultant to ensure all suspected breaches and data theft are investigated and action is taken to eliminate any recurrence.

2205.8 Disciplinary Action:

Users shall comply with this Policy at all times. Failure to abide by the Policy may result in discipline up to and including termination. Discipline shall be determined on a case-by-case basis by the Fire Chief but shall generally abide by the following parameters.

a) First-time, unintentional, or small-scale Policy violation – the Fire Chief may issue a verbal warning and train the employee in security.
b) Intentional, repeated or large-scale Policy violation or breaches, such as those that cause severe financial or other damage – the Fire Chief may invoke more severe disciplinary action up to and including termination or removal from position.
c) Users who are observed to disregard the District's security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

Adopted:_____

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: Social Media Use

POLICY NUMBER: 2415

2415 - Social Media Use

Purpose:

2415.1 The policy outlines the protocol and procedures for use of social media to publicize District services and events. In addition, this policy addresses the responsibilities of employees and District officials regarding social media and the use of District resources (time/equipment), as well as responsibilities related to public records and open meeting laws.

Definitions:

2415.2

a) Social Media: Various forms of discussions and information-sharing, including social networks, blogs, video sharing, podcasts, wikis, message boards, and online forums. Technologies include picture sharing, wall-postings, fan pages, email, instant messaging and music-sharing. Examples of social media applications include but are not limited to Google and Yahoo Groups, (reference, social networking), Wikipedia (reference), Facebook (social networking), YouTube (social networking and video sharing), Flickr, (photo sharing), Twitter (social networking and microblogging), LinkedIn (business networking), and news media comment sharing/blogging.

b) Social Networking: The practice of expanding business and/or social contacts by making connections through web-based applications. This policy focuses on social networking as it relates to the Internet to promote such connections for District business and for employees, elected and appointed officials who are using this medium in the conduct of official District business.

c) “Posts” or “postings” means information, articles, pictures, videos, or any other form of communication posted on a District social media site.

Policy:

2415.3 No District social media site may be created without the approval of the Fire Chief or his or her designee. All District social media sites created on behalf of the District, by its employees on District time, or using other District resources are the property of the District and shall be administered and regularly monitored by the Fire Chief or his/her designee. These social media sites shall be used only to inform the public about District business, services and events. The

POLICY TITLE: Social Media Use

POLICY NUMBER: 2415

District's web site, bpfpd.ca.gov, will remain the primary location for content regarding District business, services and events. Whenever possible, links within social media formats should direct users to the District web site for more information, forms, documents, or online services necessary to conduct business with the District. District social media sites shall clearly state that such sites are maintained by the District and that the sites comply with this Social Media Policy.

2415.3.1

District employees and appointed and elected officials shall not disclose information about confidential District business on the District's social media sites, personal social media sites, or otherwise. In addition, all use of social media sites by elected and appointed officials shall be in compliance with California's open meeting laws, which prohibit serial meetings of a majority of the Board or another legislative body of the District via email or other electronic means. Members of the Board, committees and/or legislative bodies shall not respond to, "like", "share", retweet, or otherwise participate in any published postings, or use the platform or any form of electronic communication to respond to, blog or engage in serial meetings, or otherwise discuss, deliberate, or express opinions on any issue within the subject matter jurisdiction of the body on which they serve. Employees and elected or appointed officials' posts to non-District social media sites are a reflection of their own views and not necessarily those of the District and should not suggest otherwise.

2415.4 Posting/Commenting Guidelines:

a) All postings made by the District to social media sites will contain information and content that has already been published or broadcast by the District. The District will not comment on other social media member's sites. All official social media postings by the District will be done solely on the District's social media sites or in response to postings made on the District's social media sites. Officers, employees and agents of the District representing it on District social media sites shall conduct themselves professionally and in accordance with all District policies. All District social media sites shall use authorized District contact information for account set-up, monitoring and access. Personal email accounts or phone numbers may not be used to set up, monitor, or post to a District social media platform.

POLICY TITLE: Social Media Use

POLICY NUMBER: 2415

b) The District reserves the right to remove from its social media sites content that it finds to violate this policy or applicable law, consistent with Federal and State law.

c) The District will only post photos for which it has copyright or the owner's permission.

d) District social media platforms are subject to the California Public Records Act. Any content maintained on a District social media site that is related to District business, including a list of subscribers, posted communication, and communication submitted for posting, may be considered a public record and subject to public disclosure. All postings on District social media sites shall be sent to a District email account and maintained consistently with the Public Records Act, provided, however, that any material removed from a District social media site consistently with this policy shall be considered a preliminary draft, note or memorandum not retained by the District in the ordinary course of business and shall not constitute a public record of the District required to be retained consistently with the District's records retention schedules.

e) The District and its employees will not use chat functions on social media sites.

f) Links to all social media networks to which the District belongs will be listed on the District's website. Interested parties wishing to interact with these sites will be directed to visit the District's web site for more information on how to participate.

g) The District reserves the right to terminate any District social media site without notice or to temporarily or permanently suspend access to District social media as to some or all persons at any time, consistent with point (d) above. The District reserves the right to implement or remove any functionality of its social media platforms, in the discretion of the Fire Chief or his or her designee. This includes, but is not limited to, information, articles, pictures, videos, or any other form of communication that can be posted on a District social media platform.

h) District social media sites may contain content, including but not limited to, advertisements or hyperlinks over which the District has no control. The District does not endorse any hyperlink or advertisement placed on District social media sites by the social media site's owners, vendors, or partners.

POLICY TITLE: Social Media Use

POLICY NUMBER: 2415

i) District employees may post to District social media platforms only during working hours.

j) After-hours or weekend postings may only be made with prior approval of the Fire Chief or his or her designee. Any person authorized to post items on any of the District's social media platforms shall review, be familiar with, and comply with this Policy and each social media platform's terms and conditions of use.

k) Any person authorized to post items on behalf of the District to any of the District's social media platforms shall not express personal views or concerns through such postings. Instead, postings on any of the District's social media platforms on behalf of the District shall only reflect the views of the District.

l) Posts must contain information that is freely available to the public and not be confidential as defined by any District policy or state or federal law.

m) Posts may NOT contain any personal information, except for the names of people available for contact by the public as representatives of the District. Posts to District social media sites shall NOT contain any of the following:

Comments that are not topically related to the information commented upon;

- Comments in support of, or opposition to, political campaigns, candidates or ballot measures;
- Profane language or content;
- Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, or status with regard to public assistance, national origin, physical or mental disability or sexual orientation, or any other category protected by federal, state, or local law;
- Sexual content or links to sexual content;
- Solicitations of commerce;
- Conduct or encouragement of illegal activity;
- Information that may tend to compromise the safety or security of the public or public systems; or
- Content that violates a legal ownership interest of any other party, such as trademark or copyright infringement; or any content that is confidential, sensitive, or includes proprietary information, or that otherwise violates another person's right to privacy.

POLICY TITLE: Social Media Use

POLICY NUMBER: 2415

Procedures:

2415.5 The Fire Chief or his designee will be responsible for responding to comments and messages as appropriate. The District will direct users to the District's web site for more information, forms, documents or online services necessary to conduct business with the District.

2415.5.1 The District may invite others to participate in its social media sites. Whether to permit public participation in social media sites will be based upon the best interests of the District, as determined by the Fire Chief or his or her designee, and the requirements of federal and state law.

Responsibilities:

2415.6 It is the responsibility of employees and appointed and elected officials to understand the procedures as outlined in this policy.

2415.6.1 Employees who are not designated by the Fire Chief to access social media sites for District business are prohibited from accessing social media sites utilizing the District computer equipment and/ or the District's web access. While at work, employees who are not granted access via District systems and computing equipment may use personal computing devices and personal web accounts to access social media sites only during non-working hours such as lunch periods and breaks. State law provides that more than occasional or incidental personal use of District resources is a crime.

2415.6.2 The Fire Chief will determine if a requested use of District social media sites or other District resources is appropriate and complies with this policy.

2415.6.3 All content on District social media sites must comply with District web standards, the rules and regulation of the social media site provider, including privacy policies, and applicable law. Employee or District confidentiality shall be maintained in accordance with all applicable laws and District policies. If a question arises regarding the use or posting of confidential information on a social media site, the matter shall be referred to the Fire Chief. The information

POLICY TITLE: Social Media Use

POLICY NUMBER: 2415

in question shall not be posted, or if already posted, shall be removed until an opinion is rendered by the Fire Chief or, at his or her request, Legal Counsel. Notwithstanding the opinion of the District counsel, the Fire Chief reserves the right to restrict or remove District information from a District social media site if the Fire Chief concludes the information does not serve the best interest of the District.

2415.6.4 All social media-based services to be developed, designed, managed by or purchased from any third-party source for District use requires appropriate budget authority and approval from the Board of Directors.

2415.6.5 The District reserves the right to change, modify, or amend all or part of this policy at any time.

Adopted: _____

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: California Public Records Act Response Policy

POLICY NUMBER: 2425

2425 – California Public Records Act Response Policy

The California Public Records Act (Government Code, section 6250 et seq.) grants California residents important rights to obtain access to records held by public agencies. The District adopts this policy to clarify how it will respond to requests for records under the Public Records Act.

2425.1 All requests for public records shall be in writing on a form approved by the Board of Directors, unless the request is to review an agenda, agenda reports, or minutes of the Board or ordinances or resolutions of the Board or any of its committees, which are available on bpfpd.ca.gov or in the District office.

2425.2 Staff will respond to all requests as soon as possible after they are received, but not later than 10 days after receipt of the request to either state whether the District has responsive records or to request an extension of up to 14 days to make that determination pursuant to Government Code section 6253(c). It is the expectation of the Board that Staff will cooperate fully with the request and act in a considerate and accommodating manner.

a) Staff shall review each request and determine whether it seeks identifiable records. If not, staff shall offer to help the requestor identify records responsive to the request.
b) Staff shall request all Directors and staff who may have the records requested to search their files. Directors and staff must report whether they have responsive records and, if so, when the records can be made available to the requestor.
c) Staff shall respond to the requestor, advising him or her in writing of the availability of the documents, a description of the medium (paper, electronic format, etc.) and location of the records, and whether any are exempt from disclosure under the Public Records Act. To the extent feasible, staff will provide suggestions to overcome any practical basis for denying access to the records sought.
d) If a request is made for copies of records, staff shall also advise the requestor of the estimated copying cost. The District shall make any disclosable records it holds in electronic format available in such format when requested.
e) The person requesting the copies shall pay the charges for the requested copies established by the Board. At present those are: $1.00 for the first page, $.05 each additional page, $.10 per page for Political Reform Act materials. Staff shall not release the copies until the actual copying cost is paid.

POLICY TITLE: California Public Records Act Response Policy

POLICY NUMBER: 2425

f) Staff shall provide a copy of the original form to the Requestor upon completion. Original request forms and documents provided to the Requestor will be filed and maintained in the District for a period of no less than 3 years.

2425.3 In accordance with the Public Records Act, staff will provide specific, identifiable records but will not research records for particular types of information or analyze information which may be contained in public records. Staff have no obligation to create records in response to a Public Records Act request.

2425.4 Staff will respond to requests for public records in accordance with the Public Records Act as the Act now exists or may hereafter be amended, and nothing in this Policy is intended nor shall it be construed to conflict with the terms of the Public Records Act.

Adopted:_____

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

REQUEST FOR PUBLIC RECORDS

Date requested:	Date required:

Please list each document, file, or record separately

I wish to ☐ Review

☐ Obtain copies of the following public records:

I/We, the undersigned, request documents as indicated and agree to pay the [District] for copies at the rate of $1.00 for the first page and $0.05 for each additional page ($0.10 per page for documents requested pursuant to the Political Reform Act) when I receive, or my representative receives them.

Name/Organization: _____

Mailing Address: _____

_____

_____

Phone Number: ( ) _____ Signature: _____

FAX Number: ( ) _____ Email: _____

FOR INTERNAL USE ONLY

Approved ☐ Denied ☐	Signature:
Reason, if denied:	

Disposition of Request: Documents/response provided on (date)

By: ☐ Mail ☐ Pick-up ☐ FAX ☐ Email ☐ Delivered ☐ Verbal ☐ Phone

Comments:

Date Completed:	Staff Member(s):	Staff Time:

BECKWOURTH PEAK
FIRE PROTECTION DISTRICT

POLICY TITLE: Types of Board Meetings

POLICY NUMBER: 4235

4235 Types of Board Meetings

4235.1 Regular meetings: Regular meetings of the Board of Directors shall be held on the First Wednesday on a bi-monthly schedule of February, April, June, August, October, and December, and starting at 6:00 PM in the Beckwourth Peak Fire Station, 180 Main Street, Beckwourth, CA 96129. The date, time and place of regular Board meetings may be reconsidered annually at the annual organizational meeting of the Board, or such other time as the Board may determine due to a change in District needs and circumstances.

4235.2 Special meetings: Special meetings of the Board of Directors may be called by the Board President or by a majority of the Board.

4235.2.1 All Directors shall be notified of the special Board meeting and the purpose or purposes for which it is called. Notice of the meeting shall be in writing, received by them at least 24 hours prior to the meeting.

4235.2.2 An agenda shall be prepared and posted at least 24 hours before the meeting and shall be delivered with the notice of the special meeting to the Board of Directors.

4235.2.3 Notice of the meeting shall be provided when possible to newspaper and other social media outlets and to any person who has requested to receive notices of meetings by serving a copy of the agenda at least 24 hours before the meeting.

4235.2.4 Only those items of business listed in the call for the special meeting shall be considered by the Board at any special meeting.

4235.3 Emergency Meetings: In the event of an emergency situation involving matters upon which prompt action is necessary, the Board of Directors may hold an emergency meeting without complying with the 24-hour notice requirement. An emergency situation means either, as determined by a majority of the Board: (1) a work stoppage, crippling activity, or other activity that severely impairs public health or safety; or (2) a crippling disaster, mass destruction, terrorist act, or threatened terrorist activity that poses immediate and significant peril (a dire emergency).

POLICY TITLE: Types of Board Meetings

POLICY NUMBER: 4235

4235.3.1 When possible, notice shall be provided to the media outlets by telephone at least one hour before the meeting.

4235.3.2 Actions taken during an emergency meeting shall be by roll call vote.

4235.3.3 The Board may meet in closed session if agreed to by 2/3 vote of the members present, or if less than 2/3 present, by unanimous vote.

4235.3.4 Following an emergency meeting, the minutes of the meeting, a list of persons notified or attempted to be notified of the meeting, and actions taken must be posted for ten (10) days in the District office.

4235.4 Adjourned Meetings: A majority vote of the quorum of the Board of Directors may adjourn any Board meeting at any place in the agenda to a time and place specified in the order of adjournment, except that if no quorum is present or no Directors are present at any regular or adjourned regular meeting, the Board President or presiding Board Director may declare the meeting adjourned to a stated time and place. Notice of the adjourned meeting shall be posted on or near the door of the meeting within 24 hours after the adjournment and the adjourned meeting shall be noticed in the same manner as a special meeting.

4235.5 Annual Organizational Meeting: The Board of Directors shall hold an annual organizational meeting at its regular meeting in December. At this meeting the Board will elect a President and Vice President among its members to serve during the coming calendar year and will appoint the Fire Chief as Finance Manager and District Treasurer.

Aligning Policies:

4205 Board Meeting Agenda

4215 Brown Act Compliance – Open Meeting Requirements

Revised: February 5, 2025
Adopted: July 3, 2024