JEFFERSON PARISH
EAST BANK CONSOLIDATED SPECIAL SERVICE
FIRE PROTECTION DISTRICT

CYNTHIA LEE SHENG
PARISH PRESIDENT

CHARLES M. HUDSON
FIRE CHIEF

To: All Personnel

From: Fire Chief Charles M. Hudson

Subject: Social Media Policy

Effective: Tentative October 11, 2025

Expiration: None

Policy: 10-2025

The following social medial policy will be implemented for all employees of East Bank Consolidated Special Service Fire Protection District.

A. Social Media Policy

1. Establishment

1.1. The parish understands that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

1.2. An employee shall not create a social media page to represent Jefferson Parish departments/programs or publicly publish to social media on behalf of the parish without approval and direction from the Office of Public Information. This requirement applies to all departments, offices and agencies under the administration of the Parish President, whether the position is classified or unclassified.

2. Policy

Jefferson Parish has a Public Information Office which operates under direction of an appointed Public Information Officer who is authorized by the Parish President to create and maintain official social media channels for Jefferson Parish (including but not limited to Facebook, Instagram, Twitter, LinkedIn, and YouTube). Directors interested in creating a social media page for their department or related programming should reach out to the Office of Public Information for direction. No Jefferson Parish social media pages are to be created unless reviewed and approved by the Office of Public Information.

3. Guidelines

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal website, social networking or affinity Web site, Web bulletin board or a chat room, whether or not associated or affiliated with the parish, as well as any other form of electronic communication including but not limited to Facebook, Twitter, Tumblr, Flicker, Instagram, etc. The same principles and guidelines found in Jefferson Parish's Administrative Management Policies manual and the Values of Jefferson Parish Government Employees apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees or otherwise adversely affects citizens, suppliers, people who work on behalf of Jefferson Parish or Jefferson Parish's legitimate business interests may result in disciplinary action up to and including termination.

4. Know and Follow the Rules

Carefully read these guidelines as well as Administrative Management Policies manual including but not limited to the sections on Workplace Violence and Prohibition against Harassment, and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

5. Be Respectful and Considerate

Always be fair and courteous to fellow employees, members of the public, suppliers or people who work on behalf of parish. Also, keep in mind that you are more likely to resolve work–related complaints by speaking directly with your co-workers or supervisor or by utilizing our Grievance Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage employees, members of the public, suppliers or people who work on behalf of parish, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of age, disability, equal pay, genetic information, harassment, national origin, race, religion, retaliation, sex, sexual orientation, gender identity, and sexual harassment or any other status protected by law or parish policy.

6. Be Honest and Accurate

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about parish, fellow employees, members of the public, suppliers or people working on behalf of parish.

7. Post Only Appropriate and Respectful Content

7.1. Maintain the confidentiality of private or confidential information. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

7.2. Do not create a link from your blog, website or other social networking site to a parish website without identifying yourself as a parish employee.

7.3. Make clear that you are speaking for yourself and expressing your personal opinions only. Never represent yourself as a spokesperson for parish. If the parish is a subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of parish, fellow employees, members of the public, suppliers or people working on behalf of parish. If you do publish a blog or post online related to the work you do or subjects associated with parish, make it clear that you are not speaking on behalf of parish. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Jefferson Parish."

8. Using Social Media at Work

Do not use social media while on work time or on equipment provided by parish, unless it is work related as authorized by your manager or consistent with the Use Information/Communication Resources Policy. Do not use Jefferson Parish email addresses to register on social networks, blogs or other online tools utilized for personal use.

9. Retaliation is Prohibited

Parish prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

10. Media Contacts

Employees should not speak to the media on parish's behalf without contacting the Office of Public Information. All media inquiries should be directed to them as stated in Administrative Management Policy 504 Media Communications Policy.[1]

11. For more information, if you have questions or need further guidance, please contact your Human Resource Manager.

Additionally, the following provisions are adopted, implemented, and applicable to all employees of East Bank Consolidated Special Service Fire Protection District to give full force and effect to the above-stated social media policy.

B. Workplace Violence

1. Establishment and Purpose

Violence in the workplace will not be tolerated in any form. The purpose of this policy is to establish guidelines and procedures, which support a safe and secure workplace.

[1] See Green Book Policy 2-2000.

2. Scope

2.1 This policy applies to all East Bank Consolidated Special Service Fire Protection District employees, whether classified or unclassified.

2.2 Workplace violence includes any physical or verbal behavior that endangers or harms another employee, contractor, vendor or citizen or that a reasonable person would perceive to constitute threat of harm.

2.3 Acts of violence may occur between fellow employees.

2.4 Acts of violence may also occur between employees and others while the employees are in the course and scope of their parish employment, which includes, but is not limited to, citizens, contractors and vendors. This policy, by extension, also applies to interaction between employees and these persons.

3. Definitions

3.1 "Assault" means a demonstrated intent to attack someone physically or verbally, causing bodily or emotional injury, pain or distress.

3.2 "Battery" means the intentional use of force or violence upon the person of another; or the intentional administration of a poison or other noxious liquid or substance to another.

3.3 "Credible threat" means a statement or action made with the intent and the apparent ability to carry out the threat so as to cause a reasonable person to fear for the person's safety or the safety of another and does, in fact, cause such fear.

3.4 "Dangerous weapon" means any device, instrument or substance capable of inflicting death or serious bodily injury, including, but not limited to, knives, any fixed blade knife, switch blade knife; guns of any kind; metal knuckles; biological contaminants; explosives; or any other object not designed as a weapon but used to inflict or threaten bodily harm.

3.5 "Domestic violence" means acts of physical, sexual, psychological or economic violence, including harassing or intimidating behavior, that occur as part of personal relationships.

4. Prohibited Conduct

The following is a non-exclusive list of prohibited conduct:

•Actions or behavior resulting in physical assault or battery against a person or property which may or may not include the use of a dangerous weapon;

•No employee shall be permitted to carry a gun or other dangerous weapon on Jefferson Parish property, or in a Jefferson Parish owned vehicle, with the exception of law enforcement/security staff who are Louisiana Post Certified Law Enforcement Officers.

•Threatening behavior or verbal abuse including offensive, profane and vulgar language that occurs in the work setting;

•Any physical altercation, hitting, pushing, shoving, holding/restraining, spitting on, blocking movement of another person, coercion, horseplay, intimidation, stalking, distracting, shouting or in any way interfering with another employee, contractor, vendor or citizen;

•Verbal or written threats communicated directly or indirectly that a reasonable person would perceive as intimidation or that otherwise cause fear of physical or emotional harm;

•Use of parish e-mail, telephones or radios to communicate threats or engage in intimidating behavior;

•Inappropriate verbal or physical behavior that would cause a reasonable person to feel unsafe, such as obscene phone calls, angry outbursts, throwing objects, or oral or written

expressions of hostility, including discussion of the use of dangerous weapons, even in a joking manner;

•Intimidating presence and/or harassment of any kind;

•Behavior that suggests a propensity toward violence, including aggressive speech or action, actions which damage, destroy or sabotage property or threats of sabotage, or repeated refusal to follow policies or procedures;

•Domestic violence introduced into the workplace in the form of assaults, threats or other actions by outside parties with whom employees have relationships and that occur at the workplace.

5. Employee Responsibility

5.1 Every employee is responsible for conducting himself in a courteous, civil and respectful manner toward all persons.

5.2 All employees have an obligation to adhere to this policy by refraining from any conduct that violates this policy;

5.3 Every employee has an affirmative obligation to assist the parish in ensuring a violence-free work environment;

5.4 Any East Bank Consolidated Special Service Fire Protection District or parish employee who reasonably believes the words or actions of another employee, contractor, vendor or citizen constitutes a violation of this policy and has the responsibility to immediately report such behavior to immediate supervisor, Chain of Command, Fire Chief, or Fire Department Human Resource Manager Representative.

5.5 In the event of an immediate threat or danger, employees should not confront the threatening party. In such case, employees should immediately retreat and call 9-1-1 if appropriate. Any use of force by an employee to protect person or parish property should be reported to their immediate supervisor, Fire Chief, and the Fire Department Human Resource Manager Representative as soon as possible.

6. Threats of Domestic Violence at Work

6.1 Any employee who is a victim of domestic violence shall report behavior that threatens the employee at work, including restraining or protective court orders related to domestic situations.

6.2 Reports may be made to the employee's immediate supervisor, Chain of Command, Fire Chief, or Fire Department Human Resource Manager Representative. The parish will work with the employee through the employee's supervisor and/or Chief Officer to implement reasonable measures designed to enhance the employee's safety and security at work while endeavoring to maintain the employee's privacy, but the parish cannot guarantee privacy.

6.3 Any employee who is a victim of domestic violence is encouraged to seek counseling through the Employee Assistance Program.

7. Supervisor Responsibility

7.1 Each supervisor has a responsibility to assist in maintaining a workplace that is free from workplace violence and to promptly address any problems encountered in an appropriate manner. This includes being aware of situations that have the potential to produce violent behavior and promptly addressing them with all concerned parties, and encouraging employees who show signs of stress or evidence of possible domestic violence to seek assistance through the Employee Assistance Program.

7.2 Supervisors must discuss this policy with current and new employees and ensure that employees are informed of this policy, have an opportunity to ask questions regarding this policy, and are aware that they are not to engage in or endure violence in the workplace.

7.3 Supervisors have the responsibility to promptly address issues of workplace violence; to thoroughly and impartially assist in investigating complaints of workplace violence; and to take, recommend or carry out appropriate action against any employee who is proven to be in violation of this policy. Supervisors are to report all complaints of workplace violence to their Human Resource Manager; to take all complaints of workplace violence seriously; and to treat these matters confidentially.

7.4 Supervisors who allow or tolerate workplace violence are considered to be in violation of this policy.

8. Investigation of Reports of Workplace Violence

8.1 All threats of violence must be taken seriously.

8.2 Supervisors, directors and Human Resource personnel and other parish staff who may receive reports of workplace violence or observe such behavior directly have the responsibility to take prompt action to see that an investigation is initiated.

8.3 An employee who has been threatened or assaulted by another employee or citizen at the workplace, or in course and scope of performing their job duties shall immediately report the situation to the employee's immediate supervisor.

8.4 Upon receipt of a report of workplace violence, the supervisor to whom the incident is reported will immediately notify the Fire Department Human Resource Manager Representative and his/her Chain of Command.

8.5 Incidents which present no immediate danger should be promptly handled by supervisors as follows:

•Employees involved in incident should be separated and isolated until the employees are interviewed or statements taken;

•Employees who witnessed incident should be identified and separated from incident until such time as their statements are taken;

•All actions should be documented and statements taken;

•The Fire Chief should be notified.

8.6 Incidents which present an immediate danger should be promptly handled by supervisors as follows:

•Contact building security or local police (9-1-1);

•Take reasonable measures to warn others or secure the area to protect other employees from danger;

•Order those presenting an immediate danger to leave;

•Do not attempt to physically remove an individual;

•Document all conduct, actions and statements;

•Notify your Chain of Command or Fire Chief as soon as practicable.

9. Reprisal and Retaliation

9.1 Any employee, who, in good faith, reports an alleged incident of workplace violence will not be subject to reprisal or retaliation of any kind.

9.2 Retaliation against employees who report acts of workplace violence is strictly prohibited. Instances of retaliation will be investigated and appropriate disciplinary action taken against the actor, which may include termination and/or referral to the appropriate civil or criminal authorities.

9.3 Any employee who feels they are the subject of retaliation or reprisal should report this to employee's Chief Officer or the Fire Department Human Resource Manager Representative.

9.4 Any employee who is found to have knowingly made false accusation of workplace violence or retaliation may be subject to disciplinary action up to and including termination.

C. Prohibition against Harassment

1. Establishment

It is the intent of the parish to provide and maintain a workplace free from all types and forms of harassment, including but not limited to initiating, directing, engaging or participating in verbal or physical conduct that denigrates, shows hostility, insults, or involves offending acts such as epithets, slurs, negative stereotyping, humiliation, or posting, distributing, creating, or displaying written or graphic materials which serve to offend or harass an individual or group of individuals based upon age, race, color, religion, national origin, mental or physical ability, sexual orientation, gender, gender identity, genetic information, pregnancy, or veteran status. Further, it is the intent of the parish to treat all employees equally and fairly regardless of their marital status, sexual orientation or gender identity. Through enforcement of this policy and by education of employees, Jefferson Parish will strive to prevent and correct behavior that violates this policy.

2. Purpose

The purpose of this policy is to ensure East Bank Consolidated Special Service Fire Protection District employees do not have to endure harassment by any other East Bank Consolidated Special Service Fire Protection District employee, parish employee, or non-employee engaged in business with the parish, and to provide for a workplace which is conducive to efficient, productive public service free from any harassing conduct or behavior. The purpose is also to provide corrective consequences where employees may seek relief from all forms of workplace harassment.

3. Scope

3.1 The scope of this policy extends to behavior which may violate state, federal or local law, but is not limited to such behavior and extends to any harassing behavior as defined below.

3.2 Workplace harassment may manifest itself in the form of conduct which violates state, federal and/or local law;

3.3 Workplace harassment may also manifest itself in the form of conduct which is not conducive to creating a work environment marked by courtesy, civility and respect.

4. Definitions

4.1 "Harassment" is defined as unwelcome verbal, physical or other conduct that is derogatory or shows hostility toward an individual for any reason, including the individual's race, color, religion, gender, marital status, familial status, national origin, age, mental or physical ability, sexual orientation, gender identity, genetic information, pregnancy, or veteran status and which has the purpose or effect:

•of creating an intimidating, hostile, abusive or offensive work environment;

•of unreasonably interfering with an individual's work performance; or

•otherwise adversely affects an individual's employment and employment-related opportunities.

4.2 "Sexual harassment" is defined as unwanted sexual advances, requests for sexual favors, and other sexually oriented verbal, visual or physical conduct where and when:

•submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment; or

•submission to or rejection of such conduct is used as a basis for employment decisions affecting such individual; or

•such conduct has the purpose or effect of unreasonably interfering with an individual's work performance, or creating an intimidating, hostile, or offensive work environment.

5. Prohibited Conduct

5.1 Verbal or physical conduct

The following represents a non-exclusive list of conduct which is prohibited by this policy:

•The use of insults, innuendos, repeated requests for dates, suggestive comments, sexual propositions, threats or slurs for any reason, including an individual's race, color, religion, gender, marital status, familial status, national origin, age, mental or physical disability, sexual orientation, gender identity, genetic information, pregnancy, or veteran status;

•Humor, jokes, pranks or other banter about sex, anatomy or gender-specific traits, suggestive or insulting sounds ("catcalls" or "kissing" noises), leering, obscene gestures, and sexually suggestive body gestures, including negative stereotyping, which relates to or is derogatory or shows hostility based on an individual's race, color, religion, gender, marital status, familial status, national origin, age, mental or physical disability, sexual orientation, gender identity, genetic information, pregnancy, or veteran status;

•Unwelcome physical touching or contact, such as pinching, kissing, grabbing, patting, hugging, brushing the body, or any coerced sexual act or actual assault.

5.2 Written or graphic material

The following represents a non-exclusive list of conduct which is prohibited by this policy:

•Text/Electronic – electronically sending messages with sexual content, including pictures and video, the use of sexually explicit language, harassment, cyber stalking and threats via all forms of electronic communication (e-mail, text/picture/video messages, internet/on-line postings, blogs, instant messages and social network sites). Sending, displaying or disseminating inappropriate jokes or other written or graphic material via e mail, the internet or by fax, or downloading this material from the internet.

•Material including but not limited to posters, signs, pin-ups or slogans, viewing pornographic materials or websites, that is disparaging or displays hostility on the basis of a race, color, religion, gender, marital status, familial status, national origin, age, mental or physical disability, sexual orientation, gender identity, genetic information, pregnancy, or veteran status and is placed on walls or elsewhere in the employer's premises or circulated in the workplace;

•Material that is reasonably deemed to be sexually provocative or stimulating and is placed on walls or elsewhere in the employer's premises or circulated in the workplace;

5.3 Although severe and overt forms of sexual harassment may be readily apparent, some sexual harassment is subtle and varies depending on interpretation and perception. Review of sexual harassment allegations are subject to the standard of what offends a "reasonable person."

6. Employee Responsibility

6.1 Every employee is responsible for conducting himself in a courteous, civil and respectful manner toward all persons.

6.2 All employees have an obligation to adhere to this policy by refraining from any conduct that violates this policy, including interactions on social media.

6.3 Every employee is required to assist the parish in ensuring a work environment free of harassment.

6.4 Any East Bank Consolidated Special Service Fire Protection District employee who reasonably believes the words or actions of another employee violates this policy has the responsibility to immediately report such behavior to his or her immediate supervisor, Chain of Command, Fire Chief, or the Fire Department Human Resource Manager Representative.

6.5 Any affected employee may respond to the harassment in the following manner:

•Politely but firmly tell the offending individual to stop the harassing conduct, and report the conduct to the employee's supervisor;

•Report the matter to your Chain of Command, the Fire Chief, or to the Fire Department Human Resource Manager Representative;

•File a grievance report.

7. Supervisor Responsibility

7.1 Each supervisor has a responsibility to assist in maintaining a workplace that is free from workplace harassment and needs to promptly address any problems encountered in an appropriate manner:

•Supervisors must take immediate action to stop and prevent harassment where they know or have reason to know that it is occurring;

•Tacit approval of harassment is prohibited; for example, treating a situation as a joke, failing to take action, or advising an employee not to complain;

•Supervisors are responsible for ensuring that notes, comments, posters and other materials on walls, bulletin boards or elsewhere in the workplace that are derogatory or show hostility are removed.

7.2 Supervisors must discuss this policy with current and new employees and assure that employees are informed of this policy, have an opportunity to ask questions regarding this policy, and are aware that they are not to engage in or endure harassment in the workplace.

7.3 Supervisors have the responsibility to promptly address issues of harassment; to thoroughly and impartially assist in investigating complaints of harassment; and to take, recommend or carry out appropriate action against any employee who is proven to be in violation of this policy. Supervisors are to report all complaints of harassment to their Chain of Command or Fire Department Human Resource Manager Representative and to take all complaints of harassment seriously.

7.4 Every effort should be made to treat matters as confidential. However, supervisors must inform complainant that strict confidentiality may not be feasible.

7.5 Chief Officers and fire line supervisors who knowingly allow or tolerate discrimination, harassment, or retaliation, including the failure to immediately report such misconduct to the Fire Chief, Chain of Command, or Fire Department Human Resources Manager Representative, are in violation of this policy and subject to discipline.

7.6 If during the course of investigation, the investigator determines that the allegation or complaint of sexual harassment was reported to a management/supervisory level

employee, and that management/supervisory employee failed to promptly report the allegation or complaint to their Fire Department Human Resource Manager or Appointing Authority, the Appointing Authority shall investigate and take appropriate action against the management/supervisory employee, to include disciplinary action.

8. Procedure

8.1 All threats of harassment must be taken seriously when received.

8.2 Supervisors, Chief Officers and the Fire Department Human Resource personnel and other parish staff who may receive reports of workplace harassment or observe such behavior directly have the responsibility to take prompt action to see that an investigation is initiated.

8.3 An employee who has been harassed by another at the workplace shall immediately report the situation to the employee's immediate supervisor. If the employee has a legitimate reason for not reporting the incident to the employee's supervisor, the incident shall be reported to the employee's Chief Officer and Fire Department Human Resource Manager Representative.

8.4 Upon receipt of a report of workplace harassment, the supervisor to whom the incident is reported will notify the Fire Chief and Fire Department Human Resource Manager Representative.

8.5 Incidents should be promptly handled by supervisors/Chief Officers as follows:

8.5.1 Affected or involved employees should be counseled as appropriate.

8.5.2 Counseling should be documented;

8.5.3 Notify Fire Chief and Fire Department Human Resource Manager Representative.

8.5.4 All reasonable measures shall be undertaken to ensure privacy and confidentiality of corrective action.

9. Review of Complaint

9.1 All complaints must be thoroughly and promptly investigated.

9.2 The Fire Chief or his/her designee shall be responsible for conducting the investigation and submitting a report and recommended action to the Appointing Authority and/or Fire Chief.

9.3 The Fire Chief or his designee, shall initiate a fair, complete and impartial investigation of the complaint as promptly as possible. The objective is to ensure that the investigation is conducted discreetly preserving confidentiality to the extent that the needs of the investigation will permit. It shall be the Parish's objective to complete all investigations within sixty (60) days unless compelling circumstances require additional time. A written statement of the complaint which is to include date(s) the incident(s) occurred, name(s) of individual(s) involved, name(s) of witnesses and a detailed description of the incident(s) constitutes the initiation of the sixty (60) day investigative period. Employees also have the right to file a complaint with the Equal Employment Opportunity Commission (EEOC), the Louisiana Human Rights Commission, or pursue other legal action in addition to their rights hereunder. The EEOC provides employees three hundred (300) days to file an official complaint.

9.4 Individual making the complaint and the accused shall be notified of the results of the investigation, which will be conducted consistent with state law, local ordinance, and department policy.

10. Retaliation

10.1 Any employee who, in good faith, reports harassing conduct or participates in an investigation will not be subject to reprisal or retaliation of any kind.

10.2 Retaliation against an employee who brings a complaint of harassment, reports an allegation of sexual harassment on behalf of another, or participates in an investigation of a harassment complaint is prohibited and may result in disciplinary action. Similarly, allegations or complaints of sexual harassment that have been determined to be fabricated, knowingly false, or otherwise baseless shall require the Appointing Authority to impose disciplinary action against the complainant found to have filed the improper complaint, as well as any other employees that participated in the false allegation or complaint.

10.3 Any employee who feels to be the subject of retaliation or reprisal should report this to the employee's Fire Chief or Fire Department Human Resource Manager Representative.

D. Use of Information/Communication Resources

1. Use of Technologies and Communication Systems

1.1. Establishment

This standard is established to govern access and usage of Jefferson Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communications systems administered by, or under supervision of, the Electronic Information Systems Department ("EIS"), including but not limited to Parish-owned and/or East Bank Consolidated Special Service Fire Protection District-owned computers, servers, networks, applications, software, electronic mail system (E-mail), Intranet, Internet access, voice systems, mobile devices, and related services.

1.1.1. This standard also defines expectations regarding usage and/or access to Jefferson Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems. It further defines the roles and responsibilities of East Bank Consolidated Special Service Fire Protection District personnel with regards to appropriate operation and use of the above-mentioned resources.

1.1.2. Information Technology resources are limited, and shall be used judiciously and with consideration for the rights and needs of others. Activities that jeopardize the integrity of the system, consume an unreasonable share of resources, infringe upon the privacy of other users, threaten the actual or perceived safety of others, or that are illegal are PROHIBITED. Violations of this standard may result in disciplinary action up to and including termination.

1.2. Purpose

Unauthorized use of Parish and/or East Bank Consolidated Special Service Fire Protection District systems could cause the Parish and/or East Bank Consolidated Special Service Fire Protection District a loss of competitive advantage, could place the Parish and/or East Bank Consolidated Special Service Fire Protection District and its employees in legal or physical jeopardy, and/or embarrass its employees, citizens, and/or elected representatives. Unauthorized use could result in the disclosure of sensitive data and/or introduce malware into the Parish's and/or East Bank Consolidated Special Service Fire Protection District's network environment, which could result in data loss or the loss of availability of the

Parish's and/or East Bank Consolidated Special Service Fire Protection District's network resources. By ensuring that only approved hardware and software are used exclusively for approved business purposes, we are attempting to reduce these risks. This section identifies some of the more well-known security concerns associated with the use of Parish and/or East Bank Consolidated Special Service Fire Protection District technology in hopes that the reader will gain an appreciation for our security standards and their importance. These standards define mechanisms (e.g., user- IDs and passwords, firewalls, etc.) which reduce security risks to Jefferson Parish and/or East Bank Consolidated Special Service Fire Protection District and provide a means to identify and recover from an actual attack. The purpose of this policy is twofold:

1. To provide strict guidelines regarding the use of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems,
2. To provide strict guidelines regarding computers, storage devices and/or mobile devices, which may be used to access the Parish and/or East Bank Consolidated Special Service Fire Protection District network or are otherwise supported by the Parish and/or East Bank Consolidated Special Service Fire Protection District network.

1.3. Scope

The scope of this policy extends to the access and usage of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems, whether through Parish-owned and/or East Bank Consolidated Special Service Fire Protection District-owned equipment (on or off the Parish and/or East Bank Consolidated Special Service Fire Protection District network) or through personal devices which access our network.

1.4. Definitions

For purposes of this policy, the following words shall have the following meaning:

"Application" means a software program that carries out some useful task. Database managers, spreadsheets, communications packages, graphics programs and word processors are all applications.

"Assets" means property of all sorts belonging to a person, association, government, or corporation.

"Breach" means unauthorized access to systems and/or data by an outside party.

"Business-Critical Information" means information which is critical to sustain an operating unit and requires protection from disclosure.

"Business Impact Analysis" means a management-level assessment technique used to determine the potential exposures and impacts associated with a major disruption, and the value to the Parish of a function, department, operation, or information.

"Business Owner" means the manager of an operating unit who is responsible for the unit's functions and operation. This individual is also responsible for identifying and establishing the information objectives and requirements for his or her organization.

"Compromise" means (v) to cause harm or negative impact. (n) The unintentional or unauthorized loss or release of information.

"Computer Networks" means the connection of computers and computer-related devices (terminals, printers, modems, door entry sensors, temperatures monitors, etc.)

“Confidential Information” means information which, if disclosed, could cause potential harm to an organization or to an individual.
“Confidentiality” means a level of privacy and secrecy associated with information.
“Custodians” means individuals to whom ownership roles and/or responsibilities have been delegated.
“Electronic mail (E-mail)” means any message or communication which is sent or received though the Parish and/or East Bank Consolidated Special Service Fire Protection District network or by Parish and/or East Bank Consolidated Special Service Fire Protection District Internet access and includes any electronic data, images, or attachments to the message or communication.
“Information” means processed data. Something told or factual; the communication or reception of knowledge or intelligence.
“Information Classification” means the process of identifying the importance or sensitivity of information to an organization and categorizing the information based on a predefined organizational classification policy or standard.
“Information Owner” means the party within an organization who is responsible for an operating unit and who may sponsor and authorize the development of automated processes for his/her operating unit.
“Integrity” is defined as being concerned with the improper modification of information regardless of whether such modification is accidental or intentional.
“Internal Use Only Information” means information which is intended to be used within an organization and requires protection from disclosure or alteration by unauthorized persons.
“Internet” means an open computer network which connects computers and other computer networks and organizational computer facilities world-wide through which communications may be made and resources gathered and shared.
“IT Security” means the organization responsible for securing the information assets of Jefferson Parish and/or East Bank Consolidated Special Service Fire Protection District and its customers.
“Laws, Codes, and Regulation Information” means information which is stipulated as confidential by State or Federal laws, Government codes or regulations.
“Mobile devices” means small, hand-held computing devices typically having a display screen with touch input and/or a miniature keyboard with an operating system which has the capability to run certain software applications.
“Owner(s)” a term used to describe a party or parties with ownership responsibilities for information in the Jefferson Parish government’s network environment.
“Parish network” means the computers and computing hardware devices that are linked together through communication channels maintained by the Parish and/or East Bank Consolidated Special Service Fire Protection District to facilitate communication and resource-sharing within Parish government and includes the Parish and/or East Bank Consolidated Special Service Fire Protection District E-mail system and Parish and/or East Bank Consolidated Special Service Fire Protection District Intranet.
“Parish Intranet” means the restricted network accessible by Parish and/or East Bank Consolidated Special Service Fire Protection District computers through which certain information and resources are shared within Parish government.

"Parish technology and communication system" means: the Jefferson Parish network and the computer hardware and software acquired and maintained by the Parish which supports use of technology by the Parish and/or East Bank Consolidated Special Service Fire Protection District through computers, mobile computing devices, printers, scanners and other supported equipment.

"Public Information" means information prepared with the intent to be shared with the general public (e.g., press releases, and brochures).

"Regulatory Agencies" means government agencies which mandate regulations unique to industries and organizations.

"Restricted Information" means highly-sensitive information whose improper disclosure could decrease an organization's advantage or compromise the organization's reputation.

"Retention Requirements" means requirements which are established by law, regulation, contract, or policy concerning the required period of time for keeping or retaining information on storage media.

"Risk of Loss" means the potential or probability of a loss.

"Roles and Responsibilities" means the functions and obligations of an individual and for which the individual is accountable.

"Safeguards" means controls or preventive mechanisms which are put in place to protect assets.

"Sensitivity" means having the capacity or ability to cause harm to an individual or organization.

"User" a term used to describe individuals (such as East Bank Consolidated Special Service Fire Protection District employees) who use computers and systems.

"Value" means usefulness, importance or general worth.

2. Acceptable Use

2.1. Ownership and access to technology and communication

Employees have no expectation of privacy on Parish and/or East Bank Consolidated Special Service Fire Protection District systems. Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communications systems are for facilitating and conducting government business and other uses related to East Bank Consolidated Special Service Fire Protection District employment. All forms of data created, entered, shared, transmitted, received or stored using Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems are considered Parish and/or East Bank Consolidated Special Service Fire Protection District property and are subject to being monitored, viewed, or released - except as may otherwise be prohibited by state or federal privacy laws. Employees should assume that all forms of data created, entered, shared, transmitted, received or stored using Parish and/or East Bank Consolidated Special Service Fire Protection District technology communication system will be monitored and viewed.

2.1.1. Employees using Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems to create, access, share, transmit or receive data or information that would otherwise be subject to any claim of confidentiality or privilege from disclosure hereby waive the right to assert such claim of confidentiality or privilege from disclosure.

2.1.2. The Parish has licensed the use of certain commercial software application programs for Parish and/or East Bank Consolidated Special Service Fire Protection

District business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use or distribute copies of such software in a manner which does not comply with applicable licensing agreement or otherwise violates the terms of the license agreement.

2.2. Electronic mail and electronic mail tampering

Parish E-mail is to be used solely for work-related communications and for responding to inquiries related to the efficient and effective operation of government and job-related duties. E-mail systems are provided for business use, and messages sent or received through the Parish's E-mail system are the property of the Parish and/or East Bank Consolidated Special Service Fire Protection District. E-mail should be treated as a document which you intend to publish. It should be drafted with care. Legitimate E-mail use includes communications between Jefferson Parish employees, East Bank Consolidated Special Service Fire Protection District employees, citizens, contractors, vendors, and business partners.

2.2.1. Exercise prudence when sending large files. Large volumes of mail can negatively impact Parish mail systems. Be careful when replying to distribution lists or using 'reply all' to avoid sending to the entire original mailing list unintentionally.

2.2.2. All E-mails shall conform to the prescribed East Bank Consolidated Special Service Fire Protection District format:

- Background shall be stark white with black or blue lettering throughout;
- Font size shall not exceed 14pt;
- Electronic signatures must adhere to the Style Guide and Logo Policy maintained by the Public Information Office;
- Personalized stationary and colored backgrounds are not allowed, nor are logos, emoticons, images, philosophies, personal message statements, or quotations.

2.2.3. Transmission or receipt of E-mails which are strictly for personal reasons is considered a misuse and abuse of the Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication system. Employees shall refrain from using non-Jefferson Parish E-mail accounts to conduct East Bank Consolidated Special Service Fire Protection District business.

2.2.4. E-mail messages received shall not be altered without the sender's permission, nor shall messages be altered and forwarded to another user and/or unauthorized attachments placed on another's E-mail without the individual's permission.

2.2.5. Auto-Forwarding of E-mail messages to accounts outside of the Jefferson Parish network is prohibited.

2.3. Internet usage and browsing

2.3.1. Internet access is a Parish and/or East Bank Consolidated Special Service Fire Protection District resource which is provided as a tool for employees to engage in necessary research, professional development and work-related communications. An Internet Access account is restricted to the individual for which the account was granted.

2.3.2. Internet access is restricted to uses which further effective and efficient operation of government, to provide enhanced service of the highest quality, and to

support other directly job-related purposes. Employees should comply with corporate encryption standards and obtain management approval to transmit information which is classified as “Internal Use Only” or “Confidential” across the Internet.

2.3.3. Internet access for personal purposes or reasons unrelated to East Bank Consolidated Special Service Fire Protection District employment and job duties shall be minimal and only with supervisory approval.

2.4. Intranet Usage

As with the Internet, use of the Employee Intranet, JeffConnect, is reserved for Jefferson Parish and/or East Bank Consolidated Special Service Fire Protection District employees and non-employee contractors to facilitate the exchange of information consistent with business purposes and goals of the Parish and/or East Bank Consolidated Special Service Fire Protection District. All users are expected to be familiar with and adhere to this standard. Controls governing access are not as restrictive as those imposed on connections to the Internet. Employees are encouraged to use the Intranet for research, education, and learning more about Jefferson Parish government and its services.

2.5. Remote Desktop Protocol

The use of Remote Desktop Protocol, “remoting to computers,” is reserved for EIS staff only. Employees shall only have one computer, therefore, eliminating the need for RDP in most instances.

2.6. Prohibited Activities

The following is a non-exclusive list of prohibited uses of the Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems:

●Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access;

●Using or accessing restricted Parish and/or East Bank Consolidated Special Service Fire Protection District computer resources or systems without or beyond one's level of authorization;

●Attempting to access, or accessing another user's accounts, private files, e-mail messages, or intercepting network communication without the owner's permission except as appropriate to your job duties and in accordance with legitimate East Bank Consolidated Special Service Fire Protection District purposes;

●Downloading files from the Internet or other devices receiving, or sending, files as attachments to E-mails which are unrelated to the efficient and effective operation of East Bank Consolidated Special Service Fire Protection District or job duties;

●Creating, or participating in, communications with derogatory or inflammatory remarks about an individual’s race, age, gender, disability, religion, national origin, physical attributes, sexual preferences, and/or political beliefs;

●Causing congestion, disruption, disablement, alteration, or impairment through misuse of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems;

●Circumventing, violating, or subverting system security or network security measures, or exploiting flaws in same, or attempting to do so;

●Attaching any device to the Parish and/or East Bank Consolidated Special Service Fire Protection District network without the express permission of EIS staff. This includes (but

is not limited to) wireless access points such as hubs, switches, routers, printers, protocol analyzers, personal computers & tablets;
●Installing and/or distributing software on Parish and/or East Bank Consolidated Special Service Fire Protection District computer without a verifiable license;
●Installing and/or distributing software on Parish and/or East Bank Consolidated Special Service Fire Protection District computers that is legally or illegally licensed to user but not licensed to Jefferson Parish and/or East Bank Consolidated Special Service Fire Protection District;
●Installing or reconfiguring hardware or software on Parish and/or East Bank Consolidated Special Service Fire Protection District computers or network without proper authorization from EIS;
●Using systems to solicit or sell products or services that are unrelated to East Bank Consolidated Special Service Fire Protection District business;
●Accessing networks, servers, drives, folders, other user accounts, or files to which the employee has not been granted access or authorization from the appropriate authority;
●Making unauthorized copies of Parish and/or East Bank Consolidated Special Service Fire Protection District files, information or data in any format, whether photographic, audio, etc.;
●Destroying, deleting, erasing or concealing Parish and/or East Bank Consolidated Special Service Fire Protection District files or other data, or otherwise making such files or data unavailable or inaccessible to the Parish or to another authorized user of the Parish system;
●Misrepresenting oneself or the Parish and/or East Bank Consolidated Special Service Fire Protection District through use of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems;
●Propagating any virus, worm, Trojan horse, or other program or code designed to disrupt, disable, impair, or otherwise harm either Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems or those of any individual computer;
●Using abusive, profane, threatening, discriminatory or otherwise objectionable language through use of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems;
●Accessing personal E-mail accounts or non-jeffparish.net E-mail accounts (gmail.com, yahoo.com etc);
●Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial E-mail (“spam”);
●Sending, receiving (without reporting) or accessing offensive materials, including but not limited to sexually explicit materials or materials whose content would otherwise be considered discriminatory or harassing;
●Engaging in unlawful or malicious activities;
●Engaging in recreational games, gambling or wagering activity through use of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems;
●Defeating or attempting to defeat security restrictions governing use of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems;
●Engaging in political or partisan activity;

●Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or social media sites. Accessing social media sites inconsistent with Social Media Policy;
●Sharing, displaying, distributing, releasing, or otherwise providing access to Parish data to individuals not authorized to access it by the data owner

2.7. Streaming Media

2.7.1. Streaming media permitted for business purposes is defined as "content deemed necessary to fulfill employee job duties and responsibilities." EIS maintains the right at any time to block access to streaming media/programs (on a per-individual or Parish-wide basis) that do not involve legitimate business purposes.

2.7.2. Reasonable recreational access to streaming media is permitted so long as it does not interfere with employee productivity (as defined by employee supervisors and these Administrative Policies), distract or impede the productivity of others, or consume an inordinate amount of system or network resources. Where possible, employees should use headphones when accessing streaming audio to avoid creating undue noise burdens upon coworkers.

2.7.3. Access to offensive or inappropriate streaming media content (any published or broadcast content that is likely to be upsetting, insulting, or objectionable to some or most people) is prohibited on all Parish systems/networks at all times.

2.8. Network File Services and Storage

The EIS Department provides centralized network file storage, sharing and backup services to individuals, groups and departments across the Parish and/or East Bank Consolidated Special Service Fire Protection District. The file servers are designed to provide users with secure, backed-up redundant storage for data and files.

2.8.1. Storing files and data on a computer's local hard drive or desktop is prohibited. Loss of data on non-network storage is the employee's responsibility and likely unrecoverable.

2.8.2. Use of Parish and/or East Bank Consolidated Special Service Fire Protection District resources for the storage of personal files, photos, music, and/or videos is prohibited and such files will be deleted immediately by EIS staff upon discovery and not returned to the employee.

2.9. Wireless Networking (Wi-Fi)

Depending on availability of bandwidth, EIS provides Wi-Fi access at several Parish and/or East Bank Consolidated Special Service Fire Protection District facilities. There is no expectation of privacy while connected to any Jefferson Parish wired or wireless network. All usage can be monitored by EIS.

2.9.1. Use of personal and/or consumer Wi-Fi hardware on the Parish network is prohibited. No employee shall establish any ad-hoc or departmental Wi-Fi network for use by East Bank Consolidated Special Service Fire Protection District personnel or resources.

2.9.2. Attachment to the Parish network of any Wi-Fi hardware (1) not approved by IT or (2) not procured through approved Parish and/or East Bank Consolidated Special Service Fire Protection District procurement channels or (3) not installed, and configured by IT is prohibited.

2.9.3. There are two primary Wi-Fi networks described below.

4.9.3.1. JeffParish-Secure Network This network can only be accessed by Parish-owned and/or East Bank Consolidated Special Service Fire Protection District-owned computers, laptops and tablets that are on our jeffparish.net domain. Users will select JeffParish-Secure and their devices will automatically authenticate to the Wi-Fi network. Users will have the same level of access as if they are physically connected to the network.

4.9.3.2. JeffParish-Public – This will be for employees and guests. It will give users access to Internet only. To authenticate, users will select JeffParish-Public from the list of available wireless networks and enter the published password. Next, users will agree to the terms to finalize their connection. The password can be shared with anyone who wants to join JeffParish-Public. By policy, domain computers will not be able to join this network.

3. Acquisition and Disposal

Acquisition of resources

3.1. EIS maintains a list of approved hardware and software on the JP Technology Store found on the Employee Intranet. EIS does not and will not support unapproved software or hardware, and unapproved hardware and software may not be installed or used within the Parish and/or East Bank Consolidated Special Service Fire Protection District environment. All approved hardware and software must be acquired with the proper Technology Store approval through authorized procurement channels and from approved vendors.

3.1.1. Employees who require a computer are allowed only one device, which must be portable. Laptops and/or tablets can be configured with external monitors, mouse, keyboard, and a docking station. Traditional tower computers will only be purchased for special-use cases approved by the Director of EIS.

3.2. Resources inventory

Hardware and software are assets. An inventory shall be maintained of all hardware and software assets. All hardware and software must be added to inventory upon receipt, and an owner assigned. Hardware and software assets will be tracked throughout their life cycles, and only removed from inventory upon disposition.

3.3. Installation by authorized personnel

At no time shall any unauthorized employee install software or hardware on Parish and/or East Bank Consolidated Special Service Fire Protection District Information Technology resources or devices. Installation of or altering of Parish and/or East Bank Consolidated Special Service Fire Protection District software or hardware shall only be done by EIS or with EIS approval. No personal hardware or software shall be installed by EIS or employees.

3.4. Secure retirement of obsolete systems

When a hardware, software, or Parish and/or East Bank Consolidated Special Service Fire Protection District Information Technology asset is determined to have reached the end of its useful life, it shall be retired and disposed of according to established Parish and/or East Bank Consolidated Special Service Fire Protection District policies and procedures. All Parish and/or East Bank Consolidated Special Service Fire Protection District software and data – including the operating system - must be securely deleted from a retired asset by EIS prior to disposal.

4. Roles & Responsibilities

It should be noted that the roles and responsibilities described in this standard are functional in nature, and are not intended to represent individuals. Several functions described in this standard can, and may, be performed by the same person. It is the responsibility of local management and the information owner to decide how these roles and responsibilities will be implemented within their business unit.

4.1. EIS Responsibilities

EIS continuously monitors usage and access to Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems, including but not limited to accessing and monitoring departmental and individual employees' use of computer equipment, IP voice telephony systems, E-mail, and Internet access. EIS is responsible for:

- Determining and maintaining a list of approved hardware and software, and a list of approved vendors from whom it can be sourced;
- Maintaining an inventory of hardware and software assets;
- Installing and maintaining approved hardware and software;
- Maintaining approved data recovery vendor(s);
- Secure decommissioning of end-of-life assets, and the secure destruction of failed assets

4.2. Supervisor and Manager Responsibilities Supervisors are responsible for:

- Monitoring and ensuring compliance by employees;
- Determine, approve or deny requests for use and access to Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems based upon departmental needs, needs for services, employee job-duties, potential for misuse or abuse of systems;
- Review employee authorization and access to Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems upon change of employee classification or position;
- Notify and confirm with EIS that employee access to Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems is terminated upon termination of employment or altered pending employee transfer, promotion or demotion;
- Receiving reports from employees of abuse or misuse of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems;
- Receiving information from employees that systems' security has been breached or otherwise compromised, including reports of viruses and computer crashes;
- Reporting abuse or misuse of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems, breaches or compromises in systems security to EIS;
- Taking appropriate disciplinary action.

4.3. Employee Responsibilities

All East Bank Consolidated Special Service Fire Protection District employees are responsible for:

- Reading, understanding, and abiding by this policy and its provisions;
- Using Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication in a manner consistent with this policy. Employees shall

refrain from engaging in any conduct which compromises the integrity of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems or otherwise violates this Policy;

●Verify the proper content of all text, audio, or images that they write, store, retrieve, or transmit through the Parish's and/or East Bank Consolidated Special Service Fire Protection District's electronic systems;

●Choosing a secure password and changing the password in accordance with the password policy;

●Protecting and preserving security by keeping confidential passwords in accordance with the password policy;

●Logging off, or locking any Parish and/or East Bank Consolidated Special Service Fire Protection District computer and/or network device each time it is unattended;

●Refraining from powering down a computer, unless told to do so by EIS;

●Reporting abuse of Parish and/or East Bank Consolidated Special Service Fire Protection District technology and communication systems to appropriate supervisor;

●Reporting information which indicates systems security has been breached or compromised or the integrity of the system is otherwise compromised; including by way of example only a misappropriated password, incident computer viruses, and malicious campaigns targeting Parish employees, or equipment intended to unlawfully access or damage the network.

●Successfully completing all required IT related training assigned by EIS.

E. Media Communications Policy

1. Establishment

An employee, other than the Fire Chief and/or his or her designee, shall not publicly publish, or allow to be published his or her statement concerning official parish business without direction from the Office of Public Information. An employee, other than the Fire Chief and/or his or her designee, shall not knowingly appear in the employee's official capacity or give the appearance of acting in the employee's official capacity, for example appearing in parish uniform, before cameras without prior approval.

2. Purpose

The purpose of this policy is to set forth guidelines and procedures for responding to inquiries and requests for information or interviews from members of the media and/or for public appearances of employees acting in their official capacity.

3. Scope

This policy applies to all administrative officers and employees of the parish responsible to the Parish President, whether they are unclassified or classified employees, including all employees of East Bank Consolidated Special Service Fire Protection District.

4. Policy

Jefferson Parish has an established Office of Public Information which operates under direction of an appointed Public Information Officer who is authorized by the Parish President to receive and respond to requests for information and interviews from members of the media and to communicate directly with members of the media. Requests for information, interviews or public appearances by employees, other than the Fire Chief and/or his or her designee at the scene of an

active fire, shall be directed to the Office of Public Information for response and/or direction. No press releases are to be issued unless reviewed and approved by the Office of Public Information.

5. Procedure

5.1 Receipt of request for information, interview or public appearance

Upon receipt of a request for information, interview or public appearance by media or upon being contacted by a member of the media, the East Bank Consolidated Special Service Fire Protection District employee, other than the Fire Chief and/or his or her designee at the scene of an active fire, shall inform the media representative that requests for information, interviews or public appearances are answered by the Office of Public Information. At that time, the employee shall provide the name and contact number of the Public Information Officer.

5.2 Fire Chief responsibilities

•Direct requests to Public Information Officer and provide contact information for Public Information Officer upon receiving requests, including but not limited to incidents where the media may appear without prior notice at a particular work site or job.

•Seek to obtain contact information from media representative, if available, and subject of requests. Promptly provide information to Public Information Officer for response and direction.

•Alert the Public Information Officer if the requests may involve a matter of particular importance and the relevant history or facts.

•Be available to Public Information Officer before, during and after regular work hours by telephone or other means of communication to assist in coordinating response and providing answers to request.

•Refrain from making any public statement or appearance, other than at the scene of an active fire, unless expressly authorized.

5.3 Employee responsibilities

•Inform media that all requests for information, interview or public appearance are received and answered by Public Information Office.

•Direct requests to immediate supervisor who shall immediately direct requests to the Fire Chief.

•Seek to obtain contact information from media representative, if available, and subject of requests. Promptly provide information to immediate supervisor.

•Refrain from making any public statement or appearance unless expressly authorized.