Brothers Fire & Security

Office Policy Manual

The policies and procedures in this manual are not intended to be contractual commitments by Brothers Fire & Security, and employees shall not construe them as such.

The policies and procedures are intended to be guides to management and are merely descriptive of suggested procedures to be followed. Brothers Fire & Security reserves the right to revoke, change or supplement guidelines at any time without notice.

No policy is intended as a guarantee of continuity of benefits or rights. No permanent employment or employment for any term is intended or can be implied from any statements in this manual.

Edited 12/9/16

Our Company

Letter from the President

Welcome to Brothers Fire & Security.

We are pleased to have you as an employee of Brothers Fire & Security and hope that you find your association with this company to be an enriching and engaging work experience.

This manual is your guide to our policies. Of course, this manual cannot cover every eventuality that may arise. Its purpose is to summarize or highlight current policies and practices for staff members. All policies are subject to change. If you have questions or would like more information, your supervisor/manager is your most immediate source.

We invite you to share with us your questions and thoughts about work life at Brothers Fire & Security. Please feel free to call upon any member of the Human Resources Department to assist you in any matter that concerns you and your job at Brothers Fire & Security.

Sincerely,

Stephen Cieslukowski
President

Equal Opportunity

Brothers Fire & Security Co. will not discriminate against any employee or applicant because of race, creed, religion, sex, sexual or affectional orientation, color, national origin, ancestry, familial status, age, disability, marital status, or status with regard to public assistance.

Brothers Fire & Security Co. will maintain zero tolerance for harassment of or by any employee or applicant for employment because of race, creed, religion, sex, sexual or affectional orientation, color, national origin, ancestry, familial status, age, disability, marital status or status with regard to public assistance, will maintain an internal complaint procedure for complaints of such harassment and will provide employees with contact information for federal, state and local enforcement agencies.

Brothers Fire & Security Co. will take Affirmative Action (AA) to ensure that all employment practices are free of such discrimination and harassment. Such employment practices include, but are not limited to, the following: hiring, upgrading, demotion, transfer, recruitment or recruitment advertising, selection, layoff, disciplinarily action, termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

Brothers Fire & Security Co. fully supports incorporation of non-discrimination and affirmative action rules and regulations into contracts.

Brothers Fire & Security Co. will commit the necessary time and resources, both financial and human to achieve the goals of Equal Employment Opportunity and Affirmative Action.

Brothers Fire & Security Co. will evaluate the performance of its management and supervisory personnel on the basis of their involvement achieving these Equal Employment Opportunity and Affirmative Action objectives as well as other established criteria. Any employee of or subcontractor to **Brothers Fire & Security Co.** who do not comply with the Equal Employment Opportunity and Affirmative Action (EEO/AA) Policies and Procedures set forth in this Statement and plan will be subject to disciplinary action. Any subcontractor not complying with all applicable Equal Employment Opportunity/Affirmative Action laws, directives and regulation of the Federal, State and Local governing bodies or agencies thereof, specifically including Section 183.04 of the Saint Paul Legislative Code and the Rules Governing Affirmative Requirement in Employment, will be subject to appropriate legal sanctions.

Involuntary Termination – The involuntary terminations notice is prepared by the supervisor/manager with concurrence of, and review by, the personnel department. The employee is notified of the termination by their supervisor/manager and will be directed to report to the personnel department for debriefing and completion of termination documentation. Involuntary termination is reserved for those cases that cannot be resolved by corrective counseling, or where a major violation that cannot be tolerated has occurred.

The following definitions and classification of violations – for which corrective counseling, performance improvement, or other disciplinary action may be taken – are merely illustrative and not limited to these examples. A particular violation may be major or minor, depending on the surrounding facts or circumstances:

- Minor violations - these are less serious violations that have some effect on the continuity, efficiency of work, safety, and harmony within the company. They typically lead to corrective counseling unless repeated or when unrelated incidents occur in rapid succession. Here are some examples of minor violations:
    - Excessive tardiness
    - Unsatisfactory job performance
    - Defacing company property
    - Interfering with another employee's job performance
    - Excessive absenteeism
    - Failure to observe working hours such as the schedule of starting time, quitting time, rest and meal periods
    - Performing unauthorized personal work on company time
    - Failure to notify the supervisor/manager of intended absence either before or within one hour after the start of a shift
    - Unauthorized use of the company telephone, Internet, or equipment for personal business

- Major violations - These more serious violations would include any deliberate or willful infraction of company rules and may preclude continued employment of an employee. Here are some examples of major violations:
    - Fighting on company premises
    - Acting in a way which might endanger the safety or lives of others
    - Departing company premises during working hours for personal reasons without the permission of the supervisor/manager
    - Bringing firearms or weapons onto the company premises
    - Deliberately stealing, destroying, abusing, or damaging company property, tools, or equipment; or the property of another employee or visitor
    - Disclosure of confidential company information or trade secrets to unauthorized persons
    - Willfully disregarding company policies or procedures
    - Willfully falsifying any company records
    - Failing to report to work without excuse or approval of management for three consecutive days
    - Bringing software into the company and installing it on company computers without authorization

- Violating the terms set out in the e-Policy
- Repeated occurrences of related or unrelated minor violations, depending upon the severity of the violation and the circumstances

Termination

Terminations are to be treated in a confidential, professional manner by all parties concerned. The supervisor, department manager, and personnel department must assure thorough, consistent, and even-handed termination procedures. This policy and its administration will be implemented in accordance with the company equal opportunity statement.

Employment with the company is normally terminated through one of the following actions:

- **Resignation –** Voluntary termination by the employee.
- **Dismissal –** Involuntary termination for substandard performance or misconduct.
- **Layoff –** Termination due to reduction of the work force or elimination of a position.

Resignation:
An employee who wants to terminate employment – regardless of employee classification – is expected to give as much advance notice as possible. Two weeks (or ten working days) is generally considered to be sufficient notice time. If an employee resigns to join a competitor, if there is any other conflict of interest, or if the employee refuses to reveal the circumstances of his or her resignation and future employer, the manager may require the employee to leave the company immediately rather than work during the notice period. This is not to be construed as a reflection upon the employee's integrity but an action in the best interests of business practice.

When immediate voluntary termination occurs for the above reasons, the employee will receive pay "in lieu of notice," the maximum being two weeks of pay based upon a 40-hour workweek at the employee's straight-time rate or salary.

Any employee not giving a full two week notice will forfeit any unpaid vacation they have accrued. Those hours need to be worked in order to receive the full benefit.

Dismissal:

- Substandard Performance – An employee may be discharged if his or her performance is unacceptable. The supervisor/manager shall have counseled the employee concerning performance deficiencies, provided direction for improvement, and warned the employee of possible termination if performance did not improve within a defined period of time. The supervisor/manager is expected to be alert to any underlying reasons for performance deficiencies such as personal problems or substance abuse. The Personnel Director must concur in advance of advising the employee of discharge action. Documentation to be prepared by the supervisor/manager shall include reason for separation, performance history, corrective efforts taken and options explored, as well as any additional pertinent information.

- Misconduct – An employee found engaged in activities showing willful disregard of company interests or policies – such as, but not limited to, theft of company property, insubordination or conflict of interest – will be terminated as soon as the supervisor/manager and personnel director have concurred with the action. Termination resulting from misconduct shall be entered into the employee's personnel file. The employee shall be provided with a written summary of the reason for termination. No salary continuance or severance pay will be allowed.

Layoff:

When a reduction in force is necessary – or if one or more positions are eliminated – employees will be identified for layoff after evaluating the following factors:

- Company work requirements
- Employee's experience, abilities and skill level
- Employee's potential for reassignment within the organization
- Employee's length of service

The immediate supervisor/manager will personally notify employees of a layoff. After explaining the layoff procedure, the employee will be given a letter describing the conditions of the layoff, such as: the effect the layoff will have on his or her anniversary date at time of call-back, the procedure to be followed if time off to seek other employment is granted, and the company's role in assisting employees to find other work.

The employee and the personnel director, after consultation with the employee's supervisor/manager, will follow one of the following procedures:

- The employee will receive at least two weeks advance notice of termination date.
- The employee will be terminated immediately and will receive one week of pay for each year of employment with the company in lieu of notice, up to a maximum of four weeks. The payment will be based on a 40-hour workweek at the employee's straight time rate or salary.

Termination Processing Procedures:

- The supervisor/manager must immediately notify the Personnel Director of the termination so that a termination checklist can be initiated. The Personnel Director will direct and coordinate the termination procedure.
- All outstanding advances charged to the terminating employee will be deducted from the final paycheck by the payroll department.
- On the final day of employment, the Personnel Department must receive all keys, ID cards, and company property from the employee.
- The Personnel Department shall conduct an exit interview with the employee, and the employee will pick up his or her final payroll check from the Personnel Department at the time of the exit interview. The final check shall include all earned pay and any expenses due the employee.

Attendance

Any employee who fails to report to work for 2 consecutive days without notice to his or her supervisor/manager will be assumed to have resigned from or abandoned his or her position. In such cases, the employee will be terminated.

E-Policies

General Principles

This policy makes it clear that Brothers Fire & Security owns and controls all workplace technology and therefore all communication and activity conducted via it. Authorized use of Brothers Fire & Security-owned or -operated computing and network resources shall be consistent with the mission of Brothers Fire & Security and of this policy. Underlying this policy is the idea that each employee is responsible for using the company's information technology resources in a manner that increases productivity, enhances the company's public image, and is respectful of other employees.

Information Technology Resources: Information technology resources are defined as all electronic devices, software, and means of electronic communication including, but not limited to, the following: personal computers and workstation; lap top computers; mini and mainframe computers; computer hardware such as disk drives (local and portable), USB devices like flash drives and tape drives; peripheral equipment such as printers, modems, fax machines and copiers; computer software applications and associated files and data, including software that grants access to external services such as the Internet; electronic mail; telephones, cellular phones, pagers, Blackberries, PDAs, Smartphones and iPhones; and voicemail systems.

Permitted General Access: As a general rule, employees are provided with a degree of access to the company's various technologies based on their job functions. Only employees whose job performance will benefit from the use of the company's information technology resources will be given access to the necessary technology. Additionally, employees must successfully complete company-approved training before being allowed access to some of the company's information technology resources.

Authorized users of Brothers Fire & Security computing and network resources may include those who do not work for the company but whose access has been authorized by management. Access, passwords, and email accounts are all granted by management of Brothers Fire & Security and therefore access to the systems can also be denied by management.

This policy defines in detail the acceptable usage of the information technology resources of the company by its employees. Generally, the resources should be used exclusively for business-related functions; however, there are a few exceptions and resources may be used to:

- Send and receive necessary and occasional personal communications
- Prepare and store incidental personal data (such as personal calendars, personal address lists, etc.) in a reasonable manner
- Utilize the telephone system for brief and necessary personal calls
- Access the Internet for brief personal searches and inquiries during meal times or other breaks or outside of work hours, provided that employees adhere to all other usage policies

In subsequent sections, this policy defines unacceptable uses of the information technology resources of the company in more detail. The company reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions, to determine if a user is violating this

policy or state or federal laws.

User Responsibilities

Privacy

No user should view, copy, alter, or destroy another's personal electronic files without permission (unless authorized or required to do so by law or regulation). In addition, users should not have an expectation of privacy. The information technology system belongs to the company and its users expressly waive any right of privacy in anything they create, store, send, or receive.

Sharing of Access

Computer accounts, passwords, and other types of authorization are assigned to individual users and should not be shared with others. You are responsible for any use of your account. If an account is shared or the password is divulged, the holder of the account will lose all account privileges and be held personally responsible for any actions that arise from the misuse of the account.

Prohibited Use

Abuse of Brothers Fire & Security computer resources is prohibited and includes, but is not limited to:

- **Game Playing:** Computing and network services are not to be used for recreational game playing. Game playing on company time is counterproductive.
- **Chain Letters:** The propagation of chain letters is considered an unacceptable practice by Brothers Fire & Security and is prohibited. If an employee receives a chain letter, the company prohibits the forwarding of that email to anyone.
- **Faxing:** Using the company fax machine or computer faxing capabilities for non-company related activities is strictly prohibited. The company prohibits the use of any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine unless authorized by management.
- **Harassing, Discriminatory, and Defamatory Use:** Employees use electronic mail for correspondence that is less formal than written memoranda. Employees must take care, however, not to let this informality degenerate into improper use. The company does not tolerate discrimination or harassment based on gender, pregnancy, childbirth (or related medical conditions), race, color, religion, national origin, ancestry, age, physical or mental disability, medical condition, marital status, sexual orientation, family care or medical leave status, veteran status, or any other status protected by state and federal laws. Under no circumstances may employees use the company's information technology resources to transmit, receive, or store any information that is in any way discriminatory, harassing, or defamatory (such as sexually explicit or racial messages, jokes, cartoons, etc.).
- **Gambling:** The use of company computers and networks to gamble is strictly prohibited.
- **Online Shopping:** The use of the company computers and the Internet to conduct personal online shopping is strictly prohibited.

- **Unauthorized Monitoring:** A user may not use computing resources for unauthorized monitoring of electronic communications. However, the company has the right – but not the duty – to monitor any aspects of its computer system, including monitoring sites visited by employees, chat groups, newsgroups, and the downloading and uploading of files.
- **Flooding or Spamming:** The company prohibits its employees to post messages to multiple list servers or news groups with the intention of reaching as many users as possible. Spamming email addresses within or outside of the company is also prohibited.
- **Private Commercial Purposes:** The computing resources of Brothers Fire & Security shall not be used for personal or private commercial purposes or for financial gain.
- **Political Advertising or Campaigning:** The use of Brothers Fire & Security computers and networks shall not be used for political purposes.
- **Software Piracy:** Access to the Internet enables users to download a wide variety of software products for a fee as shareware or for free. You are required to fulfill all license and copyright obligations of any software that you download for your own use. These software downloads become the property of the company. Any employee who knowingly violates this software piracy rule is subject to termination.
- **Use of Unlicensed Software:** The use of unlicensed software on company computers is strictly prohibited. All software for use on the company's information technology resources must be officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the company's computers by any means of transmission, unless authorized in writing in advance by [NAME – specify Technology Coordinator, Chief Information Officer, etc.]. Authorization for installing software onto the company's computers should not be given until the software to be loaded has been thoroughly scanned for viruses.
- **Pornography:** Employees are not allowed to visit sites that are considered "obscene", and are also prohibited from using company computer resources to send sexually oriented images or messages. The company may maintain a system to monitor Internet usage. In the event that an employee disregards this policy and continually visits "unauthorized" sites, it will be grounds for termination (after a warning has first been issued to the employee). The company has the right to view private files that have been downloaded to check for the propriety of these downloads.

General e-Policies

Social Media Resources:

Brothers Fire & Security expressly forbids its employees from frequenting social media-related sites in the workplace. Under no circumstances should any employee of Brothers Fire & Security use company assets (such as computers, Internet access, email, etc.) to utilize social media technologies on billable company time.

Employees are expected to adhere to this no-use policy even if there is no web filter for blocking online social networks and media-related sites in place. Brothers Fire & Security reserves the right to apply such filtering technology at any time, without warning, and at its own discretion.

Brothers Fire & Security requests that its employees remember that company technological assets are intended solely for purposes relevant to the responsibilities assigned to each associate, and that social networking sites are not defined as a requirement for any position within Brothers Fire & Security. Therefore, the use of company resources to peruse social networking or media-related sites is not permitted. Any activity conducted on such sites by employees will be considered dilatory and counterproductive to the company's goals and mission.

Acceptable Email Usage

In the operation of this company, email is a business tool. The use of email is reserved primarily for business use. Under some circumstances, Brothers Fire & Security's email systems can be used to send and receive messages to and from children, spouses, domestic partners, and immediate family – however, the time involved in such activity should be limited to no more than [15 minutes] per day.

General Email

In general, the use of Brothers Fire & Security's email system as medium for the bulk distribution of information is discouraged.

On rare occasions, email may be the best mechanism to distribute information to large segments of the Brothers Fire & Security community. Approval of a designated official is required for messages sent to more than 100 people.

In addition, these guidelines should be followed:

- Messages should be plain text with no attachments. If recipients require another kind of material, it can be posted at a website and links included in the message.
- Distribution lists should be kept private. This can be done by listing recipients in BCC addresses instead of To: addresses or CC addresses.
- Timing and other details of bulk mailings should be coordinated with the company postmaster.

Accurate Communication via Email

All employees should make every attempt to communicate truthfully, accurately and clearly via email. Employees should use the same due care in drafting email as they would for any other company communication.

Spamming

Employees are prohibited from sending spam (unsolicited email) and company-wide email messages to all employees without the approval of an appropriate supervisor.

Spoofing

Employees are prohibited from hiding their identity ("spoofing") when sending email. All anonymous or pseudonymous email messages are prohibited.

Confidential and Sensitive Information via Email

Sending proprietary information, trade secrets, or other confidential information of the company via email is strictly prohibited. This type of information is a valuable asset of the company and its unauthorized dissemination may result in civil liability as well as criminal penalties. Email messages are like paper documents. Client-related email messages should be carefully guarded and protected. Before sending an email message, every employee should think about how a third party to the message might interpret the message.

Blind 'Carbon Copies'

Due care must be exercised when sending blind carbon copies (BCC) of email messages. All employers using "blind CC" must ensure that the addressee's privacy is not violated.

Email Retention

Email is a generic term and does not refer to any particular type of record; however, most email is typically considered to be correspondence. Records in email systems include not only the messages sent and received, but also the transmission and receipt data as well.

Since email is considered a usually type of correspondence, email retention periods should agree with company records retention policy.

If you have determined that the email message is not correspondence, but it is another type of record, then review the appropriate retention schedule to determine the applicable retention / disposition period.

Certain email messages may be considered non-records. Examples of such non-records include:

- Non-business Listserv messages
- Courtesy copies (duplicates) of messages
- Minor non-policy announcements or reminders (i.e., blood drives, company fund raising activities, etc.)

All employees are responsible for retaining emails. Employees are also responsible for

deleting drafts and non-business email messages once they are no longer needed. Do not assume that even though you have deleted email messages that they cannot be recovered.

Management Access to Technology Resources

Information Assets are Company Property: All messages sent and received (including personal messages) and all data and information stored on the company's electronic mail system, voicemail system or computer system(s) is company property, regardless of the content. As such, the company reserves the right to access all of its information technology resources – including its computers, voicemail, and electronic mail systems – at any time, and at its sole discretion.

Employee Privacy: Although the company does not wish to examine the personal information of its employees, the company may need to access its information technology resources – including computer files, electronic mail messages, and voicemail messages – on occasion. Employees should therefore understand that they have no right of privacy with respect to any messages or information created or maintained on the company's technology resources, including personal information or personal messages. The company may, at its discretion, inspect all files or messages on its information technology resources at any time for any reason. The company may also monitor its information technology resources at any time in order to determine compliance with these policies for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

Employees should assume that any communication – whether business-related or personal – that they create, send, receive, or store on the company's information technology resources may be read or heard by someone other than the intended recipient. In particular, highly confidential or sensitive information should not be sent through email or the Internet.

The company reserves the right to keep an employee's email address active for a reasonable period of time following an employee's departure from the company to ensure that important business communications reach the company. Brothers Fire & Security will review such communications and send any appropriate personal communications along to the former employee if the employee provides forwarding information at the time of termination.

Monitoring: Brothers Fire & Security has the right to monitor any and all usage of its computer systems including (but not limited to) sites visited by users on the Internet, chat groups, and newsgroups, and downloaded or uploaded software. All employees must be aware that the company may use automated software to monitor documents created, stored, sent, or received.

Passwords: Some of the company's information technology resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. Passwords do not confer any right of privacy upon any employee of the company – therefore, even though employees may maintain passwords for accessing information technology resources, employees must not expect that any information maintained on the information technology resources (including electronic mail and

voicemail messages) is private. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access coworkers' systems without express authorization.

Data Collection by the Company: The best way to guarantee the privacy of personal information is to refrain from storing or transmitting it on the company's information technology resources. To ensure that employees understand the extent to which information is collected and stored, below are examples of information maintained by the company (the company may, however, at its sole discretion, and at any time, alter the amount and type of information that it retains):

- Telephone Use and Voicemail – Records may be kept of all calls made from and to a given telephone extension. Although voicemail is password protected, an authorized administrator can reset the password and listen to voicemail messages.
- Electronic Mail (Email) – Electronic mail may be backed up and archived. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail.
- Desktop Facsimile Use – Copies of all facsimile transmissions sent and received may be maintained on a facsimile server.
- Document Use – Each document stored on the company computers has a history that shows which users have accessed the document for any purpose.
- Internet Use – Internet sites visited, the number of times visited, and the total time connected to each site may be recorded and periodically monitored.
- Deleted Information – Deleting or erasing information, documents, or messages maintained on the company's information technology resources is, in most cases, ineffective. All employees should understand that any information kept on the information technology resources may be electronically recovered regardless of whether it was "deleted" or "erased" by an employee. Because the company periodically backs up all files and messages – and because of the way in which computers re-use file storage space – files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.

Document Retention Policy/Schedule

This policy specifies how important documents (hardcopy, online or other media) should be retained, protected and eligible for destruction. The policy also ensures that documents are promptly provided to authorities in the course of legal investigations or lawsuits.

SCHEDULE:

CORPORATE RECORDS:	
Articles of Incorporation	Permanent
Sales Tax Exemption documents	Permanent
Tax or employee identification number designation	Permanent
Annual Corporate filings	Permanent
FINANCIAL RECORDS:	
Chart of Accounts	Permanent
Fiscal Policies and Procedures	Permanent
Audits	7 Years
Financial Statements (Audited)	Permanent
General Ledger	Permanent
Check registers/books	7 Years
Business expenses documents	7 Years
Accounts Receivable Invoices	7 Years
Credit Card Receipts	7 Years
Accounts Payable Invoices and check stubs	7 Years
TAX RECORDS:	
Annual Tax filing for the organization	Permanent
Payroll Registers (electronic with in Software Program)	Permanent
Payroll tax withholdings	7 Years
Earnings records	7 Years
Time Sheets	7 Years
Payroll tax returns	7 Years
W-2 Statements	7 Years
PERSONNEL RECORDS:	
All contents of Employee Personnel Folder – including but not limited to – New hire packet; Offer letter; Benefits description per employee; Pension records; Employee applications and resumes; promotions, demotions, letter of reprimand, annual reviews, termination; job descriptions; workers compensation records; salary ranges; I-9 Forms	7 Years after Termination
Employee Set up and all history Information – (Electronic information with Software Program)	Permanent
INSURANCE RECORDS:	
All Insurance Policies – Work comp, general liability, auto, property, etc	7 Years after change in policy
Safety (OSHA) reports	7 Years
CONTRACTS:	
Construction Contracts – AKA/Job Files	7 Years after completion of project
Legal correspondence	7 Years
Leases/Deeds	Permanent
Loan/Mortgage Contracts	Permanent

Document Destruction: Hardcopy of documents will be destroyed on the premises by shredding after they have been retained until the end of the Document Retention Schedule.