Information Security Policy

Effective Date: January 06, 2025

1. Statement of Policy

COMFORT BREEZE HVAC REFRIGERATION LLC ("Employer") is committed to the highest standard of information security. In doing so, Employer implements this Information Security Policy ("Policy") to effectively communicate to its employee base the proper way to properly identify, categorize, and handle different levels of secured information.

This Policy applies to all employees and contractors of COMFORT BREEZE HVAC REFRIGERATION LLC. This Policy also applies to all individuals and entities who use Employer's resources including but not limited to, contractors, temporary employees, and volunteers. This Policy is not intended to restrict communications or actions protected or required by applicable law.

As such, everyone listed above is expected to:

- Read, understand, and follow this Policy. You must seek guidance from your manager or other designated Employer resource before taking any actions that create information security risks or otherwise deviate from this Policy's requirements. Employer may treat any failure to seek and follow such guidance as a violation of this Policy.

- Keep this Policy Confidential. Do not share this Policy with any person or entity within or outside of COMFORT BREEZE HVAC REFRIGERATION LLC unless authorized by the Information Security Coordinator. The Information Security Coordinator maintains a set list of approved persons and entities to whom this Policy can be shown. It is the Information Security Coordinator's responsibility to oversee, evaluate, and assess person and entity risks before granting permission for the Policy to be shared.

Strong information security requires diligence by all workforce members, including employees, contractors, volunteers, authorized partners and any others accessing or using our information assets.

2. Definitions

For the purpose of this Policy:

"Publicly Available" shall mean information that Employer has made available to the general public. Information received from another party including customers that is covered under a current, signed non-disclosure agreement must not be classified or treated as Public Information

"Confidential Information" shall mean information that may cause harm to Employer, its customers, employees, or other entities or individuals if improperly disclosed, or that is not

otherwise publicly available.

"Restricted Information" shall mean information that may cause serious and potentially irreparable harm to Employer, its customers, employees, or other entities or individuals if disclosed or used in an unauthorized manner.

3. Scope

This Policy provides detailed information security guidance that you must follow in addition to any other relevant documentation, including an Employee Code of Conduct and Employee Handbook. This Policy covers all written, verbal and digital information held, used or transmitted by or on behalf of the Employer, irrespective of media. This includes, but is not limited to:

a. paper records;
b. hand-held devices;
c. telephones;
d. information stored on computer systems; and
e. information passed on verbally.

The information covered in this Policy may include:

a. personal data relating to, but not limited to, staff, customers, clients or suppliers;
b. other business information; and
c. confidential, classified, restricted and publicly available information.

4. Guiding Principles

Employer follows these guiding principles when developing and implementing information security controls:

a. COMFORT BREEZE HVAC REFRIGERATION LLC strives to protect the confidentiality, integrity, and availability of its information assets and those of its clients/customers.
b. We will comply with applicable information security, privacy, and data protection laws.
c. We will balance the need for business efficiency with the need to protect sensitive, proprietary, or other confidential information from undue risk.
d. We will grant access to sensitive, proprietary, or other confidential information only to those with a need to know and at the least level of privilege necessary to perform their assigned functions.

5. Responsibilities

The Employer and its leadership recognize the need for a strong information security program.

The below will be implemented to ensure this goal is met:

a. Understand the information classification levels defined in the Information Security Policy.

b. As appropriate, classify the information for which one is responsible accordingly.
c. Access information only as needed to meet legitimate business needs.
d. Not divulge, copy, release, sell, loan, alter or destroy any information without a valid business purpose and/or authorization.
e. Protect the confidentiality, integrity and availability of Employer Information in a manner consistent with the information's classification level and type.

6. Classification Levels

Maintenance of this Policy is the responsibility of Employer's Information Security Coordinator. The use of this Policy has been approved by COMFORT BREEZE HVAC REFRIGERATION LLC's executives/board members. It is the responsibility of the Information Security Coordinator to ensure that the Policy is reviewed at least annually and remains consistent. This Policy is enforced by the Information Security Coordinator and the appropriate team within COMFORT BREEZE HVAC REFRIGERATION LLC.

a. Classification Levels

The Employer has established a classification scheme to protect information according to risk levels. The information classification scheme allows the Employer to select appropriate security controls and balance protection needs with costs and business efficiencies.

The classifications levels are:

i. Restricted Information

The following Classified Information is classified as Restricted:

- Social security number
- Bank account number
- Driver's license number
- State identity card number
- Credit card number
- Protected health information (as defined by HIPAA)

Sharing of Restricted Information within the Employer may be permissible if necessary to meet the Employer's legitimate business needs. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), no Restricted Information may be disclosed to parties outside the Employer, including contractors, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted Information; (ii) not to disclose the Restricted Information to any other party for any purpose absent the Employer's prior written consent or a valid court order or subpoena; and (iii) to notify the Employer in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy.

ii. Confidential Information

Employer Information is classified as Confidential if it falls outside the Restricted classification, but is not intended to be shared freely within or outside the company due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include all non-Restricted Information contained in personnel files, misconduct and law enforcement investigation records, internal financial data, donor records, and education records (as defined by FERPA).

Sharing of Confidential Information may be permissible if necessary to meet the Employer's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential Information to parties outside the Employer, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of the information; (ii) not to disclose the information to any other party for any purpose absent the Employer's prior written consent or a valid court order or subpoena; and (iii) to notify the Employer in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this Policy.

iii. Publicly Available

Employer Information is classified as Publicly Available if it is intended to be made available to anyone inside and outside of COMFORT BREEZE HVAC REFRIGERATION LLC.

7. Acceptable Use Policy

Employer provides employees and others with network resources and systems to support its business requirements and functions. This section limits how you may use Employer's information assets and explains the steps you must take to protect them.

If you have any questions regarding acceptable use of resources, please discuss them with your manager or contact the Information Security Coordinator for additional guidance.

a. General Use of Information Technology Resources. Employer provides network resources and systems for business purposes. Any incidental non-business use of Employer's resources must be for personal purposes only. Do not use Employer's resources for commercial purposes, personal gain, or any purpose that may create a real or perceived conflict of interest with COMFORT BREEZE HVAC REFRIGERATION LLC.

Do not use Employer's resources in a manner that negatively impacts your job performance or impairs others' abilities to do their jobs. Employer's network and systems are subject to monitoring.

Do not use Employer's network or systems for activities that may be deemed illegal under applicable law. If Employer suspects illegal activities, it may report them to the appropriate authorities and aid in any investigation or prosecution of the individuals involved.

b. Prohibited Activities. Employer prohibits using its resources to engage in activities such as (but not limited to) the following:

i. hacking, spoofing, or launching denial of service attacks;
ii. gaining or attempting to gain unauthorized access to others' networks or systems;
iii. sending fraudulent email messages;
iii. distributing or attempting to distribute malicious software (malware);
iv. distributing or attempting to distribute malicious software (malware);
v. spying or attempting to install spyware or other unauthorized monitoring or surveillance tools;
vi. committing criminal acts such as terrorism, fraud, or identity theft;
vii. downloading, storing, or distributing materials in violation of another's copyright;
viii. uploading, downloading, or disseminating defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate or offensive messages or media;
ix. distributing joke, chain letter, commercial solicitations, or hoax emails or other messages (spamming);
x. using encryption or other technologies in an attempt to hide illegal, unethical, or otherwise inappropriate activities; and
xi. installing or distributing unlicensed or pirated software.

The Employer may block or limit access to particular services, websites, or other internet-based functions according to risks and business value. Recognize that inappropriate or offensive websites may still be reachable and do not access them using Employer resources.

c. General Internet Use. Limit your web browsing and access to streaming media (such as videos, audio streams or recordings, and webcasts) to business purposes or as otherwise permitted by this Policy. Internet use must comply with this Policy.

Never use internet peer-to-peer file sharing services, given the risks to Employer 's information assets they create.

d. Email and Social Media. Do not disclose Confidential or Restricted Information to unauthorized parties on blogs or social media or transmit it in unsecured emails or instant messages.

Use good professional judgment when drafting and sending any communications. Remember that messages may be forwarded or distributed outside your control, and your professional reputation is at stake. Email signatures should be professional, appropriate for your business role, and not long or complex.

Never open an email attachment that you did not expect to receive, click on links, or otherwise interact with unexpected email content. Attackers frequently use these methods to

transport viruses and other malware. Be cautious, even if messages appear to come from someone you know because attackers can easily falsify (spoof) email senders. Employer may block some attachments or emails based on risk.

Do not respond to an email or other message that requests Confidential or Restricted Information unless you have separately verified and are certain of its origin and purpose. Even then, always protect Confidential or Restricted Information as described in this Policy.

If you have any doubts regarding the authenticity or risks associated with an email or other message you receive, contact the Information Security Coordinator immediately and before interacting with the message. Do not reply to suspicious messages, including clicking links or making unsubscribe requests. Taking those actions may simply validate your address and lead to more unwanted or risky messages.

e. Mobile Devices and Bring Your Own Device to Work. Mobile devices, including laptops, smartphones, and tablet computers, can provide substantial productivity benefits. Mobile storage devices may simplify information exchange and support business needs. However, all these mobile devices also present significant risks to information assets, so you must take appropriate steps to protect them.

Use encryption, other protection strategies (for example, device management software, access controls, remote wiping in case your device is lost or stolen, or other security controls), or both on any mobile or personal device that contains Confidential Information, Restricted Information, or has access to the employer's network. Mobile and other personal devices, including those that provide access to Employer email, must be protected using a password or other approved authentication method.

f. Communications and transfer of information. Staff must abide by the following when communicating about work-related matters and when in transfer of work-related data:

    i. When speaking in public places (e.g., when speaking on a mobile phone), Staff must take care in maintaining confidentiality.
    ii. Confidential Information must be marked 'strictly private and confidential' and circulated only to those who need to know the information in the course of their work.
    iii. Confidential Information must not be removed from the Employer's offices (and systems) unless required for required for authorized business purposes, and then only in accordance with the subsequent paragraph.
    iv. If the removal of Confidential Information from the Employer's offices is permitted, all reasonable steps must be taken to maintain the confidentiality and integrity of the information. This includes, but is not limited to, Staff ensuring that Confidential Information is:

        1. stored with strong password protection, with devices and files kept locked when

not in use;
2. not transported in see-through or other unsecured bags or cases, when in paper copy;
3. not read in public places when working remotely (e.g., in waiting rooms or on trains); and
4. not left unattended or in any place where it is at risk (e.g., in airports or conference centers).

v. Care must be taken to verify all postal and email addresses before any information is sent concerning work-related matters. Particular care must be taken when checking and verifying email addresses where auto-complete features may have inserted incorrect email addresses.
vi. Before sending an email, all sensitive or particularly confidential information should be encrypted.

g. Office Access. All office doors, office keys and access codes must, at all times, be kept secure. Office keys and access codes must at no time be given to or communicated to any third parties.

h. Visitors. All visitors must:

i. Sign it at reception;
ii. be accompanied by staff at all times; and
iii. not be left alone in areas or situations where they may have access to Confidential Information.

Meetings with visitors must, where possible, take place in meeting rooms. If a visitor meeting takes place outside a meeting room, in an office or other room containing Employer information, steps must be taken to ensure no Confidential Information is visible and accessible to the visitors.

8. Reporting Data and Security Breaches

Applicable law may require Employer to report cyber incidents that result in the exposure or loss of certain kinds of information or that affect certain services or infrastructure to various authorities or affected individuals or organizations, or both. The Information Security Coordinator's incident response plan includes a step to review all incidents for any required notifications. Coordinate all external notifications with Legal and the Information Security Coordinator. Do not act on your own or make any external notifications without prior guidance and authorization. All Staff are under an obligation to report actual or potential data protection compliance breaches to appropriate personnel so that Employer can:

a. investigate the breach and take any necessary remedial actions;
b. maintain a register of compliance breaches; and
c. make any applicable notifications to applicable authorities

Data breaches vary widely and include physical and technical issues. Some examples of data and security incidents that you should report include, but are not limited to:

a. loss or suspected compromise of user credentials or physical access devices (including passwords, tokens, keys, badges, smart cards, or other means of identification and authentication);
b. suspected malware infections, including viruses, Trojans, spyware, worms, or any anomalous reports or messages from anti-virus software or personal firewalls;
c. loss or theft of any device that contains Employer or customer/client information (other than Public Information), including computers, laptops, tablet computers, smartphones, USB drives, disks, or other storage media;
d. suspected entry (hacking) into Employer's network or systems by unauthorized persons;
e. any breach or suspected breach of Confidential or Restricted Information;
f. any attempt by any person to obtain passwords or other Confidential or Restricted Information in person or by phone, email, or other means (sometimes called social engineering, or in the case of email, phishing); and
g. awareness of a compromised computer or other device
h. any other any situation that appears to violate this Policy or otherwise create undue risks to Employer's information assets.

For all reporting and questions concerning the Employer's reporting procedure, please contact Daniel Holifield at comfortbreezellc@gmail.com and 251-262-0062.

9. Training

Employer recognizes that an astute workforce is the best line of defense. We will provide security training opportunities and expert resources to help employees and contractors understand their obligations under this Policy and avoid creating undue risks. Employees must complete the information security training assigned them upon hiring and throughout their employment with Employer. All workforce members must complete information security training on at least an annual basis. Managers must ensure that their employees complete all required training.

10. Disciplinary Action

Any violation of this Policy may result in disciplinary action or other sanctions. Sanctions may include suspension, access restrictions, work assignment limitations, or more severe penalties up to and including termination, in accordance with applicable law. If Employer suspects illegal activities, it may report them to the applicable authorities and aid in any investigation or prosecution of the individuals involved.

Company Information

COMFORT BREEZE HVAC REFRIGERATION LLC
13340 Tom Gaston Rd
Mobile, Alabama 36695

Information Security Coordinator

Name: Daniel Holifield
Email: comfortbreezellc@gmail.com
Telephone number: 251-262-0062