Code of Conduct

We expect our employees, including officers and executives, to comply with applicable laws, regulations, company rules and policy, and instructions from supervisors. We expect our employees to always treat customers, vendors, and employees respectfully, courteously, and professionally. We prohibit conduct that is rude, condescending, discourteous, unprofessional, offensive, disparaging, insubordinate, disruptive, and defamatory. We expect our employees to conduct business in a professional, ethical manner, and with integrity. This means:

- We never compromise our integrity or the integrity of a fellow employee or customer.
- We protect our business' reputation.
- We adhere to a set of professional values, tell the truth, and keep promises.
- We always treat others courteously and with respect.

Disciplinary action, including possible immediate dismissal, will be taken if an employee's or manager's conduct is considered in violation of the Code of Conduct, applicable policies, laws or regulations.

Employment-At-Will

Our company adheres to the policy of employment-at-will. This means the company or the employee can terminate the employment relationship at any time, for any reason, or with two-weeks' notice, for no reason at all. **Nothing contained herein is to be construed as creating a contract of employment.**

No Harassment

We prohibit harassment by employees, customers and vendors toward any other person. Violation of this policy will result in disciplinary action, up to and including immediate discharge.

Anti-Harassment

Harassment includes verbal or physical conduct that shows hostility or aversion toward an individual (or group of individuals) with the intent of creating an intimidating, hostile or offensive work environment in regard to any category protected under federal, state, or local law, including a person's **Race, Color, Religion, Gender, Age, National Origin, Disability, Sexual Orientation, or Gender Identity.** Be respectful at all times. We aren't here to regulate your personal morality. Rather, this policy assures that no employee, customer or vendor will harass or bully another person.

Harassment adversely affects work performance and morale. It is not always easy to define harassing behaviors, but they certainly include slurs, epithets, threats, derogatory comments, inappropriate touching, unwelcome jokes, and teasing. In addition to in-person, harassment can occur over social media and other technological mediums. If you have any questions about what

constitutes harassing behavior, or what conduct is prohibited by this policy, please reach out to management, or **TALK TO US**.

Sexual Harassment is Never Allowed. EVER.
Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when this conduct explicitly or implicitly affects an individual's employment, unreasonably interferes with an individual's work performance, or creates an intimidating, hostile, or offensive work environment.

Sexual harassment can occur in a variety of circumstances, including but not limited to the following:

- The victim as well as the harasser may be a woman or a man. The victim does not have to be of the opposite sex.
- The harasser can be the victim's supervisor, an agent of the employer, a supervisor in another area, a co-worker, or a non-employee.
- The victim does not have to be the person harassed but could be anyone affected by the offensive conduct.
- Unlawful sexual harassment may occur without economic injury to or discharge of the victim.
- The harasser's conduct must be unwelcome.

If you believe you or someone else is a victim of harassment, promptly report the actions or behavior to management, or **TALK TO US**. You will be directed to a person who can best help with your situation and who will investigate to your concern as quickly as possible.

During an INVESTIGATION of Workplace Harassment:
- You have the right and responsibility to report in good faith any harassing behaviors in the workplace.
- We trust all employees will act responsibly in using this policy; any accusations not made in good faith may result in disciplinary actions.
- First Watch and its subsidiaries will investigate reported incidents of harassment as soon as possible.
- Remedial actions toward the accused harasser may take place immediately.
- We will investigate every reported incident as discreetly and confidentially as possible, keeping all parties aware of the investigation process and results.
- No reprisals will be made against you, or any employee participating in good faith in an investigation, as a result of a harassment complaint.

Anti-Retaliation
You will not be penalized or retaliated against for reporting improper conduct, harassment, discrimination, retaliation, or other actions you in good faith believe may violate this policy. It is important to report all policy violations so appropriate action can be taken.

Whistleblower Policy

First Watch and its subsidiaries are committed to facilitating open and honest communication relevant to its governance, finances, and applicable laws and regulations. As such, you are expected to report unlawful activities taking place in the workplace.

A whistleblower is an employee of First Watch and its subsidiaries who reports an activity that he or she considers to be illegal to one or more of the individuals listed below. The whistleblower is not responsible for investigating the activity or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.

If you have knowledge or a concern of illegal activity in the workplace, you are encouraged to contact Human Resources, your manager/supervisor, or anyone in management with whom you are comfortable speaking. All violations or suspected violations of the law will be investigated promptly and thoroughly.

Violations or suspected violations may be submitted on a confidential and/or anonymous basis. To the extent possible and permitted by law, the confidentiality of the whistleblower will be maintained. However, a whistleblower's identity may have to be disclosed in order to conduct a thorough investigation, to comply with the law and/or to provide the accused individuals their legal rights to defense.

Retaliation against a whistleblower is strictly prohibited. Any whistleblower who believes he or she is being retaliated against is encouraged to immediately contact Human Resources, his or her manager or supervisor, or anyone else in management. The right of a whistleblower for protection against retaliation does not include immunity for any personal wrongdoing that is alleged and investigated.

You must exercise sound judgment to avoid baseless allegations. An employee who intentionally files a false report of wrongdoing will be subject to discipline up to and including termination.

Nothing in this policy is intended to or prevents employees from engaging in protected whistleblowing rights. Employees will not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that is made: (1) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, and solely for the purpose of reporting or investigating a suspected violation of law; or (2) in a complaint or other document filed in a lawsuit or proceeding, if such filing is made under seal.

Conflict of Interest Policy

First Watch and its subsidiaries expect its employees to conduct their business according to the highest ethical standards of conduct and to comply with all applicable laws. This policy is intended to increase awareness of potential conflicts of interest and establish a procedure for reporting them. Any violation of this Policy or applicable laws or standards will subject you to disciplinary action, up to and including discharge. Further, it may involve a violation of laws,

resulting in significant civil or criminal penalties for First Watch and its subsidiaries and the individuals involved, including possible jail sentences for individuals. Failure to report a potential or actual violation may, by itself, subject you to disciplinary action up to and including discharge.

Conflict of Interest

You should always act in the best interest of First Watch and its subsidiaries and not permit outside interests to interfere with your job duties. You may not use your position of employment or First Watch and its subsidiaries' relationship with its clients, customers, vendors, suppliers, and contractors for private gain or to obtain benefits for yourself or for members of your family.

For purposes of this policy, a potential conflict of interest occurs when an employee's outside interests (for example, financial or personal interests) interfere with First Watch and its subsidiaries' interests or work-related duties. For example, a conflict of interest can occur when you are in a position to influence a decision that may result in a personal gain or gain for a family member as a result of your business dealings.

If you have any questions about whether a situation is a potential conflict of interest, please contact your direct supervisor or **TALK TO US.**

Favors and Gifts

Business decisions should be made in the best interests of First Watch and its subsidiaries. You may not seek or accept any gifts, favors, entertainment, payment or loans for yourself or your family from any client, customer, vendor, supplier, or contractor, or any other party doing business with First Watch and its subsidiaries. If you violate this policy, you may be subject to discipline, up to and including termination.

Anticorruption Compliance and Relations with Customers, Suppliers, and Competitors

You must refrain from directly or indirectly engaging in corrupt activities anywhere in the world. Situations that create the appearance of improper conduct should also be avoided. Bribery of government officials is illegal and contrary to First Watch policy.

Bribery is the offer, promise, payment, or acceptance of money, gifts, or other favors to gain a business advantage. Corruption is the misuse of public power for private profit or personal gain. Bribery and corruption – whether involving government officials or commercial entities – is prohibited by the U.S. Foreign Corrupt Practices Act (FCPA), which criminalizes bribery of government officials.

You are prohibited from offering, paying or making payments or offering or giving anything of value to government officials in order to improperly obtain a business advantage. "Anything of value" means anything that might have value to a government official, including cash, gifts, meals, entertainment, travel and lodging, personal services, business opportunities, or offers of employment. There is no monetary threshold, and therefore, any amount could be considered a bribe. A modest meal related to a government employee's legitimate business on the property would likely not violate the FCPA, but a fancy expensive dinner would.

A government official is any officer or employee of any government or government-controlled entity anywhere in the world. Government officials also include political parties and party officials, candidates for political office, employees of public international organizations such as the United Nations, Red Cross, or World Bank, and all levels of officials of any commercial enterprise partially-owned, owned, controlled, or operated by a government such as national customs or tax authorities.

Payments to third-parties are illegal when you have knowledge that the third-party will give some portion of the payment to a government official. Knowledge includes actual knowledge or a firm belief that a payment or offer is being made, will ultimately be made, or is substantially certain to be made to the government official. Knowledge also includes the conscious disregard of, or "willful blindness" to, circumstances that indicate a substantial likelihood that the third-party will pass on some of the payment to a government official to obtain business. Even if bribery is customary or legal in a particular place, keep in mind that it is always a violation of our policy and never allowed.

We may never hire a third-party to do something that we may not ethically or legally do ourselves. Employees and third-parties alike should refuse any request or demand to participate in bribery or corruption.

Furthermore, you may not lend to or accept a loan or credit from any of our customers, tenants, vendors/suppliers or competitors, or from any of their employees, supervisors or managers or other agents or representatives.

Gratuities for services rendered to restaurant employees are acceptable within the ordinary course of business, as are personal loans from banks or other financial institutions, which may also do business with us. All of our purchases for goods and services are to be done strictly on the basis of price, quality, performance and our particular commercial requirements.

You shall deal fairly with our customers, suppliers, competitors and employees and should not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice.

Reporting Procedure

If you become aware of any potential conflict of interest or ethical concern regarding your employment or another employee at First Watch or its subsidiaries, you must promptly speak to, write, or otherwise contact your direct supervisor, or, if the conduct involves your direct supervisor, the next level above that person, as soon as possible. You should be as detailed as possible. We will investigate all concerns regarding conflicts of interest.

Cooperation With First Watch and Law Enforcement

You must fully cooperate with all law enforcement and other governmental authorities in a truthful and honest manner. You must also cooperate fully and truthfully with any and all Frist Watch investigations and audits.

You may not withhold, tamper with, or fail to communicate relevant information in connection with an externa or internal investigation or audit of First Watch.

Failure to cooperate fully with any investigation or audit may be grounds for disciplinary action, up to and including termination of employment or business with First Watch.

You should **not** submit to any interviews, depositions, provide testimony, or answer questions about First Watch's business, products or services; produce any documents; or discuss externally compliance with this Policy or any federal, state, or local law without consulting Human Resources.

If you receive a summons or subpoena involving First Watch or its subsidiaries from any governmental agency, court, administrative agency or legal counsel, you should immediately notify a supervisor or Human Resources.

Anti-Retaliation
First Watch and its subsidiaries prohibit any form of discipline, reprisal, intimidation, or retaliation for reporting a potential conflict of interest of violation of this policy in good faith, or for cooperating in related investigations.

Accurate Books and Reporting Policy

All financial books and records must accurately reflect all funds, assets, transactions, and information pertaining to the business of First Watch and its subsidiaries.

Litigation Policy

Should you become aware of service (or any attempts at service) of a lawsuit upon First Watch and its subsidiaries, or receive information indicating a potential dispute involving the company, the matter should be immediately referred to your supervisor and Human Resources.

No lawsuit, other than routine debt collection, may be initiated by First Watch and its subsidiaries without the prior written approval of Human Resources.

Employee Discipline

Disciplinary action may be assessed at the sole discretion of First Watch and its subsidiaries, and may include a verbal warning, written warning, suspension with or without pay, demotions, reassignments, and termination. Disciplinary procedures do not modify at-will employment and do not create a contract of employment. **First Watch and its subsidiaries maintain the right to skip, repeat, or modify disciplinary procedures at its discretion**.
Examples of misconduct* that are subject to discipline and/or discharge may include:

- Violation of policies, standards, or safety rules
- Violation of the Code of Conduct

- Violation of the Conflicts of Interest Policy
- Failure to report a breach of the Conflict of Interest Policy
- Poor attendance or tardiness
- Performance issues
- Customer complaints
- Theft or dishonesty
- Disrespect toward employees, customers or other members of the public
- Failing to cooperate with supervisors or otherwise engaging in conduct that does not support the company's goals and objectives
- Failing to follow instructions of a supervisor
- Being under the influence of alcohol or a controlled substance
- Possession of a weapon on company property (subject to local or state law)
- Workplace violence
- Bullying, abusive, physical, or verbal harassment of any kind
- Discrimination against another employee, customer, or vendor
- Misuse or failure to safeguard company assets, funds, trade secrets or technology
- Falsifying or failing to maintain accurate company records
- Failure to cooperate with a workplace investigation
- Violation of cash handling procedures
- Use of video, audio, or photograph recording devises in restaurant kitchens or restrooms
- Failing to behave courteously, respectfully, and professionally

*This list is not all-inclusive. Discipline and discharge decisions will be made in the sole discretion of First Watch and its subsidiaries.

Anti-Retaliation

First Watch and its subsidiaries strictly prohibit and do not tolerate unlawful retaliation against any employee, by any employee. All forms of retaliation are prohibited, including any form of discipline, reprisal, intimidation or other form of retaliation for participating in any activity protected by law.

Any employee, regardless of position or title, whom is found to have engaged in retaliation in violation of this policy, will be subject to discipline, up to and including termination of employment.

Restaurant Safety and Security

Restaurant Security

- Keep doors locked when restaurant is not open.
- Lock up after receiving deliveries and after cleaning areas around the perimeter of the building.
- Follow proper cash handling practices. This includes keeping cash out of sight and locked up, and locking the office door when not in use.
- Do not give out keys to the building or locked storage areas.

In the event of a robbery:

- Give the robber anything they want. Do not risk your personal safety.
- Try to stay calm and follow the robber's directions. Do not argue.
- Do not make sudden movements. Tell them what you are going to do.
- When safe, call 911. Provide names of any witnesses.
- Call your Regional Manager / RVP and Human Resources to report the incident.

Personal Items and Valuables

It is your responsibility to ensure personal items are kept in a safe place and not brought into the restaurant(s). The company assumes no liability for lost or stolen property.

Stay Safe

Safety can only be achieved through teamwork. Each employee and manager must practice safety awareness by:

- Thinking defensively.
- Anticipating unsafe conditions.
- Reporting unsafe conditions.
- Notifying management of any emergency situation immediately.
- Informing management if you are injured, no matter how slight.
- Using, adjusting and repairing machines and/or equipment only if trained and qualified.
- Ask for help when lifting or pushing heavy objects.
- Knowing where the Material Safety Data Sheets (MSDS) are in your restaurant.
- Asking management if you are unsure of a safety procedure: Don't guess.
- Knowing the location of exits, First Aid Kits and Fire Extinguishers.
- Using all required safety equipment.

Be aware of things like:

- Broken glass, sharp objects (especially knives), hot food, hot pans and heavy lifting.
- Never set anything on ledges.
- Pour coffee away from the table to avoid spills and burns.
- Be alert for wet or slippery spots on the floor and clean up any spills immediately.
- Let falling things fall.

Appearance & Cleanliness

Even if you're not in direct contact with our customers every day, you represent the company with your **appearance** as well as your **actions**. You should maintain a clean and neat appearance and dress according to the requirements of your position, and are expected to present a neat, professional appearance at all times.

The following rules apply to EVERYONE:

- Read, sign, and abide by the uniform policy.
- Clothing and shoes should be in good repair, without rips, and clean.
- Avoid excessive perfume, cologne or other fragrances.

- Hair should be clean, maintained, and pulled back at shoulder length.
- Fingernails must be neat and trimmed, without cracked/chipped polish.
- Shirts are to be tucked in with a belt.
- Belts are worn with belt loops.
- Mustaches, sideburns and beards must be neat, clean and trimmed.
- Non-offensive tattoos are permitted (subject to the manager's discretion). Please see tattoo policy for further guidance.
- Small facial piercings are permitted (subject to the manager's discretion). No tongue piercings, dangling or excessive jewelry are allowed.
- No jewelry (except for a wedding ring) can be worn in prep areas.

Any employee who is not properly dressed with a clean and neat appearance consistent with this policy will be considered unsuitable to work, and may be dismissed from duty. In such a case, you will not be compensated for time spent away from work. Failure to comply with this policy and its standards will be subject to discipline, up to and including termination.

Food Safety

You are expected to comply with all local, county, and state rules concerning food safety. This includes ensuring food is from a safe source, held at a safe temperature, cooked properly, and handled to prevent cross-contamination. You must comply with all applicable food safety rules and regulations, and cooperate with any public health inspection administered by the local county, municipality or state. You must also comply with the Employee Health Foodservice Agreement and notify the person in charge anytime you experience certain conditions that may risk transmission of foodborne illnesses.

Hand Washing and Cleanliness

All employees are required to wash hands before returning to work and where necessary to prevent cross-contamination. Ensure that the restaurant, kitchen, and equipment are properly cleaned, organized, and cared for. Report needed repairs or replacements to your manager.

Workplace Romance, Non-Fraternization and Anti-Nepotism

In order to minimize the risk of conflicts of interest and to promote fairness, First Watch and its subsidiaries maintain the following policy with respect to workplace romance, non-fraternization, and anti-nepotism. Employees in violation of this policy may be subject to discipline, including termination of employment.

Workplace Romance

There are certain situations which may make it difficult to operate a business; dating someone you work with is one of them. Therefore, no person in a manager or supervisory position shall have a romantic or dating relationship with an employee whom he or she directly supervises or whose terms or conditions of employment he or she may influence (examples of terms or conditions of employment include promotion, termination, discipline, and compensation). In

addition, such persons are not allowed to live with each other, or otherwise share any type of close relationship.

To the extent possible, a supervisor or manager who has a previous romantic or dating relationship with a subordinate or employee whose terms and conditions he or she may influence may not be involved in decisions relating to that individual's promotions, raises, terminations, or other terms and conditions of employment.

All employees engaged in this type of romantic or dating relationship are required to notify their direct supervisor or to **TALK TO US**.

Non-Fraternization
Employees are expected to conduct themselves in a professional manner at all times. In particular, management personnel are expected to set a high standard of professional conduct both at work and in any social setting at events sponsored by First Watch and its subsidiaries. For this reason, management personnel are prohibited from social interaction with subordinates that may be perceived as inappropriate or harassing.

Anti-Nepotism
Anti-Nepotism essentially means that "family-members-should-not-work-together." However, First Watch and its subsidiaries recognize that family members or current employees may seek employment with the company. In order to promote a productive environment, free from conflicts of interest as well as favoritism and unfair advantage, whether perceived or real, First Watch and its subsidiaries prohibit family members (including spouse, domestic partner, parent, child, sibling, cousin, aunt or uncle, or any other person with such a close bond as to suggest conflict in the employment relationship, such as a fiancé) from working in a supervisory relationship. In addition, where working with family members in the same location creates a distraction or problem in the restaurant, whether perceived or real, the manager has the discretion to have a family member transferred to a different location, or to terminate one or both family members' employment.
You, your family member, and management must decide together who will transfer to a different location, or who will end employment.

First Watch and its subsidiaries is committed to an equal employment opportunity workforce. All hiring decisions of family members must be reviewed by Human Resources to ensure compliance with the company's policies and applicable non-discrimination laws.

Drug / Alcohol Free Workplace

For the safety of all, no employee shall report to work or be present on the company premises, in company vehicles or engage in company activities while under the influence of alcohol or **controlled substances.**

We reserve the right to request a drug and/or alcohol test based on certain circumstances in accordance with the law.* Any violation of this substance abuse policy or refusal to comply with a drug or alcohol test may result in disciplinary action, up to and including termination.

What is a controlled substance?

- Illegal drugs
- Illegal use of prescription drugs
- Illegal use of over-the-counter medicine

No Tobacco

In order to provide a safe and healthy environment for everyone at First Watch and its subsidiaries, employees are prohibited from using tobacco (including smoking, vaping, or juuling) while working and while on company premises.

This includes no use of tobacco:

- In hallways
- In break areas
- In stairwells
- In offices
- In parking lots
- In restaurants
- In restrooms
- In company vehicles

* This policy is enforced in accordance with all federal, state and local laws.

Social Media Policy

Do you blog or contribute to virtual networks or any other kind of social media? Examples might include Twitter, Yelp, Wikipedia, Facebook, YouTube or Pinterest. Of course you do! Most people participate in social media in some form or another.

Our goal is to ensure that employees of First Watch and its subsidiaries are participating on social media sites in a respectful way that protects our reputation and follows the letter of the law. Employees' use of social media can pose risks to First Watch and its subsidiaries' confidential and proprietary information, reputation, and brands, can expose the company to discrimination and harassment claims, and can jeopardize the company's compliance with business rules and laws.

To minimize these risks, avoid decreased job performance, and ensure the company's IT resources and communication systems are used appropriately, First Watch and its subsidiaries expect its employees to adhere to the following guidelines and rules regarding social media use:

- Follow the company's IT resources and communications systems policies.
- Follow the company's code of conduct, policies, and safety rules.
- Never engage in unlawful harassment or discrimination against others, including current employees, applicants for employment, and customers.

- If you write or comment about our company, use your real name, identify that you work for us and be clear about your role.
- Never represent our company in a false or misleading way. All statements must be true and all claims must be verified as fact.
- Never use vulgar or offensive language while referencing our company.
- Do not publish comments, photos, or information identifying customers, vendors, or employees, or that is meant to be private, without permission.
- Do not violate our confidentiality agreement or expose intellectual property (recipes, financial information, etc.).
- Do not discuss any potential crisis situations occurring at First Watch or its subsidiaries.
- All activity specific to First Watch and its subsidiaries must be kept professional. Your posts, comments and pictures all reflect on our company.

Failure to follow these guidelines may result in disciplinary action, up to and including termination.

Intellectual Property

A work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.

Intellectual property exists for a reason. Please respect copyrights, trademark rights, patent rights, trade secret rights, and publicity and privacy rights of First Watch and its subsidiaries. This includes recipes, financial data, this handbook, and anything else that the company reasonably would want to keep confidential. Copying material from websites without permission may be a copyright infringement.

Technology Guidelines

Use of Personal Technology
Except in the case of an emergency, personal phone calls, texting, emailing, social media or other use of personal technology (such as a cell phone) shall be prohibited between 7:00 am and 2:30 pm.

Use of Company Technology
To perform your job duties, you may be given access to company technology. **Company Technology** is defined as company owned or issued **computers**, **software** programs, **voicemail** systems, **email** addresses, **tablets**, **fax/scanners** and other telecommunication systems. All information collected, processed, stored on or transmitted over computer systems and networks owned and operated by First Watch and its subsidiaries will be treated as Company Technology.

As your employer, we have the right to monitor your use of **Company Technology**, including but not limited to reviewing emails, voice recordings, materials/documents accessed and all website/Internet activity.

Unauthorized access, disclosure, supplication, modification, diversion, destruction, loss, misuse or theft of sensitive information is prohibited. Use of Company Technology is subject to the following guidelines:

- Personal use of company phones that is excessive, unproductive, distracting or not in the best interest of the company is prohibited.
- You may not use company technology for:
  - Commercial or personal advertisements, solicitations or promotions.
  - Sharing of destructive programs; viruses or self-replicating codes.
  - Transmitting, receiving, displaying, printing, storing, forwarding or disseminating materials that are **fraudulent, illegal, harassing or offensive**.
- Our policy prohibiting sexual harassment and discrimination applies to use of computers, Internet and other company technology.
- Non-company downloads from the Internet or via hardware devices (USB drive, memory cards) must be scanned for viruses before being exposed to company hardware.
- Trade secrets, sensitive or confidential information should not be communicated via technology unless security safeguards are in place.
- Unauthorized codes or passwords to gain access to company files is prohibited.

If you lose, damage or break any equipment or company property, please let your manager know immediately. You may be held responsible for replacing damaged or broken equipment.

Use of Company Property

The use of the company's property, equipment or services for any unlawful or unauthorized purpose or personal benefit is strictly prohibited. Therefore, the removal from the company's facilities or the company's property for purposes other than company business is not permitted unless authorized in writing. This applies to property such as furnishings, equipment and supplies and to property created, obtained or copied by the company for its use, such as client lists, files, reference materials and reports, manuals, computer software, data processing systems and data bases.

The company reserves the right to monitor or review any and all data and information contained on any computer or other electronic device issued by the company. In addition, the company reserves the right to monitor or review an employee's use of the Internet, company's Intranet and company's e-mail or any other electronic communications without prior notice.

Credit Card Data and Card Handling

All company personnel who come in contact with and/or handle, store, transmit or read Customer Credit Card data (CHD), need to ensure that all relevant Payment Card Industry Data Security Standard (PCI-DSS) requirements and security measures are taken to safeguard and secure credit card data while in our possession.

The Payment PCI-DSS standard is a set of requirements for the management and handling of credit card information and cards. It was established in 2005 and is governed by VISA, Master Card, Discover, JCB and American Express to protect customer's credit card information from theft, fraud and abuse.

All employees, particularly personnel and departments with specific roles related with the processing and management of credit and debit card information, need to be aware of, and employ the following relevant security practices related to credit card information:

Prohibited Credit Card Information
Under no circumstances should the credit card **PIN or security code** be requested, stored or transmitted.

FAX Machine Usage
Any fax machine used in the transmission of credit card information must be located in a secure area that only company personnel with a job designated business reason can access. This does not limit an employee from using a fax machine for business purposes in the ordinary course. This PCI Compliant procedure is meant to ensure the safeguarding of credit card information.

Scanning Credit Cards;
Scanning of credit cards is ONLY allowed if the Security Code and all but the last 4 credit card numbers are made illegible PRIOR to the scanning of the card.

Email & Instant Messaging Communications
Sending credit card information, specifically the card number or security code via any digital medium including but not limited to email and instant messaging is STRICTLY PROHIBITED. You should also always HIGHLY discourage customers from sending their credit card information via email. If an email is received containing credit card information, delete it as soon as possible (including from the trash bin).

Physical Media
Avoid writing credit card information down on paper media, and ensure that this media is destroyed and illegible immediately after use. If collection and retention of paper containing credit card information is required for business purposes (i.e. manual credit card impression machine, group sales) after the transaction is completed, the **SECURITY CODE must be** made **ILLEGIBLE** and the paper **MUST** be physically secured (i.e. locked file cabinet).

When paper media containing credit card data is no longer required, it must be disposed of by cross-shredding only.

Offsite Storage
If off-site third-party storage is utilized, ensure that the vendor is PCI compliant prior to any vendor agreement or contract. If off site storage is simply a storage unit, ensure complete security of the unit (i.e. key or combination lock only, surveillance cameras, etc…). The storage site must meet the standards set forth by the regulatory authorities in which each property is located.

Digital Credit Card Data Storage
Electronic copies of credit card information should be deleted from all places on a computer, including but not limited to; applications (i.e. Outlook email, Excel, or Word file) and then immediately from the Recycle Bin.

Credit Card Handling
Never maintain the physical credit card for any time beyond what is required. Any area where credit cards are handled should be monitored for unlawful access. For example non-employee access should be restricted and/ or monitored by staff for un-authorized personnel and reported to management.

All employees should be trained to notify management about any unusual credit card activity, for example, being asked to scan or copy credit cards.

No Solicitation
Sorry folks: Solicitation of any products or literature to other employees (including Girl Scout Cookies) is prohibited while on working time or on company property.

This includes non-employees selling products or literature on company premises.

TALK TO US

If you believe any policy is being violated, report the concerns to management. If you prefer *not* to discuss the matter with your manager, there are additional sources listed on the TALK TO US poster, including the name and telephone number of your Regional Manager and/or Regional Vice President. Any employee, at any time, is welcome to call (844-484-8963) and ask to speak to someone that will help with your question or problem. Your call will be directed to the person who can best help you and who will respond as quickly as possible.

When YOU TALK, We Listen
- You will be treated courteously.
- The problem or concern will be handled promptly.
- The concern will be kept as confidential as possible.

Locate the **TALK TO US** poster at your restaurant.