
# CODE OF BUSINESS CONDUCT

**(Revised) September 16, 2016**

**INTENTIONALLY BLANK**

## A MESSAGE FROM THE CEO

Dear SUPERVALU Colleagues,

Integrity is, and always will be, a fundamental part of SUPERVALU's culture. We all share a responsibility for ensuring that SUPERVALU maintains its reputation as an ethical company. It's important to strive for business success, but success should never come through poor ethical choices.

As you perform your responsibilities for SUPERVALU, the Code of Business Conduct (the "Code") is intended to help you make the right ethical and legal decisions. All employees, regardless of level or role, are expected to comply with the Code and to conduct themselves with the utmost personal and professional integrity every day.

If you believe someone is violating the law, the Code or other corporate policy, you should immediately report it to your manager, Human Resources, or the Chief Compliance Officer. You may also call the SUPERVALU Employee Hotline which allows you to submit an anonymous complaint.

Our Code prohibits retaliation against anyone who raises a concern in good faith. I am personally committed to maintaining an environment where people are encouraged to raise issues.

Please take time to review the Code of Business Conduct and make sure that you adhere to it in your daily work life. If a potential course of action seems questionable, seek guidance. Questions about any of the provisions of the Code should be directed to the Legal Department for assistance.

I appreciate your commitment to upholding our high standards of business conduct.

Sincerely,

Mark Gross
President and CEO
SUPERVALU Inc.

**INTENTIONALLY BLANK**

# TABLE OF CONTENTS

# OVERVIEW

### *What This Code of Business Conduct Covers*

This Code of Business Conduct (the "Code") sets forth general standards and policies for legal and ethical conduct for many everyday business situations. The Company has also established policies that apply to specific job types or groups of employees based on their positions within the Company.

### *Persons Covered/Definitions*

This Code applies to all employees of SUPERVALU INC. and all of its banners, regions, and subsidiaries (collectively the "Company" or "SUPERVALU"), and with respect to policies herein that relate to the Company's information or electronic communications systems, it also applies to contractors, vendors and other persons who have access to Company information or such systems.

The term "employee" refers to all persons employed by the Company in a full or part-time capacity, including officers. When the terms "you" or "we" are used in this Code such terms refer to employees. When titles of officers or departments are referred to in this Code, such as Chief Executive Officer, senior management, or the Office of Ethics & Compliance, they refer to officers or departments of SUPERVALU INC. unless otherwise indicated. Similarly, the term "Board of Directors" means the Board of Directors of SUPERVALU INC.

### *Compliance*

All employees are expected to read and understand this Code, including any future published updates. Full compliance with the policies set forth in this Code is both expected and required. If you violate this Code or other Company policies, or engage in unethical or illegal conduct, you may be subject to disciplinary action up to and including termination, subject to applicable laws and regulations.

Employees who deliberately withhold information concerning another employee's violation of this Code, other Company policies, or engagement in unethical or illegal conduct may also be subject to disciplinary action.

You are required, upon request, to provide written acknowledgement of your awareness of and compliance with the provisions of this Code.

### *Seeking Advice*

From time to time, situations involving ethical issues or potential deviations from this Code may arise where it is difficult to determine the proper course of action. When that happens, do not rely solely on your own judgment. Discuss the matter with your supervisor or a higher level of management to secure their judgment before taking action, and where required, to obtain their approval.

If a situation arises that involves an actual or potential violation of law:

**Contact the Chief Compliance Officer at: (952) 828-4159 or the**

**Legal Department or (952) 828-4230**

If you are unsure of, or have questions regarding any of the policies contained in this Code:

**Contact the Office of Ethics & Compliance at: ethics.compliance@supervalu.com or**

**(952) 828-4159 or (952) 828-4230**

# REPORTING VIOLATIONS

***Procedure***

Vigilance is a key component of an effective compliance program and all of us must take responsibility for reporting violations of this Code or other unethical or illegal conduct. They may cause injuries to persons or damage property, including the Company's assets and reputation, and result in harm to our employees or shareholders.

You are required to report actual or suspected violations of this Code or other unethical or illegal conduct. Such matters should be reported using one of the following procedures:

- Contact your immediate supervisor. This may encourage the resolution of any problems within the appropriate work unit and provide valuable insights or perspectives on the matter reported.

- If you are not comfortable reporting the matter to your immediate supervisor or believe that he or she did not handle it properly after it was reported, contact your local Human Resources Department or a higher level of management within your organization.

- **If you are not comfortable with either approach or if you want to remain anonymous, call the Company's toll-free**

## EMPLOYEE HOTLINE

**at**

**1 (800) 841-6371**

The Employee Hotline is a service provided by an independent company for the purpose of reporting suspected violations. Calls to the Employee Hotline are confidential and you may remain anonymous if you wish. Your call will be promptly investigated and appropriate action will be taken as necessary. Reports concerning accounting, internal controls, fraud or audit matters will be reported to the Audit Committee of the Board of Directors in accordance with the procedures established by the Company for such purpose.

***Non-Retaliation***

It is strictly against the Company's policy for anyone to be subjected to retaliation for reporting in good faith to the Company or any legal or regulatory authority, a suspected violation of any provision of this Code, any Company policy, or any illegal or unethical conduct. If you feel that you have been retaliated against in violation of this policy, please follow the procedures for reporting suspected violations above.

# FINANCIAL INTEGRITY

## Purpose

Financial integrity is vital to the Company's continued success. To achieve this goal, the Company has adopted several measures, including the following:

- Employment of independent, objective external auditors to review the Company's financial records;
- Maintenance of an internal audit department which has responsibility for auditing and reviewing the Company's internal controls;
- Appointment of independent directors to the Audit Committee of the Board of Directors (the Audit Committee is responsible for overseeing the Company's internal and external audit processes, and the Company's maintenance of an independent relationship with the external auditors);
- Providing internal and external auditors with direct access to the Audit Committee; and
- Employment of competent management and staff with a commitment to training and a process that encourages consultation.

The purpose of this policy is to set forth the Company's expectations with respect to the standards employees and other persons acting on behalf of the Company must adhere to, in order to foster an environment within the Company that promotes financial integrity and compliance with applicable laws, regulations and accounting principles pertaining to the Company's financial transactions.

## Policy

To ensure that the Company achieves its goal of complete financial integrity, you must:

- Comply fully with all applicable accounting principles, standards, laws and regulations for the accounting and financial reporting of transactions, estimates and forecasts which pertain to the Company's business;
- Comply fully with the Company's accounting policies and procedures;
- Use rigorous business processes to ensure that management decisions and operational plans are based on sound economic analysis (including prudent consideration of risks) and that the Company's physical, financial and intellectual property assets are safeguarded;
- Prepare reports accurately and honestly to ensure accurate financial reporting, including appropriate reporting of revenue and expense recognition;
- Provide timely, candid forecasts and assessments to management when requested;
- Ensure that all Company communications regarding actual or forecasted financial information are accurate, timely and not misleading; and
- When involved in preparing or reporting any financial or business records, make certain all such records are complete, accurate and timely, and reflect all relevant business transactions.

## Violations

Maintaining financial integrity is everyone's responsibility; therefore, it is important that you report actual or suspected violations of this policy, financial irregularities or fraudulent activity promptly.

- Generally they should first be reported to your immediate supervisor.
- If you are not comfortable reporting the matter to your immediate supervisor or believe he or she did not handle it properly after you reported it, contact your local Human Resources Department or a higher level of management within your organization.
- **If you are not comfortable with either approach or if you want to remain anonymous**, **call the Company's toll-free Employee Hotline at: 1 (800) 841-6371.**

Calls to the Employee Hotline can be made anonymously and confidentially at the request of the reporting individual and retaliation for reporting alleged violations in good faith is expressly prohibited.

Shareowners, as well as general members of the public, can report alleged violations of this policy by contacting the:

**Office of Ethics & Compliance at: ethics.compliance@supervalu.com,** or

**(952) 828-4159** or **(952) 828-4230**

Complaints of a financial nature, regardless of the source of the complaint, will be handled in accordance with the Company's Procedures for the Receipt, Retention and Handling of Complaints Relating to Issues of Financial Integrity.

## Disciplinary Action

If you violate this policy, including the policy against retaliation, you may be subject to disciplinary action, up to and including immediate termination from employment, subject to applicable laws and regulations.

# REPORTING AND INVESTIGATING FRAUD

## Purpose

It is the Company's intent to promote consistent Company practices in preventing, detecting, reporting and investigating suspected fraudulent activities. This policy provides an overview of responsibilities for preventing and detecting fraudulent activities, guidelines on how to report suspected fraudulent activities and responsibilities and guidelines for investigating them and communicating the results of investigations.

This policy applies to any fraud, or suspected fraud, involving employees as well as shareholders, consultants, vendors, contractors and any other parties with or without a business relationship with the Company.

## Policy

### *Actions Constituting Fraud*

The term "fraud" refers to, but is not limited to:

- Intentional misstatements or omissions of amounts or disclosures in internal or external reports;
- Manipulation, falsification, or alteration of accounting records or other supporting documents from which internal or external financial information is prepared;
- Intentional misapplication of accounting principles to manipulate results;
- Forgery or alteration of any document or account belonging to the Company;
- Forgery or alteration of a check, bank draft, or other financial document;
- Misappropriation of funds, securities, supplies, or other assets;
- Impropriety in the handling or reporting of money or financial transactions; and
- Any dishonest or fraudulent act or similar/related inappropriate conduct.

**If there is any question as to whether an action constitutes fraud, you should contact:**

**Loss Prevention at: (952) 828-4205;**

**Internal Audit at: (952) 294-7729; or the**

**Office of Ethics and Compliance at: (952) 828-4159 or (952) 828-4230.**

**Your question may also be submitted anonymously to the Company's toll-free Employee Hotline at**:

**1 (800) 841-6371**

Allegations or suspected improprieties concerning an employee's moral, ethical, or behavioral conduct should be reported to and resolved by department management and Human Resources.

### *Management Responsibility*

Management is responsible for the prevention and detection of fraud. Each member of the management team should be familiar with the types of improprieties that might occur and the adequacy of policies, procedures and controls within their areas of responsibility to prevent them. Management must make sure that they obtain and/or provide adequate job guidance and training, as appropriate in the circumstances, to help prevent and detect fraud. Management must also be alert for any indications of irregularity and take immediate action in accordance with the requirements and guidelines of this policy.

### *Reporting Suspected Fraud*

If you suspect or discover fraudulent activity, you must promptly report it. As a general rule, you should contact your immediate supervisor. This may provide valuable insight or perspective on the matter reported. However, if you are not comfortable reporting the matter to your immediate supervisor or believe they did not handle it properly after you reported it, contact your local Loss Prevention Department, a higher level of management within your organization, or the Office of Ethics and Compliance. If you are not comfortable with these approaches, or want to remain anonymous, call the **Company's toll free Employee Hotline at:**

**1 (800) 841-6371**

Care must be taken when reporting suspected improprieties to avoid alerting suspected individuals and to keep information confidential while investigations are in process. If you are reporting a matter, you must not attempt to personally conduct investigations, perform interviews, or interrogate individuals related to any suspected fraudulent activity. Do not discuss the suspicions, facts, or allegations with anyone outside of the reporting process noted above, unless specifically directed to do so as part of a Company investigation. This is important to avoid damaging the reputation of individuals suspected of, but subsequently found innocent of, wrongful conduct.

***Investigation and Reporting Responsibilities***

Investigation of matters related to accounting, internal accounting control, or auditing will commence with the Legal Department, as described in the Company's Procedures for the Receipt, Retention and Handling of Complaints Relating to Issues of Financial Integrity. Loss Prevention with the assistance of the Legal Department, and Internal Audit if necessary, has the primary responsibility for the investigation of any other suspected fraudulent activities as defined in the procedures. Suspected fraudulent activities under investigation are also required to be reported as follows:

- Matters related to accounting, internal accounting control, or auditing must be routed to the Office of Ethics & Compliance and the Chairperson of the Audit Committee of the Board of Directors, as described in the Company's Procedures for the Receipt, Retention and Handling of Complaints Relating to Issues of Financial Integrity;
- All other cases with a total estimated loss of $2,500 or more must be reported to the Director of Loss Prevention;
- The Director of Loss Prevention must notify his/her supervisor of any cases with a total estimated loss of $5,000 or more;
- The Director of Loss Prevention must notify the Senior Director of Internal Audit of any cases involving an estimated loss of $10,000 or more; and
- The Senior Director of Internal Audit must review and follow up as considered necessary, all cases with an estimated loss of $10,000 or more and advise the Controller and Executive Vice President, Chief Financial Officer of those cases that need to be reported to the Audit Committee of the Board of Directors.

Any investigative activity required will be conducted without regard to the suspected individual's length of service, position or title, or relationship to the Company. The investigative team will have free and unrestricted access to all Company records and premises, whether owned or rented. When it is within the scope of their investigation, the investigative team will have the authority in accordance with guidelines provided by the Technology Services Department and the Legal Department, to examine, copy, and/or remove all or any portion of the contents of on-line files, computer hard drives, hard copy files, desks, cabinets and other storage facilities on Company premises without the prior knowledge or consent of any individual who may use or have custody of any such information, items, or facilities. The investigative team will treat all information received confidentially.

If the investigation substantiates that fraudulent activities have occurred, reports will be issued to applicable management personnel. Reports may also be issued to Senior Management and the Audit Committee of the Board of Directors as appropriate in the circumstances. Decisions to seek restitution, refer cases for prosecution, or refer investigation results to law enforcement or regulatory agencies for independent investigation will be made in conjunction with the Legal Department and Senior Management.

The investigative team does not have the authority to discipline an employee. The decision to discipline an employee including potential termination is the responsibility of Company management. If an investigation results in the recommendation to discipline an employee, the recommendation will be reviewed by management with Human Resources, and the Legal Department, as considered appropriate, before a final decision is made.

# SAFEGUARDING INFORMATION

**Purpose**

During the course of your employment with the Company, you may have access to or become aware of information about the Company, its customers, employees or business partners ("Company Information"). Examples include:

- Financial data, including sales reports, earnings reports, or estimates of financial performance;
- Sensitive business information such as marketing strategies, pricing policies, store development plans, and acquisition or disposition activities;
- Business processes, inventions, designs, trade secrets, and other intellectual property;
- Product specifications, or product purchase or sales forecasts;
- Vendor information, such as procurement data or pricing policies;
- Information about customers, including customer lists, personally identifiable information such as social security numbers, as well as purchase requirements, purchase history, prescription information, loyalty card, credit or other financial information; and
- Information pertaining to employees, such as wage and salary data, health records, family data, or other personally identifiable information, including social security numbers.

Company Information must be protected from unauthorized access, disclosure, reproduction, misappropriation or misuse, not only to protect the privacy of customers and employees and the value of such information, but also to prevent breaches of agreements and violations of laws pertaining to data privacy, trade secrets, business practices, and securities trading.

The purpose of this policy is to identify the types of Company Information that may arise in the ordinary course of the Company's business and the steps that employees and others engaged to perform services for the Company must take to adequately secure and safeguard such information.

**Policy**

Employees and others engaged to perform services for the Company may collect and use Company Information only for authorized purposes. While employed by the Company or engaged to provide services to the Company, and at all times thereafter, you must:

- Keep all Company Information that you possess or have access to secret and maintain it in strictest confidence; and
- Protect all Company Information that is collected, generated, accessed, maintained, transmitted or stored using the Company's informational assets (computer hardware, software, electronic communications systems and the media used to collect, store or transmit data) against unauthorized disclosure, transfer, modification, or destruction throughout its life cycle, from its origination to its destruction, in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes (electronic or paper), what technology is used or what purpose it serves.

You must also follow Company procedures and use reasonable judgment to adequately secure and safeguard Company Information, regardless of the format in which it is maintained. This requires that you:

- Do not use, reproduce, misappropriate or disclose to any third party, any Company Information that you collect, generate, manipulate, receive, transmit or have access to;
- Lock offices, access areas, storage cabinets, files and desks that contain Company Information and never leave it unattended where it can be easily viewed or accessed by others;
- Store Company Information that resides on personal computers, personal data assistants, cell phones, memory cards or storage discs, in a secure manner and safeguard such items from loss, unauthorized access or theft;

- Follow Company procedures that restrict access to physical areas where its information systems or communications systems are located;
- When accessing the Company's information or communications systems, only use passwords that are created in accordance with Company guidelines, maintain the confidentiality of such passwords and follow related security controls and codes;
- Do not disclose Company Information to anyone other than on a "need to know basis," and only to those authorized by management to receive it in order to perform their job duties;
- Destroy or discard Company Information in secure disposal facilities after it is no longer needed, unless you are required to retain it pursuant to the Company's record retention policies or have been advised by the Legal Department to retain it for other reasons;
- Ensure that service providers who may have access to Company Information are bound by confidentiality agreements; and
- Be aware of and follow any privacy or other policy the Company publishes for its customers.

If Company Information is inadvertently or wrongfully accessed or disclosed, the Company may have immediate obligations to notify customers or business partners of such access or disclosure, depending on applicable law or agreements.

**In the event Company Information is inadvertently or wrongfully accessed or disclosed, employees and others engaged to perform services for the Company must immediately notify the Technology Services Department at cyber@supervalu.com and the Office of Ethics and Compliance at (952) 828-4159 or (952) 828-4230.**

**Seek Advice**

When in doubt as to whether or not information you possess or have access to is Company Information, or if you are unsure how it should be handled, consult with senior management or call the **Legal Department at: (952) 828-4230**.

Additional policies regarding information security, data classification standards, and the handling of credit card and personally identifiable information relating to customers, employees and other parties have been developed by the Company's Technology Services Department or the Office of Ethics and Compliance. To obtain copies of these policies or for questions regarding information security procedures or privacy policies, contact the:

**Technology Services Department at IT.Communications@supervalu.com or the**

**Office of Ethics and Compliance at: (952) 828-4159 or (952) 828-4230**

# INSIDER TRADING AND STOCK TIPPING

## Purpose

Federal securities laws and the regulations adopted by the Securities and Exchange Commission prohibit persons from using material nonpublic information to trade in the stock or other securities of public companies, or passing material nonpublic information on to others who may trade on the basis of such information. This policy is intended to help prevent violations of those laws and regulations by identifying what constitutes material nonpublic information and the actions you must not engage in when in possession of such information.

## Overview

It is illegal to use material nonpublic information to trade in the stock or other securities of a public company or to disclose such information to others who may buy or sell securities based on such information. Persons who engage in such illegal conduct may be subject to significant criminal and civil penalties.

### *What is Material Nonpublic Information?*

"*Material nonpublic information*" is any information not generally known to the public, that is of such a nature that there is a substantial likelihood that a reasonable investor would consider it important in making a decision to buy, sell or hold a company's securities. **Any information that could reasonably be expected to affect the price of a company's stock or other securities is likely to be considered material,** and either positive or negative information may be material. Information is considered "public" only after it is released by a company through normal media outlets or filed with the Securities and Exchange Commission or stock exchanges, and sufficient time has elapsed for it to be circulated and absorbed by investors and the marketplace. Information is not public merely because it is the subject of widespread or publicly reported rumors, even if they are accurate.

Prior to our reporting them, each of the following examples would constitute material nonpublic information:

- Discussions, proposals or agreements for a significant transaction such as a merger, acquisition or divestiture;
- Quarterly or annual earnings or sales results or forecasts, including estimates or revisions;
- Threatened litigation or administrative actions, or material developments in such matters;
- Proposals or agreements with major customers, including obtaining or losing key contracts;
- Research and development programs;
- Business strategies or changes to business strategies;
- Changes in debt ratings; and
- Events regarding Company securities such as stock splits or changes in dividend policies.

### *What is Insider Trading?*

Insider trading means buying or selling the stock or other securities of a company while in possession of material nonpublic information relating to such company. Trades made while in possession of material nonpublic information may be unlawful even if the trader did not make a profit or avoid a loss.

### *What is Stock Tipping?*

Stock tipping means disclosing material nonpublic information about a company to another person, including a friend or a relative, thereby enabling such person to buy or sell the stock or other securities of a company on the basis of that information. The person making the tip is liable even though he or she did not actually trade and even though the trader did not make a profit or avoid a loss.

**Policy**

If you have access to "material nonpublic information" pertaining to SUPERVALU or another company (such as an acquisition candidate, customer or supplier) whose stock or other securities are publicly traded, you must not:

- Trade directly or indirectly in the securities of SUPERVALU on the basis of such information. Transactions covered by the foregoing include:
  - Open market purchases or sales;
  - Transactions in the Employee Stock Purchase Plan or 401(k) plans sponsored by the Company, such as investment allocations, fund transfers and loans or withdrawals which may involve the acquisition or disposition of shares of SUPERVALU INC. stock in a plan account;
  - The exercise of a stock option where the shares acquired upon such exercise are immediately sold (a "same day sale"); or
  - The exercise of a stock option where the exercise price or tax liability for all or a portion thereof is satisfied by having shares that would have been received upon such exercise, sold to pay the exercise price or taxes arising from the transaction ("sell to cover").
- Trade directly or indirectly in the securities of the other company on the basis of such information;
- Recommend the purchase or sale of the securities of SUPERVALU or the other company to others based on such information; or
- Disclose such information to others (including family members), except within the scope of your duties as an employee, director, consultant, contractor, advisor, or person engaged by or acting on behalf of the Company or when compelled by law, and then, only after consultation with Legal Department or external counsel.

You should also exercise due care to protect the confidentiality and security of material nonpublic information by following the Company's policy titled "Safeguarding Information" that is set forth in this Code of Business Conduct. In addition, you should ensure that members of your staff and others who may be familiar with projects you are working on are aware of this policy, especially when confidential transactions are pending.

**Penalties**

If you engage in insider trading or tipping, you may be subject to civil and criminal penalties in addition to any disciplinary action the Company may elect to take. Civil penalties include fines of up to three times the gains or losses avoided and can be imposed upon the trader and the tipper. Criminal penalties can include fines of up to $5,000,000 and 20 years in prison. If you disclose material nonpublic information to someone who trades based on that information, both you and that person may be liable under the federal securities laws. These penalties may apply regardless of whether or not you derived a benefit from the other person's actions.

**Seek Advice**

If you are in doubt as to whether or not information is "nonpublic" or "material," have questions regarding the securities of SUPERVALU or another company, or are simply uncertain whether or not you may engage in a particular transaction, then before engaging in the transaction or disclosing the information, contact the:

**Office of the Corporate Secretary at: (952) 828-4623**, or the

**Chief Compliance Officer at: (952) 828-4159**

# COMMUNICATIONS WITH THE MEDIA, SECURITIES ANALYSTS AND OTHER ENTITIES

## Purpose

The Company values the relationships it has with representatives of the media, securities analysts and investment communities who seek to accurately report on, analyze or invest in the Company, and will endeavor to provide full and prompt disclosure of all material developments and events relating to its business, consistent with the Company's disclosure obligations under the federal securities laws and the rules of the New York Stock Exchange. Communications must be coordinated throughout the Company in such a manner that ensures that they are accurate and consistent.

In addition, Regulation FD (Fair Disclosure) of the Securities Exchange Act of 1934 requires that the Company promptly disclose to the public, any material nonpublic information that is disclosed intentionally or unintentionally by the Company or any person acting on its behalf, to certain persons (generally securities market professionals such as broker-dealers, industry analysts, investment advisors, investment companies or shareholders, or others who might trade on the basis of the information).

This policy sets forth the procedures you must follow when contacted by the media, investors, or securities analysts, to avoid disclosing information that is inaccurate, inconsistent with Company policy or in violation of Regulation FD.

## Policy

Communications with the media, securities analysts and investor communities are the responsibility of the Company's Communications Department and all statements or responses to inquiries from representatives of such groups should be handled by or coordinated through those departments.

You should not disclose to, or discuss with, any securities analyst, industry analyst, investment advisor, investment company, shareholder, or other person who might trade on the basis of such communication, any material nonpublic information pertaining to the Company's business or financial performance without the prior approval of the Chief Executive Officer, the Chief Financial Officer, the Director of Investor Relations or the Director of Communications.

If a member of the news media, a securities analyst or investor contacts you with a question or a request for information, either directly or through another source, do not attempt to answer or respond. Obtain the name of the person making the inquiry and immediately notify the:

**Communications Department at: (952) 903-1645**, or the

**Investor Relations Department at: (952) 828-4144**.

A member of the appropriate department will deal with the inquiry in order to ensure an appropriate and consistent response.

Industry events, trade shows and communications activities pertaining to vendor relationships all have the potential for media, security analyst and investor exposure. For that reason, all materials related to such activities must be reviewed and approved in advance by the Communications Department or the Investor Relations Department.

# SOCIAL MEDIA

## Participation in Interactive, Online and Mobile Channels of Communication

**PURPOSE**

We are committed to improving customer experiences and providing new opportunities for engagement, proactive communications and the promotion of our Company, its banners and brands. Utilizing interactive, online and mobile channels of communication is an effective means of accomplishing that objective.

We respect the rights of our employees and independent contractors to participate in social media forums and to write, post, comment or share information in a responsible and lawful manner. This policy sets forth our expectations when such activities occur.

**SCOPE**

This policy applies to all persons employed as full or part-time employees or engaged as independent contractors of SUPERVALU INC. or any banner, region, subsidiary or affiliate thereof (collectively referred to as the "Company") regardless of their location. Our use of the first person singular or plural in this policy through terms such as "we," "our," or "us" also refers to the Company.

**KEY TERMS**

**As a public company, we are legally obligated to protect against and regulate the disclosure of Confidential Information. "Confidential Information"** is information not generally known to the public and includes but is not limited to:

- Financial data, such as sales or earnings reports, or estimates of financial performance;
- Predictions about Company business or performance;
- Sensitive business information such as marketing strategies, promotions or sales events, product launches, pricing policies, or vendor information or performance;
- Plans for the development of stores or the acquisition or disposition of assets or businesses;
- Business processes, product specifications, designs, and other trade secrets or proprietary data; and
- Customer information or information relating to other employees, such as social security numbers, health records, or credit information.

**"Social media"** is user-created video, audio, text or multimedia published in social media forums.

**"Social media forums"** are websites and other interactive communications platforms that allow users to share information, and include blogs, micro blogs, and content sharing sites such as Facebook, Twitter, You Tube, MySpace, Flickr, LinkedIn, and Wikis, as well as bulletin boards, message boards, and chat rooms:

## POLICY

### I. General Provisions

#### *Privacy Expectations*

You have no expectation of privacy when you engage in social media forums. In order to protect the Company's legal interest, we monitor postings and other communications in social media forums that reference or pertain to our Company or our brands. We also monitor and review electronic communications and data sent, received, stored or accessed using our systems or equipment and will cooperate with law enforcement and other government agencies to identify persons that communicate information in social media forums.

#### *Compliance with Other Policies*

You have an obligation to review and understand our policies pertaining to the disclosure or use of Confidential Information and the use of our electronic information systems, which are set forth in our Code of Business Conduct. Your engagement in social media forums should not violate those policies. (Pay particular attention to the policies titled: Electronic Communications; Safeguarding Information; Information Security; Insider Trading and Stock Tipping; and Communications with the Media, Securities Analysts and Other Entities.). The Code may be accessed in the Links Section of mySUPERVALU.com or you may obtain a copy from your Human Resources representative. Our Technical Services Department has also published policies on internet usage and electronic mail standards. You may obtain copies of those policies by emailing: IT.Communications@supervalu.com.

#### *Disciplinary Action*

You are solely responsible for your postings or comments in any social media forum. You may be subject to legal liability from third parties if they are found to be in violation of laws prohibiting defamation, harassment, discrimination, and other matters. You may also be liable if your postings or comments include the confidential or copyrighted information of others.

If you violate this policy, you may also be subject to disciplinary action, up to and including immediate termination from employment contracts or relationships with independent contractors and other parties may be terminated if they violate this policy, and we reserve the right to pursue all legal or equitable remedies available to us under contract, law or otherwise.

#### *Questions*

If you have questions regarding this policy, feel free to contact our Corporate Communications Department at communications@supervalu.com or our Chief Compliance Office at ethics.compliance@supervalu.com.

## II. Personal Non-Company Related Activities

We recognize that employees and independent contractors who participate in social media forums may wish to share information about the Company or their work-related experiences. However, sharing or discussing information in social media forums increases the risk that Confidential Information may be disclosed or that sensitive or inaccurate information may be communicated. Such disclosures could damage our image or reputation; create confusion in the markets we serve; affect our stock price; interfere with our ability to compete; violate the privacy rights or expectations of employees, customers or others; or violate applicable laws or regulations.

**If you participate in the social media environment, you must never:**

- Represent directly or indirectly that you are authorized to communicate on behalf of the Company unless you have been expressly authorized to do so by someone within the Company who is specifically authorized to give you such authorization;
- Make comments on behalf of the Company without prior Company authorization;
- Disclose, distribute or otherwise communicate Confidential Information;
- Make knowingly false statements about the Company, its brands, officers, directors, employees, customers, business partners, vendors or competitors; or
- Use the Company's names or trademarks for commercial purposes. Unfair competition or false or deceptive advertising is also prohibited.

**You must adhere to the Guidelines for Participation in Social Media Forums (see below).**

## III. Engagement by Persons Authorized to Represent the Company

It is extremely important that persons who use social media to communicate on behalf of the Company obtain our consent before doing so and that they be properly trained to ensure that they conduct themselves in a manner consistent with our mission, goals and objectives.

**Before engaging in social media forums as an authorized representative of the Company, you must obtain the recommendation of your supervisor, be screened for such purpose by the Human Resources Department, and approved by the Corporate Communications Department.** Contact the Corporate Communications Department to obtain a copy of the selection criteria.

If selected, you must undergo training that includes information on the types of social media, its value as a communication tool, our approach to social media, and the Securities and Exchange Commission's Regulation FD pertaining to the selective disclosure of corporate information.

## IV. Business Use of Social Media

**Specific requirements apply to the establishment and operation of social media forums by the Company or a specific banner, division, store, distribution center or department. All such sites, including Facebook and Twitter, require prior corporate approval.**

To create a Company-sponsored social media forum for a banner, region, brand or activity that reaches external audiences, the head of the department seeking to create the site must submit a request to the Corporate Communications Department that includes: (i) the business reason for the forum; (ii) its intended audience; and (iii) the expected return on the investment for the site.

When establishing any blog, space or other area within the given framework of the terms provided by the host of such spaces (e.g. Facebook, LinkedIn, Twitter, etc.), you must contact the Corporate Communications Department, before using any Company banner, brand or product as any part of the name or URL to avoid confusion with official Company communications.

**Guidelines for Participation in Social Media Forums**

**You must follow these guidelines when participating in social media forums.**

1. ***Author and commenter identification.***

   a. If you are authorized to participate on behalf of the Company, clearly identify yourself by using your legal name, indicate that you work for or are affiliated with the Company, and state your designated role or purpose for posting or commenting. If required, you must register on external sites, provide your work email address, and log-in before posting a comment.

   b. If you are not authorized to participate in such forums on behalf of the Company and the Company is the subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of the Company

2. ***Identify your comments as your own and use a disclaimer.*** If you are not authorized to participate on behalf of the Company, specifically state that your postings or comments are your own opinions, not corporate statements. Include a disclaimer such as the following:

   **"I work for [Company or specific banner name] and this is my personal opinion," or**

   **"The postings on this site are my own and don't necessarily represent [Company or specific banner name]'s positions, or opinions."**

   Managers and executives should note that a standard disclaimer does not by itself exempt you from a special responsibility when engaging in social media forums. By virtue of your position, you must consider whether the personal thoughts you publish may be misunderstood as expressing Company positions. You should also assume that employees will read what is written.

3. ***Disclose any personal interest you have in the matter you are posting about or commenting on.***
   If you are posting or commenting on the products or services of the Company, its business partners or vendors, either on their behalf or in your individual capacity, for the purpose of endorsing or promoting them or for the purpose of seeking others to provide endorsements or testimonials, you must disclose that fact, as well as the fact that you are employed by the Company. You must also disclose whether or not you are being compensated for your services or seeking to compensate others.

4. ***Accuracy is important.*** You should strive to be as accurate as possible.

   - Never represent yourself or the Company in a manner that is knowingly false or in reckless disregard of the truth.
   - Attempt to Substantiate all statements before you make them.
   - If you are commenting about a competitor, be sure that what you say is factual and does not disparage the competitor.
   - Unless you are authorized to communicate on behalf of the Company, do not respond to misrepresentations in external social media forums. Instead, notify the Corporate Communications Department at (952) 903-1645. If you work at a retail banner, contact Communications.

5. ***Respect your audience.*** Your postings or comments should be meaningful and respectful and contribute to the discussion.

6. ***Content restrictions.*** Do not post the following forms of content on any social media forum.

- Content about the Company, its brands, employees, customers or business partners that is knowingly false.
- Confidential Information that has not been approved for release to the public.
- Content that violates a legal ownership interest of the Company or any other party.
- Content that intrudes on the privacy of the Company's customers or business partners.
- Conduct that is illegal or encourages such activity.
- Profane or vulgar language, threatening content, sexual content, or links to same.
- Content that promotes, fosters or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, sexual orientation, gender identity, or other factors as protected by applicable law.

7. ***Respect copyright, trademark and fair use laws.*** You must respect the copyrighted material of others, including the Company's copyrights and brands, and exercise caution when using them.

- Postings on non-Company sponsored sites must not include the commercial use of our logos or trademarks
- The use of our logos or trademarks in a manner that constitutes unfair competition or false or deceptive advertising is also prohibited.
- You should not post any copyrighted material unless you **ow**n the copyright for such material, have written permission from the copyright owner to post it, or are sure that its use is permitted by the legal doctrine of "fair use."
- You should never quote more than short excerpts of someone else's work, and it is a good practice to link to others' work or properly cite the reference to it.

8. ***Never disclose or comment on Confidential Information.***

9. ***Correct your own mistakes.*** If you make an error related to information that you have posted or commented on, indicate your mistake and correct it quickly. If you choose to modify an earlier posting or comment, clearly indicate that you have done so.

10. ***Use good judgment.*** There may be consequences to what you publish, especially if you violate the law or Company policy (see "Disciplinary Action" above). If you are authorized to participate in social media forums on behalf of the Company and have doubts about what you are about to publish, discuss them with your manager or contact the Corporate Communications Department.

11. ***Do not respond to media inquiries on behalf of the Company.*** If a member of the news media or a blogger contacts you about a posting that concerns the Company, do not attempt to answer or respond on behalf of the Company. Obtain the name of the person making the inquiry and immediately notify the Corporate Communications Department at (952) 903-1645. If you work at a retail banner, contact Communications.

This policy or any specific provision of this policy does not create a contract or guarantee a term and/or condition of employment between an employee and SUPERVALU. This policy is in effect as of the date noted below and supersedes any previous versions of the policy.

The policy applies to all employees except those who are subject to a collective bargaining agreement where a conflict to this policy exists. In such case, the collective bargaining agreement shall be followed as negotiated.

This policy replaces and supersedes prior policies and may be modified or deleted by SUPERVALU without prior notice.

# CONFLICTS OF INTEREST

**Purpose**

The Company is entitled to the best efforts and undivided loyalty of all employees. This requires that employees avoid situations that interfere with their ability to perform their job responsibilities in a proper manner or potentially conflict with the Company's interests.

The purpose of this policy is to identify those areas that may give rise to conflicts of interest for employees and what employees must do to avoid them.

**Policy**

You and your immediate family members (spouse, domestic partner, parents, children, brothers and sisters) must strive to avoid doing anything that creates a conflict of interest or the appearance thereof with your responsibilities to the Company. Generally, this means not engaging in activities that compete with the Company's businesses, have the potential to affect your objectivity and independence when acting on behalf of the Company, or allow you to personally gain from a relationship the Company may have with another party. To avoid conflicts of interest or even the appearance thereof:

- You must not engage in any outside business activity that competes with any of the Company's businesses;
- You must not provide services to a competitor, customer or supplier through any form of an employment or consulting arrangement;
- You must not engage in any outside business activity that is so substantial as to call into question your ability to devote appropriate time and attention to your job responsibilities;
- Neither you nor any member of your immediate family may use for personal gain or the benefit of others, confidential information obtained by you during your employment with the Company;
- You may not take advantage of or divert a business opportunity to yourself or any member of your immediate family that could be reasonably anticipated to benefit the Company or that the Company might have an interest in pursuing;
- Neither you nor any member of your immediate family may have a direct or indirect interest in any transaction or business arrangement to which the Company may be a party, including, without limitation, any ownership interest in:
  - Any retail store supplied by or affiliated with the Company;
  - Any customer, supplier or competitor of the Company, other than nominal amounts of stock in publicly traded or private companies not exceeding one-tenth of one percent (0.1%) of such company; or
  - Any real estate or other property leased by or to the Company;

  without the prior written approval of management (see section titled "Waivers" below).
- You must not be in a position of supervising, reviewing or having any influence on the job evaluation, pay or benefits of any immediate family member; and
- Neither you nor any member of your immediate family may sell anything to the Company or buy anything from the Company, without the prior written approval of management (see section titled "Waivers" below), except pursuant to store based consumer transactions or any normal program of disposal of surplus Company property that is offered to all employees in general.

Several additional areas that may also give rise to conflicts of interest include the acceptance of gifts and gratuities, the misuse of confidential information, and membership on certain boards and associations. These areas are addressed in separate policies within this Code.

**Reporting**

At the direction of the Company, you may be requested to complete a questionnaire to report the facts called for under this policy. Upon receipt of each report, a determination will be made as to whether it discloses any conflict of interest which violates this policy. If the Company determines that a conflict exists, or that you have failed to properly report a conflict, the Company may, in its sole discretion, take any one or more of the following actions:

- Waive the conflict;
- Require that you modify or dispose of the conflicting interest, or modify or terminate the conflicting relationship;
- Modify your employment duties or those of your immediate family member that is involved, if applicable, including salary and benefits if necessary; or
- Subject you to disciplinary action, up to and including termination, subject to applicable laws and regulations.

**Seek Advice**

If you suspect that any activity or situation you are involved in may constitute a conflict of interest or are unsure based on the facts or circumstances of a particular situation, contact your supervisor or the **Office of Ethics & Compliance at ethics.compliance@supervalu.com** for advice.

**Waivers**

Deviations from this policy are permitted only upon full disclosure to, and the prior written approval of:

- The Executive Vice President, Human Resources, or any Vice President, Human Resources to whom the Executive Vice President, Human Resources has delegated authority for such purpose, in consultation with the Chief Compliance Officer, in the case of employees; or
- The Board of Directors, in consultation with the General Counsel, in the case of Executive Officers (or the Board of Directors, in consultation with the Chief Compliance Officer, in the case of a waiver pertaining to the General Counsel).

# GIFT & ENTERTAINMENT POLICY

## Purpose

Every day our employees make business decisions regarding our vendors and service providers. These decisions must be based on what is best for the Company and its customers. Employees are expected to conduct themselves with integrity and maintain impartial relationships with our customers, vendors, suppliers, contractors, consultants, franchisees, licensees and other persons doing or seeking to do business with the Company ("Third Party Business Partners").

Meals and entertainment are occasionally appropriate tools for building goodwill and strengthening business relationships with suppliers and customers. However, accepting a meal or entertainment is unacceptable if it is given with the intent to influence you to make a business decision based on something other than service, quality or price. Remember, it is vital to avoid even the appearance of partiality or improper influence. As a result, employees may not accept business gifts, favors or benefits, including meals and entertainment, except in the limited circumstances as further described in this policy.

## Scope

This policy applies to all employees and to immediate family members (spouse, domestic partner, parents and children). Any gift or entertainment given to an employee's family member will be treated as a gift or entertainment given to the employee.

## Specific Situations

The following are common situations applying to this policy. In other situations, if your obligations are unclear, you should follow the procedures described in "Seek Advice" below.

### Gifts and Personal Benefit

Employees should never accept, request or solicit gifts, gratuities, favors or any form of personal benefit from Third Party Business Partners. Examples include:

- Bottle of wine, iPad, sporting/entertainment event tickets for an event the Third Party Business Partner does not attend;
- Cash or cash equivalents (including gift cards), loans, extensions of credit, commissions, shares of stock or stock options, or other forms of payment or financial consideration, regardless of amount;
- Services or labor that are provided at no cost or at prices that are less than their fair value, such as auto repairs or home improvements; and
- Personal travel accommodations, including aircraft or other forms of transportation, or lodging accommodations such as the use of a vacation property.

Promotional items (such as pens, coffee mugs, calendars, or t-shirts) that display the vendors' logo or name and have a value less than $50 may be accepted on an infrequent basis.

A gift that does not fall within the promotional item exception must be turned over to the Community Relations Department within Home Office Human Resources for donation to charity. If the gift is immediately perishable and impractical to donate to charity, it may be kept but must be shared with other employees. Employees should also notify the sender of this policy and discourage future gifts.

**Meals and Entertainment**

Employees may accept business entertainment (e.g. meals, round of golf, tickets to the theatre or a sporting event) offered for legitimate business purposes such as building goodwill and enhancing relationships with Third Party Business Partners provided that it complies with these requirements:

- Unsolicited
- Infrequent
- Valued at $75 or less. Pre-approval as set forth below is required if the value exceeds $75
- Reasonably related to a legitimate business purpose (e.g. accompanying a customer or supplier to a local theatre/sporting event or attending a business meal)
- In good taste and occurs at a business appropriate venue
- Attended by both the giver and recipient

**Business meetings**

Meetings should typically occur on Company premises. An exception applies to those parts of the Company where it is customary to meet with independent retailers and licensees at their stores (such as Wholesale and Save-A-Lot). Outside meetings with Third Party Business Partners should occur infrequently and should take place in reasonable and appropriate settings for the business at hand, such as touring a vendor's facility or meeting at an outside lawyer's office.

- **Off-site business meetings hosted by a Third Party Business Partner -** All costs associated with an employee traveling to or attending an off-site meeting hosted by a Third Party Business Provider (i.e. plant tour) must be paid by the employee and allowable expenses will be reimbursed pursuant to the Company Travel and Expense Policy provided appropriate approval to attend the meeting is obtained from the employee's manager.

  An exception allowing a Third Party Business Partner to pay for these costs will apply if there is a legitimate business purpose (i.e. conference or seminar), the event is an industry event not limited to just SUPERVALU employees and all attendees have received the same opportunity/benefit being provided to the employee. Participation in any such event must be approved in advance by a Corporate Senior Vice President or above or a Business Unit President. The employee may accept meals ancillary to the event that are provided to all attendees.

- **Off-site business meetings hosted by a Licensee or Independent Retailer** - There may be times that business meetings and social events hosted by licensees or Independent Retailers coincide with each other. Participation in such social events may be acceptable so long as prior approval is obtained. In the case of Save-A-Lot, approval should be obtained from the Chief Executive Officer. In the case of Wholesale, approval should be obtained from a Region President or the Executive Vice President of Wholesale.

**Contests/Prizes**

Employees attending an event sponsored by a Third Party Business Partner, such as a trade show, convention or charity event, may not participate in random drawings, contests or skill based events.

Employees attending an event sponsored by an industry organization, such as a trade show, convention or charity event, may participate in random drawings, contests or skill based events and accept a prize with a value of up to $200, provided that the random drawing, contest or skill based event is not sponsored by a Third Party Business Partner.

Store or Region level contests sponsored by Third Party Business Partners are permitted so long as the contest is pre-approved by Banner/Region Management and the value of the prize is reasonable.

**Product Samples**

Employees whose jobs require them to evaluate products may receive samples of products developed or promoted by outside parties as part of an evaluation process. Such samples should be used for evaluation purposes only and shared with other employees in quantities limited to the amount necessary for their evaluation and review. Samples should typically be consumed on Company premises and not at home. Once the evaluation process is complete, all unused samples should be returned (if practical), used for charitable purposes, or destroyed. No excess samples may be used for an employee's personal use.

**Company Meetings and Events**

Meetings and events should be conducted and funded without contributions from Third Party Business Partners whether monetary or otherwise (such as donated products, merchandise, or volunteer workers) unless approved by an Executive Vice President. Third Party Business Partners may be invited to attend certain Company meetings and may be asked to pay the proportionate cost of their participation. Modest product samples from Third Party Business Partners for immediate consumption may be accepted by employees.

**Charitable Donations**

- *Events Sponsored by the Company*. Funding or other support, whether monetary or otherwise (e.g., donation of products or merchandise, promotional efforts, or the use of employee resources including volunteers) may not be solicited or obtained from Third Party Business Partners for Company sponsored events unless approved by an Executive Vice President.
- *Events Sponsored by Third Party Business Partners.* At the request of a business partner, Company resources, in monetary form or otherwise (e.g., donation of products or merchandise, promotional efforts, or the use of employee resources including volunteers) may be contributed to charitable or political activities or events sponsored by business partners if the contribution is approved in advance by an Executive Vice President.

**Reporting and Approval Required**

The Company's Gift & Entertainment Reporting System ("GERS") must be used to seek approval of items. Employees must get pre-approval from their manager for any meals or entertainment which has a value in excess of $75. Any meals or entertainment valued at more than $250 must be pre-approved by an Executive Vice President.

Approval should be granted only if the meal or entertainment is unsolicited, infrequent and there is a clear business benefit.

**Seek Advice**

When questions or doubts arise about how to interpret this policy, you should seek advice in writing and in advance by contacting your immediate supervisor who will involve the Executive Vice President for your group if needed or to seek an exception or you may contact the **Office of Ethics & Compliance at: ethics.compliance@supervalu.com**, or **(952) 828-4159 or (952) 828-4230.**

**Exceptions**

Exceptions to this policy may only be made in advance and in writing by an Executive Vice President in consultation with the Vice President of Compliance. No exception may be granted unless there is a clear business benefit, no favoritism or appearance of favoritism and the spirit of this policy against accepting anything of value is not violated.

# FOOD & DRUG LAWS

## Purpose

The Company is committed to ensuring that its retail and shopping customers are offered safe food and making every effort to comply with all applicable food and drug laws of the United States and the countries to which it delivers goods. It is imperative that employees follow all statutes and regulations governing the safe shipping of food, the sale of specific types of food, the advertising or labeling of food items, food quality and food safety.

## Policy

Under no circumstances should you knowingly engage in the sale or distribution of any food or drug item that is contaminated or mislabeled. In addition, you should not knowingly market or sell any drug that has not received approval from the federal Food and Drug Administration.

You are required to report to your management knowledge of products that do not comply with applicable food and drug regulations, as well as violations of food safety standards, suspected tampering, or other suspicious activity.

Specific policies relating to the handling and preparation of food items, as well as the handling and dispensing of drugs have been adopted by the Company. These policies apply to those employees who work in areas where such tasks are performed and are available from their supervisors or representatives within their local Human Resources Department. If you work in an area that involves the handling or preparation of food items or the dispensing of drugs, you are expected to be aware of such polices and to fully understand and comply with them.

## Seek Advice

Whenever questions arise regarding the safety, handling, labeling or shipment of any food or drug item, or the applicability of any food or drug law, please consult with your supervisor or manager, or contact the: **Director of Regulatory and Compliance at: (952) 828-4150** for advice.

# ENVIRONMENT

## Purpose

The Company is committed to protecting and promoting the health and well being of the environment. This means operating its stores and distribution facilities in compliance with pertinent environmental regulations, minimizing environmental risk within its portfolio of properties, and embracing a culture of sustainable operations.

## Policy

It is the Company's objective to conserve natural resources and manage its business in ways that are sensitive to the environment. To achieve this objective, the Company will strive to comply with all applicable environmental laws as well as internally established environmental requirements.

Any written complaints, concerns, ideas and/or inquiries from employees, customers or regulatory agencies (e.g., the Environmental Protection Agency), whether formal or informal, must be reported immediately to the **Environmental Affairs Department at: (208) 395-4794**. Employees should also use these contact numbers if there are any questions regarding proper handling of hazardous or other potential environmentally sensitive materials.

# CORPORATE HIPAA POLICY
## GENERAL USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

**Purpose**

The purpose of this policy is to establish the Company's expectations of all employees regarding the use and disclosure of protected health information ("PHI") gathered or maintained by the Company as an affiliated covered entity under the Health Insurance Portability and Accountability Act ("HIPAA").

**Policy**

You should use and disclose PHI only as specifically permitted or required by the HIPAA privacy or security rules, or any more restrictive state law, and in accordance with Company policies and procedures.

**Procedural Implementation**

***PHI Access.*** The Company operates as an affiliated covered entity under HIPAA. This means that you may come in contact with or have reason to have access to PHI as part of your responsibilities. Therefore, you must complete HIPAA training appropriate to your position with the Company relative to the potential level and frequency of your access to PHI. Also, you are responsible for protecting all PHI to which you have access, that is gathered or maintained by the Company, and for consistently incorporating reasonable safeguards and applying the minimum necessary standard, as explained below, when handling or requesting PHI. These standards must also be applied to decisions related to allowing other employees access to Company data and systems containing PHI.

***Basic Rule for Use and Disclosure of PHI.*** PHI may not be used or disclosed unless permitted or required by the HIPAA privacy or security rules, as explained below. Guidance on HIPAA compliance may be obtained from a member of the Privacy Office/Legal Department staff by calling the:

**HIPAA Hotline**

**(208) 395-4455**

***Permitted Uses and Disclosures.*** The HIPAA privacy rule permits the use and disclosure of PHI under the following circumstances:

- Disclosures to the patient;
- Uses or disclosures necessary to carry out treatment, payment, or health care operations;
- Uses or disclosures pursuant to, and in compliance with, a valid patient authorization; or
- Disclosures covered under the HIPAA "national priority" exceptions, such as disclosures required by law.

***Required Disclosures.*** The HIPAA privacy rule requires the disclosure of PHI in only two instances:

- When the patient requests access to their own PHI; and
- When the Department of Health and Human Services ("HHS") requests information to investigate or determine HIPAA compliance.

***Incidental Disclosures.*** Incidental disclosures are those that are "incidental to" a permitted use or disclosure, and are not considered a HIPAA violation so long as it can be demonstrated that "reasonable safeguards" and the "minimum necessary" standard (explained below) were consistently applied.

***Reasonable Safeguards.*** Reasonable safeguards are the physical and procedural precautions taken to avoid PHI disclosure to, or use by, unauthorized individuals. HIPAA does not grant patients a total right of privacy over their PHI, but does support a "reasonable expectation of privacy" by requiring that covered entities adopt appropriate reasonable safeguards to guard against unauthorized uses and disclosures.

***"Minimum Necessary" Standard.*** When using, disclosing, or requesting PHI, reasonable effort must be made to limit the use or disclosure to the minimum information necessary to accomplish the intended purpose. Certain exceptions, as outlined below, apply. HIPAA places the burden for compliance with this standard on both the requesting and the disclosing parties.

- Exceptions. The minimum necessary standard does not apply to the following:
  - Uses and disclosures for treatment purposes;
  - Disclosures to the patient who is the subject of the information;
  - Uses or disclosures made pursuant to a valid patient authorization;
  - Disclosures to HHS when requested by HHS for compliance and enforcement purposes; and
  - Uses or disclosures that are otherwise required by law.
- Reasonable Reliance. HIPAA allows for reasonable reliance on a requesting party's representation that they have limited a request for PHI to the minimum necessary to achieve the stated purpose.

**To Report Violations or Seek Advice**

To report HIPAA complaints or violations, or for advice or guidance on HIPAA compliance, call the:

**HIPAA Hotline**
**(208) 395-4455**

Violations may also be reported through the Company's Employee Hotline at: **1 (800) 841-6371**.

**Enforcement**

Failure to follow this policy may subject you to disciplinary action, up to and including immediate termination from employment, subject to applicable laws and regulations.

# EQUAL EMPLOYMENT OPPORTUNITY AND HARASSMENT

## Purpose

The Company recruits and hires diverse individuals whose qualifications, abilities and interests most closely match our current employment needs. It is also committed to providing a work environment free of discrimination and harassment.

The purpose of this policy is to set forth the Company's expectations regarding behavior of employees when interacting with other employees and the Company's customers and business partners.

## Policy

The Company is committed to providing equal employment opportunity for all individuals and following employment practices designed to prevent illegal discrimination. This means that it will strive to hire and promote individuals and to administer all human resources actions without regard to race, color, creed, religion, national origin, sex, gender identity, sexual orientation, disabilities of otherwise qualified individuals, age, marital status, familial status, status relating to public assistance, genetic information, and other characteristics as required by law. It is also the Company's policy to provide a work environment that is free from any form of illegal harassment.

Harassment is unwelcome behavior based on a legally protected characteristic, including, but not limited to, verbal or physical conduct that creates a hostile or intimidating environment or interferes with an individual's work performance, employment opportunities or other privileges of employment. Sexual harassment includes unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature. Illegal harassment can be based upon conduct by a co-worker, temporary employee, contractor, supervisor, vendor, customer or supplier. Examples of such behavior include:

- Telling jokes that are racist, sexist or otherwise offensive due to national origin or disability;
- Making offensive, derogatory or degrading remarks about gender, race, ancestry, religion, national origin, age, sexual orientation or disability;
- Sending offensive or derogatory e-mail or text messages;
- Unwanted physical contact, advances or propositions;
- Unwanted staring or leering;
- The display of sexually suggestive objects or pictures; and
- Any other behavior that creates a hostile or intimidating work environment.

To comply with the Company's commitment to equal employment opportunity and policies against discrimination and harassment, you should not discriminate against any employee, customer or employee of any business partner of the Company on the basis of a legally protected characteristic, including but not limited to their race, color, creed, religion, national origin, sex, gender identity, sexual orientation, disability, age, marital status, familial status, veteran status, or status relating to public assistance. When making employment related decisions regarding individuals or groups of persons, these factors cannot be taken into account.

You are also expected to refrain from engaging in any activity that constitutes harassment based on a legally protected characteristic of employees, independent contractors, or any person with whom the Company does business.

You should report any inappropriate or harassing behavior, whether it is directed at you or any other employee, to your immediate supervisor, a higher level of management in your organization or your local Human Resources Department. If you are uncomfortable with those approaches and/or wish to remain anonymous, please **call the Company's toll-free Employee Hotline at:**

**1 (800) 841-6371**

**Protection from Retaliation**

Employees who report good faith concerns under this policy or participate in good faith in an investigation of a concern under this policy are protected from retaliation. If you are concerned that you have been retaliated against in violation of this policy, please report your concern in one of the ways identified in the preceding paragraphs of this policy.

# THREATS AND VIOLENCE FREE WORKPLACE

**Purpose**

The Company is committed to providing each employee a work environment that is safe, secure and free of threats, intimidation and violence.

**Objective**

The objective of this policy is to provide directions for all employees to ensure a workplace intended to protect employees and customers, their belongings and company property.

**Policy**

Any behavior or action that threatens another person's safety, or property, or causes them to perceive their safety or property is threatened, will be thoroughly investigated and if confirmed, will not be tolerated.

Any employee who, for any reason, says or does something to threaten another person's safety or property will be subject to disciplinary action up to and including discharge. Violations of this policy may result in immediate termination of employment without prior warnings.

This policy applies to all statements and acts, even those that are not intended to be harmful, or are intended as jokes or horseplay. This policy also applies to comments or acts that are directed at persons other than SUPERVALU employees.

It is every employee's responsibility to immediately report any situation that could result in harm to themselves or anyone in the workplace. Any employee who may witness or become aware of troubling persons or situations that may cause serious anxiety, stress or fear should immediately report such situations to their supervisor or Human Resources/Associate Relations representative.

Employees who feel they have been the victim of a violent act, the threat of a violent act, or suspect that such an act might occur, have the responsibility to report the matter immediately to their supervisor or a Human Resources/Associate Relations representative. In addition, if an employee has knowledge of a circumstance in their personal life that could result in an act of violence at work, they are required to report it.

Employees may report their concerns through the **Company's toll-free Employee Hotline at:**
**1 (800) 841-6371.**

# FIREARMS AND WEAPONS FREE WORKPLACE

**Purpose**:

The Company is committed to providing each employee a work environment that is safe, secure and free of firearms and weapons.

For purposes of this policy, a weapon is considered to be any device that is designed to or traditionally used to inflict harm. This includes, but is not limited to: 1) firearms, switchblades, daggers, hunting knives, clubs, etc.; and 2) any object that could be reasonably construed as a weapon.

Company property includes company-owned or leased vehicles, Company-owned or leased parking areas and Company-owned or leased buildings.

**Objective**:

The objective of this policy is to provide clear direction for managers and employees regarding the prohibition of firearms and weapons at all Company locations.

**Policy**:

It is prohibited to possess firearms, weapons or explosives on Company property, at off-site Company functions, and while conducting Company business, to the extent permissible by law, without explicit, written authorization by the Company. This prohibition applies to Company employees, vendors, contractors, and suppliers. This prohibition also applies to visitors to Company non-retail locations, such as store support centers, distribution centers, and corporate offices.

Any Company employee, vendor, contractor, supplier or visitor suspected of violating this policy may be subject to search to the extent permissible by law, including the search of any vehicle located on Company-owned/leased premises.

Employees must report violations of this policy immediately to their supervisor, a human resources representative, Company security or when appropriate, law enforcement personnel. Employees can report violations of this policy by contacting Company's toll free **Employee Hotline (1 (800) 841-6371)**. Employee Hotline reports can be made anonymously. Retaliation for reporting violations of this policy is expressly prohibited.

Employees who violate this policy may be subject to discipline, up to and including termination of employment.

# DRUG FREE WORKPLACE

## Purpose

It is the Company's goal to provide a work environment free of the negative effects of drug and alcohol abuse. The presence of these substances may lead to increased accidents and medical claims, deteriorates the health of employees, interferes with their lives and inhibits the safety of the Company's workplace. This policy sets forth the prohibitions against the possession or use of drugs or alcohol in the Company's workplace or while conducting Company business.

## Policy

It is against the Company's policy for you to possess, manufacture, distribute, sell or be under the influence of illicit drugs on Company property, while on Company business or during working hours. Further, you must report convictions of any criminal drug or alcohol statute to your supervisor or your local Human Resources Department. Unauthorized use of alcohol, possession of alcohol or being "under the influence" of alcohol on Company property, while on Company business or during working hours, is also prohibited.

Prescription drugs or over the counter drugs must be taken in accordance with the physician's and manufacturer's instructions. If you are in a safety sensitive position you must notify your supervisor of medications you are required to take to ensure that workplace and employee safety are not compromised.

Early recognition and treatment of chemical dependency or its symptoms are critical to successful rehabilitation and to the minimization of business, personal, family and social disruption. If you are experiencing problems of this nature, you are strongly encouraged to use the Company's **Employee Assistance Program**. Please contact your local Human Resources Department for more information regarding this service.

# MEMBERSHIP ON BOARDS OF DIRECTORS, PUBLIC COMMISSIONS AND TRADE ASSOCIATIONS

## Purpose

Outside directorships or memberships on the governing bodies of companies, public commissions or trade employees must be closely monitored so that the possibility of any conflict of interest or violation of the federal antitrust laws can be evaluated. This policy sets forth the procedures you must follow before accepting a position on the board of directors or governing body of, any corporation, public commission or trade association.

## Policy

Prior to agreeing to serve as a director, trustee, partner or employee, with or without compensation, of any corporation, partnership or the governing body of any public commission or trade association, you must obtain the clearance of the Chief Compliance Officer or the Vice President, Legal to ensure that your acceptance of such position will not create a conflict of interest with your duties as an employee of the Company or violate the provisions of any antitrust laws. You may contact the:

**Chief Compliance Officer at: (952) 828-4159.**

In addition, if you are an officer of the Company, prior to accepting a position on the board of directors of a for-profit corporation, you must first obtain the approval of the Chief Executive Officer. If the Chief Executive Officer is offered such a position, he or she must first obtain the approval of the Company's Board of Directors before accepting the position.

All existing directorships, trusteeships, partnerships or employment relationships (except in not-for-profit corporations or other charitable institutions without compensation) must be reported to the Company.

These provisions do not pertain to memberships on the boards of non-profit entities engaged in businesses that are unrelated to the business of the Company.

# ANTITRUST LAWS & FAIR TRADE PRACTICES, COMMUNICATIONS WITH COMPETITIORS, AND ATTENDANCE AT TRADE ASOCIATION MEETINGS

## Purpose

Federal and state antitrust laws generally forbid all agreements or implied understandings between competitors to fix or manipulate the price at which they sell products or services to others, or to allocate territories or customers for the sale of products or services. Other federal and state laws prohibit the use of unfair business practices when conducting business. The purpose of this policy is to identify certain activities that may violate these laws and steps that may be taken to minimize possible violations.

## Scope

This policy applies to all employees and persons engaged by the Company to provide services.

## Policy

All employees and persons acting on behalf of the Company must strictly adhere to federal and state antitrust laws as well as those pertaining to fair trade practices, both domestically and internationally. Various activities prohibited by such laws include:

- Imposing restrictions as to whom, where or at what price customers may resell products;
- Bid rigging or collusion;
- Agreeing with a competitor(s) to allocate customers or markets;
- Agreeing with a competitor(s) to boycott suppliers or customers;
- Disparaging competitors;
- Making false or misleading statements regarding products or services;
- Stealing trade secrets or misappropriating confidential information; and
- Providing and/or accepting bribes or kickbacks.

These shorthand descriptions are intended to suggest possible problem areas. The laws applicable to this area reach informal and oral arrangements or understandings, as well as those set forth in writing. You should refrain from engaging in any of the types of conduct listed above.

### *Communications with Competitors*

Particular attention must be paid to communications with competitors. The following types of communications with a competitor may raise serious antitrust implications and are expressly prohibited:

- Communications regarding the terms under which goods will be sold to customers, including not only the price at which such goods may be sold, but also other issues that affect the wholesale cost of goods, overhead, or retail prices (e.g., delivery charges, finance charges, couponing and advertising plans, discounts, credit terms, shipping and/or inventory allowances, and shelf space payments/slotting allowances);
- Communications regarding the allocation (or splitting or sharing) of markets or customers;
- Communications regarding the treatment of vendors in any manner, or boycotting a vendor;
- Communications relating to price fixing;
- Communications regarding a specific vendor or customer (except those between Company pharmacists and pharmacists employed by competitors as permitted or mandated by law); and
- Communications regarding service aspects (e.g., appropriate holiday hours for stores).

Prohibited communications may take many forms including but not limited to, meetings, brief encounters, chance meetings that are not intended (e.g. "I ran into them on the street"), social occasions, telephone

conversations, emails, faxes, and written correspondence. If any of the communications described above occur, disclose them immediately to the **Legal Department by calling (952) 828-4230.**

You are cautioned to avoid even seemingly innocent contacts with competitors on the topics described above and to leave any area in which such discussions take place, whether at trade association meetings or otherwise. There must be a specific, legitimate purpose for each contact with a competitor.

The types of conduct discussed above do not cover every potential antitrust or anti-competitive violation. In some instances, some of the conduct discussed above is legal; for instance, contact with competitors is appropriate for the purpose of collective bargaining. You must consult with the Legal Department if there is a question about a contact with a competitor.

### *Anti-bribery*

The United States (through the Foreign Corrupt Practices Act ("FCPA")) and many foreign governments, through their respective anti-bribery laws, make it illegal to offer or provide, directly or through a 3rd party, anything of value to a foreign government official in order to influence an act or decision to obtain, retain and/or direct business or to secure an improper advantage of any kind.
The Company strictly prohibits all Employees from giving, offering, promising or paying anything of value to government officials directly or indirectly with the purpose of obtaining or retaining business or otherwise securing an improper advantage. All Employees must take reasonable steps to ensure that business partners and other third-parties understand that the Company expects them to act with the same level of honesty and integrity in any activity engaged in for or on behalf of the Company.
The FCPA contains an exception for "facilitation payments", which are small amounts paid to secure the performance of routine government actions. No facilitation payments may be made by anyone in the Company without prior written approval from the Chief Compliance Officer.

### *Attendance at Trade Association Meetings*

Because it is unlawful to enter into certain types of agreements with competitors, communications or meetings with competitors are risky, even if no prohibited topics are discussed and even if no agreement is contemplated. To protect against the risk that innocent, permissible conversations or meetings will be misinterpreted; the Company requires that all employees follow these rules:

- Get advance approval from your supervisor before contacting a competitor, joining a trade association or attending a meeting where competitors will be present; *
- Attend meetings with competitors only where (i) an agenda, schedule, announcement, or letter describing the purpose of the meeting is distributed in advance and followed during the meeting, and (ii) the meeting is sponsored or arranged by a trade association or similar entity (where possible, it is suggested that the trade association's attorney attend the meeting); and
- If a discussion about a prohibited topic begins, refuse to participate, end the discussion immediately, excuse yourself and report the incident to the Legal Department as soon as possible.

There may be situations that do not meet the requirements above where a meeting with competitors is lawful and appropriate. For example, if the Company and a competitor are both defendants in a lawsuit, it is lawful and helpful to meet, even though no trade association arranged the meeting. If you want to meet with a competitor in situations where these requirements are not met, or if you want more information, contact **the Legal Department/Office of Ethics & Compliance at: (952) 828-4230 or ethics.compliance@supervalu.com.**

*Before joining the governing body of any trade association, you must obtain management approval in accordance with the Company's policy titled "Membership on Boards of Directors, Public Commissions and Trade Associations" that appears in this Code of Business Conduct.

# INFORMATION SECURITY

## Purpose

The purpose of this policy is to set forth certain IT practices that are to be followed to protect Company Information. Protecting information is the responsibility of every employee, consultant or third-party representative who has access to Company Information. It is therefore imperative that every individual be aware of what actions are required to ensure Company Information assets are adequately protected. This obligation continues after the termination of an individual's employment, contractual arrangement or any authorization to use or access Company Information or the company's electronic communications systems, regardless of reason. The intent of this policy is to preserve and protect the investment in information and to:

- Ensure confidentiality, integrity and availability
- Prevent unauthorized use/disclosure for commercial or malicious purposes
- Foster compliance and ensure operational procedures exist for specific legal regulations such as Payment Card Industry (PCI) Security Standards, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX) and industry standards relating to data privacy and information security
- Reduce the risk of loss by accidental or intentional means
- Preserve SUPERVALU's rights in the event of such a loss

The term "Company Information" refers to all information relating to the Company's businesses or operations that is processed, generated, maintained, transmitted or stored in electronic or paper format, through the use of the Company's electronic communications systems (computer and telecommunications systems) or otherwise. For purposes of this policy, the term "Company Information" should be interpreted broadly which includes examples such as: Financial Data, Marketing Analysis, Acquisitions/Dispositions, Business/Product strategies, Data Configurations, Security Procedures, System Operations, Customer and Vendor pricing, Customer Personal Information, Employee Personal Information, etc.

## Scope

This Policy applies to all Company employees, contractors, vendors and other persons who have access to Company Information or the Company's electronic communications systems. It supersedes all previous versions of Company policies related to this topic including those at any location, banner or regional level.
All individuals or entities using company information, connecting to its network or other IT infrastructure will be responsible for adherence to the IT Policy.

## Policy Statement

Company information and systems are to be used to support business processes and functions. All persons subject to this policy are responsible for safeguarding and protecting Company Information within their possession and control against unauthorized access, disclosure, transfer, reproduction, misappropriation, misuse, modification, or destruction throughout its life cycle, from origination to destruction, in a manner commensurate with its classification. This applies regardless of where such Company Information resides, what form it takes (electronic or paper), or what technology is used. These obligations continue even after the termination of a person's employment, contractual arrangement, or any authorization to use or access Company Information or the Company's electronic communications systems, regardless of the reason.

Compliance with the IT Policy will be monitored and enforced. Misappropriation or unapproved disbursement of company information will not be tolerated and may be subject to disciplinary action, up to and including termination.

The Chief Information Security Officer (CISO) is responsible for the Company's information security including overseeing the development, monitoring and communication of security policies, standards and procedures. The Security, Governance, Risk and Compliance team is responsible for the actual maintenance of the IT Policy, which will be communicated to employees, consultants, banners, and business partners. Any new or modified standards will be communicated to the impacted individuals and groups as deemed necessary.

The Security, Governance, Risk and Compliance team is responsible for facilitating the development and approval of a comprehensive suite of IT Standards which will be risk-based, devised to support business processes, and meet our regulatory requirements. These standards define the minimum set of controls that must be followed.

The IT Policy will be reviewed and approved annually by the CIO. The appropriate Technical Services VPs will approve new standards as well as any modifications to the existing standards.

Exceptions to this policy require the written approval from the CISO. Refer to the Exception Management Standard for requirements for an exception.

**Internal and External Audit**

The Company's Internal Audit Department is responsible for independently testing compliance with the Company's IT Policy, Standards and Procedures, and reporting to the Company's executive management on the adequacy of information security controls.

At the direction of the Company, or when required to affirm compliance with any industry standards, such as those established by the Payment Card Industry (PCI) or Sarbanes Oxley (SOX), an independent external accounting firm will be engaged for such purpose.

**Policy Interpretations or Questions**

Questions regarding this policy or any interpretation of the provisions or any other policy or standard referenced should be referred to the Security, Governance, Risk and Compliance team by contacting: IT.Compliance@supervalu.com.

**Roles and Responsibilities**

Ownership of this policy resides with the Security, Governance, Risk and Compliance Team. This Policy applies to all Company employees, contractors, vendors and other persons who have access to Company Information or the Company's electronic communications systems. It supersedes all previous versions of Company policies related to this topic including those at any location, banner or regional level. Any employee found to have violated the SUPERVALU IT policy will be subject to disciplinary action, up to and including termination of their employment. Any consultant, vendor or business partner found to have violated SUPERVALU IT Policy may be subject to action, up to and including termination of their contract. SUPERVALU reserves the right to seek any legal recourse to protect and defend its information assets.

# ELECTRONIC COMMUNICATIONS

## Purpose

One of the Company's essential business tools is its electronic communication systems. These systems include, but are not limited to, electronic mail, Internet messaging, text messaging, Internet browsing, Company-run networks, network services, facsimile services, modems, file transfers, electronic data interchange, audio and video teleconferencing, voice mail, telephone systems and wireless technologies such as Company owned iPads and cellular phones.

The purpose of this Policy is to ensure that the Company's electronic communication systems are used only for lawful purposes related to the efficient operation of its business and in an appropriate manner so as to minimize risks to the Company's information, equipment, and systems.

## Policy

### *Usage*

The Company's electronic communication systems are intended primarily for use in connection with the Company's business. The Company permits occasional personal use of its email, telephone, facsimile and Internet systems; however, employees should understand that personal use (i) must not in any way interfere with or impede the Company's business, (ii) must not interfere with an employee's job performance, (iii) must be occasional and minor, (iv) must be promptly discontinued at the request of Company management, and (v) is expressly subject to all of the provisions in this policy and other applicable Company policies and guidelines.

You are responsible for ensuring that the Company's electronic communications systems are not used for any unethical, illegal or improper purpose and will be held accountable for any misuse. The Company's systems should not be used to: (i) create or transmit disruptive messages such as chain letters or jokes, or messages containing sexual implications, racial slurs or other comments that offensively address a person's age, sex, gender identity, sexual orientation, religious or political beliefs, national origin, disability or other characteristics; (ii) solicit or persuade for commercial ventures, religious or political causes, or other matters unrelated to the Company's business; or (iii) disseminate or intentionally access material that could be defamatory, sexually oriented, pornographic, harassing, threatening, illegal, fraudulent, offensive or unwelcome to anyone who may view it.

### *Security*

You must take appropriate care to safeguard the security and integrity of the Company's electronic communications systems and not deliberately interfere with the Company's access to data stored on the systems or deliberately circumvent the Company's security procedures. You are also prohibited from using the Company's electronic communications systems in any manner that creates an unreasonable risk of permitting unauthorized outside access to the systems or in a manner that compromises the security and integrity of the Company's network, such as allowing intruders or viruses into the network.

You must not intentionally develop, download or use software that: (i) identifies or bypasses computer system security mechanisms, (ii) discloses passwords or enables unauthorized access to information, (iii) is designed to replicate itself or attach itself to other programs (e.g. viruses, worms) whether or not it has any malicious intent, (iv) is designed to get around software licensing or copyright restrictions, (v) attempts to or actually does consume all of a computer systems resources (e.g. memory, disk space, processing queues, bandwidth), (vi) harasses other computer system users, or (vii) is not consistent with a vendor's license.

If you wish to download any documents, files or software from non-Company sources you must observe the Company's procedures for virus checking and system security. Persons not employed by the Company may not be given access to, and are not permitted to use the Company's systems unless such access or use has been approved in advance, in writing by the Technical Services Department. If access or use is approved, such persons (including contractors and temporary employees) will be subject to this policy.

***Unauthorized Copying***

The Company's electronic communications systems may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary information or similar materials without proper authorization. Use of the Company's systems for unauthorized copying of copyrighted software or content is expressly prohibited.

**Privacy/Monitoring**

You should have no expectation of privacy when using the Company's electronic communications systems and you are expected to follow the Company's Electronic Mail Standards, which are available from the Technical Services Department. The Company reserves and intends to exercise the right to monitor, review, electronically scan, audit, intercept, access and disclose all electronic communications and data that are created, sent, received, stored and/or accessed using its systems, and does from time to time examine the content of electronic communications. The source of any e-mail message is clearly identifiable and the message may remain part of the Company's business records long after it has supposedly been deleted. Notwithstanding the Company's right to retrieve and read electronic communications, such communications should be treated as confidential. You are not authorized to retrieve, read or listen to any electronic message unless you are its intended recipient.

All electronic communications and data created, sent, received, stored and/or accessed by you during your employment by the Company, or which relates in any way to your employment by the Company, is the property of the Company (whether such data is stored or accessed using Company provided electronic communications systems, maintained in hard copy, or stored electronically on systems not belonging to the Company).

**Seek Advice**

The Company's Technical Services has developed additional policies regarding internet usage, electronic mail standards and information security. If you wish to obtain copies of such policies, or if you have questions regarding this policy, contact the Technical Services Department at IT.Compliance@supervalu.com.

# SOFTWARE PROTECTION

**Purpose**

Software is an important asset that is developed or acquired by the Company for business use. It is important to respect the ownership rights of the authors of such software and to refrain from using it in any manner that violates intellectual property ownership rights.

This policy sets forth the Company's standards relating to the use and ownership of software developed or acquired by the Company.

**Policy**

All employees have an obligation to protect and manage software that is developed by the Company or obtained from third parties, that is entrusted to them or to which they have access. This includes any intellectual property rights (copyrights, patents and trade secrets) associated with such software.

The term "software" includes not only the programs, routines and procedures that cause a computer system to perform a predetermined function(s), but also supporting documentation such as algorithms, flow charts, diagrams, specifications, diagnostic and testing materials, and operating or maintenance manuals.

All software that is developed by an employee or independent contractor using Company time or resources is Company property. If you develop software, you must ensure that the appropriate intellectual property rights in such software are obtained and secured for the Company, whether it is to be used inside the Company or marketed externally. This may be accomplished by contacting the **Legal Department at: (952) 828-4230** for guidance.

You are prohibited from using unlicensed software or creating or using unauthorized copies of software. If you are acquiring software from a third party or have been provided software that the Company has purchased or licensed from a third party, you must ensure that it is obtained or used in compliance with applicable copyright laws as well as any contractual obligations assumed by the Company. Such provisions may restrict the manner in which such software is used, the extent of its usage or the number of copies of such software that can be made.

All software, whether developed or acquired, must be identified, accounted for, controlled, documented, priced and classified for security purposes by the business unit that develops or acquires it.

If you have questions concerning software protection, acquisition or distribution, please contact the **Legal Department at: (952) 828-4230.**

# INTERNATIONAL BUSINESS AND OPERATIONS

**Purpose**

The Company is committed to applying uniformly high standards of ethics and business conduct in every country in which it operates, and in every business relationship or affiliation it has worldwide, and of course, in compliance with the law. When conducting business outside the United States, the Company will be guided both by the laws and regulations of the United States and the laws and regulations of the countries within which it does business. In some circumstances that will mean that the Company is subject to different rules and will have to do business somewhat differently from country to country. Additionally, laws may be in conflict and therefore, in such circumstances, legal advice must be sought.

There are many United States laws and regulations that apply to activities outside the boundaries of the United States. For example, the Foreign Corrupt Practices Act prohibits U.S. companies from making improper payments or gifts to foreign government officials, politicians or political parties. In addition, the United States prohibits companies from doing business with certain countries and entities. While the details of each such trade embargo may differ, U.S. companies may not directly or indirectly export or import goods, technology, or services to or from embargoed countries. Similarly, financial transactions with embargoed countries and all dealings with citizens of such countries are generally prohibited. The list of countries and entities covered changes periodically, as do the details of the embargo for each country.

**Policy**

You may not be familiar with the laws or regulations of the United States or other countries that apply when conducting business on behalf of the Company outside of the boundaries of the United States. Therefore, when such a situation arises, you should always seek the advice of legal counsel to ensure that you comply with and do not violate the laws of the United States or any other country.

Before conducting business outside of the United States, seek advice by contacting the **Legal Department at: (952) 828-4230.**

# GOVERNMENT INVESTIGATIONS

**Purpose**

It is the Company's policy to cooperate with government investigations and give government investigators the full measure of assistance to which they are entitled, consistent with the safeguards that the law has established for the benefit of persons under investigation. Notwithstanding, such persons should have the opportunity to be adequately represented in such investigations by legal counsel.

This policy sets forth the standards you should follow if you are contacted by a government investigator or law enforcement official.

**Policy**

Generally, if a government investigator or agency contacts you seeking information or access to the Company's records or facilities, politely inform the investigator or agency that the Company's policy is generally one of cooperation, but that you must obtain clearance from the Legal Department before furnishing such information or access, unless management has established written policies relating to the agency and type of inspection that is being requested (e.g. OSHA). Exceptions to this policy may exist for certain groups of employees, such as those in the Company's distribution facilities, who may allow government inspectors to review routine records (receiving and shipping documents) without obtaining permission from the Legal Department. Check with your supervisor to see if there are any specific requirements applicable to your area.

If you are approached at home or at work by a government regulatory official or law enforcement officer investigating the Company, its operations or business practices, you can insist that any interview take place at your office or another location away from your home. You should also know that no government official or law enforcement officer can require you to give information without the opportunity to consult with an attorney in the Legal Department or with your personal legal counsel.

Under no circumstances should you lie or make any misleading statements to any government investigator or law enforcement official, attempt or cause any other Company employee or any other person to fail to provide information to any government investigator, or provide any false or misleading information.

If you obtain information that would lead you to believe that a government investigation is underway or if you are contacted by any government regulatory or law enforcement official regarding the Company, please contact the **Legal Department at: (952) 828-4230** immediately.

# IMPORTANT REMINDERS

**Compliance**

Full compliance with the policies set forth in this Code of Business Conduct is both expected and required. You are expected to read and understand this Code, including any future published updates.

**Violations May Result in Disciplinary Action**

If you violate this Code or any other Company policy, or engage in unethical or illegal conduct, you may be subject to disciplinary action up to and including termination, subject to applicable laws and regulations.

Employees who deliberately withhold information concerning another employee's violation of this Code, other Company policies, or engagement in unethical or illegal conduct may also be subject to disciplinary action.

**Acknowledgement**

You are required, upon request, to provide written acknowledgement of your awareness of and compliance with the provisions of this Code.

**Reporting Violations**

You are required to report actual or suspected violations of this Code or other unethical or illegal conduct. Matters should be reported using one of the following procedures:

- Contact your immediate supervisor.
- If you are not comfortable contacting your immediate supervisor to report the matter, or believe he or she did not handle it properly after it was reported, contact your local Human Resources Department or a higher level of management within your organization.
- **If you are not comfortable with either approach or want to remain anonymous, call the Company's toll-free**

## EMPLOYEE HOTLINE

## at

## 1 (800) 841-6371

Calls to the Employee Hotline are confidential and you may remain anonymous if you wish. Your call will be promptly investigated and appropriate action will be taken as necessary.

***Non-Retaliation***

It is strictly against the Company's policy for anyone to be subjected to retaliation for reporting in good faith to the Company or any legal or regulatory authority, a suspected violation of any provision of this Code, any Company policy, or any law or regulation. If you feel that you have been retaliated against in violation of this policy, please follow the procedures for reporting suspected violations above.