



Code of Conduct

"Integrity Always" is one of our core values – a value that requires us **to do the right thing – always.**

It means that we have to be **fair and honest** in all our dealings with our co-workers, customers, business partners, shareholders, competitors and the communities in which we live and work.

Failure to act with integrity will cost us dearly, in terms of loss of image and reputation, and ultimately, performance.

The reputation we enjoy today is the legacy of generations of associates who have worked to build our Company and make our red star an emblem of integrity. But, as we all know, a good reputation is a fragile thing – while it takes years to build, it may be destroyed overnight by just one unethical, thoughtless or misguided action.

Since our Company's image and reputation are a reflection of what each one of us says or does, we must maintain the highest standards of ethical business conduct – even when not legally mandated – so that our actions reflect well, both on our Company and us. We have a shared responsibility to make legal compliance and ethical business practices a part of the psyche and fabric of our Company so that we always act in a manner that upholds our values, creates trust and burnishes our image as an honorable and law abiding company.

To meet this responsibility, we must understand what is expected of us – and what is not.

That is the purpose of this Code – OUR Code of Conduct. It will help guide us to live our Company's values as we work towards making our Company stronger and better. We must all read it, seek to understand it, and be guided by its letter and spirit.

Thank you for your personal engagement in ensuring that our Company consistently succeeds the **right way.**



Table of Contents

About This Code	4
Being Respectful... Our Workplace	8
Diversity and Equal Opportunity	8
Treatment of Co-Workers.....	8
Health and Safety	9
Lawful Employment Practices	10
Being Loyal... Conflicts of Interest.....	11
Certain Relationships.....	11
Gifts and Entertaining	12
Fraternization	15
Other Employment	15
Being Honest... Company Assets and Information.....	16
Confidential Information	16
Insider Trading.....	17
Information Disclosure and External Communications	17
Use and Protection of Personal Data	18
Business or Financial Opportunities	19
Protection and Use of Company Assets	19
Accuracy and Protection of Company Records.....	20
Being Responsible... Legal Compliance and Social Responsibilities	21
Antitrust.....	21
Intellectual Property	22
Advertising.....	22
Product Integrity and Purchasing Practices.....	23
Government Investigations and Contacts.....	24
Environmental and Social Responsibilities	24
Company Policies	26
EEO & Anti-Harassment Policy	26
Employee Rights and Responsibilities Under the Family and Medical Leave Act	28
Vendor-Paid Trip Policy	30
Policy Regarding Confidentiality and Acceptable Use of Company Systems.....	31
Associate Data Security Policy.....	38
Product Safety Policy and Procedure.....	40

About This Code

Who is governed by this Code?

This Code applies to all Macy's and Bloomingdale's associates, whether working in stores, central offices, support organizations or elsewhere. When this Code refers to the 'Company,' it means the group of entities where all such associates work. ALL associates at ALL levels, referred to here as "we" or "us", are governed by this Code.

What are our responsibilities as associates?

Each of us should:

- follow all Company policies, including those discussed in this Code and in other materials distributed by the Company, such as associate handbooks and accounting policies,
- know that it is a fundamental principle of Company policy that each of us seek to understand and comply with all laws that relate to our jobs,
- use our voice to speak up and raise concerns, ask questions when in doubt or report suspected violations of Company policies, and
- make the necessary disclosures of any personal conflict of interest as described later in this Code.

Do supervisors have additional responsibilities?

Associates who are supervisors are responsible for creating a culture in which all associates understand the Company's commitment to conducting business legally and ethically, and following the Company's policies, including those in this Code. Above all, those of us who are in leadership positions must lead by example and create an open environment in which associates feel comfortable raising concerns without fear of retaliation.

Does this Code explain all of the standards and policies we need to know?

This Code is a starting point and provides general guidance. In addition, throughout this Code there are references to other Company policies. We have been provided access to such policies in this Code, as well as guidance on who **must READ, UNDERSTAND AND FOLLOW**.

Although compliance with all applicable laws is a fundamental requirement of our Company's policy, in certain instances, Company policy goes above and beyond the requirements of applicable law. This Code cannot and does not address every standard and policy we must follow, nor does it guide us through every situation or dilemma that we may face while performing our jobs. There are, however, additional resources that give specific guidance, which we may obtain from our supervisor, an HR representative or the Law Department.

As a rule of thumb, when acting on behalf of our Company, associates must ask themselves the following:

Is it legal?

Even if it is legal, does it comply with Company policies?

Even if it is legal and consistent with Company policies, is it the RIGHT THING TO DO?

Would it reflect well on our Company if it appears in tomorrow's newspaper?

If the answer to any of the above questions is "No," or if our good judgment or this Code and the other Company policies do not provide an answer, we must promptly seek help through one of the many channels discussed below.

Is it really necessary to speak up?

Yes, it is absolutely critical to do so. By using your voice and speaking up, you help protect our Company, our co-workers, our Company's customers and other stakeholders. The Company is counting on each one of us to preserve and protect its image and reputation. A vital way you can do this is by expressing your concern if and when you suspect in good faith that a Company policy has been violated.

- **Speak up and raise concerns early.** If you wait, it may get worse.
- **You can report anonymously.** However, if you identify yourself, the Company may be able to follow up with you and provide feedback. If you choose to report anonymously, please give enough details so the Company can investigate fully and accurately.
- **Confidentiality is respected to the maximum possible extent.** If you provide your name, your identity and report will be shared only as needed to look into and address the concern, or if required by law.
- **Retaliation is not tolerated.** Our Company absolutely prohibits retaliation against anyone who uses his or her voice to speak up for integrity to report a potential violation that he or she reasonably believes has occurred or is likely to occur. Retaliation is grounds for discipline up to and including dismissal. If you believe you have been subjected to retaliation, report it promptly to your HR representative, the Office of Solutions InSTORE or through ComplianceConnections. (ComplianceConnections are telephone and online facilities we may use for this purpose. Details regarding ComplianceConnections are provided below.)

If I report a possible violation, will I get in trouble if my concern turns out to be wrong?

No. You will not be punished or disciplined if you report a violation you believe has occurred or will occur. In fact, as Company employees, we all have a duty to report suspected violations of Company policy. We must, of course, have a reason for suspecting that a violation has occurred or will occur.

Q: I ran into a senior member of my department, Sandy, in the store the other day. She introduced me to her sister who told me that she was very excited because Sandy was using her discount to buy a lot of china for her and that because of Sandy's discount she was getting a lot more pieces than she would otherwise. I thought that Company policy prohibits associates from using their discount for others?

A: Yes, it is a violation of Company policy for associates to use their discount to make a purchase for another person and get reimbursed for the cost of the purchase. Although it is okay to use our discount to buy gifts for family and friends, it is not okay to do so if we receive payment for the cost of such gifts. If you believe a policy has been violated, you should discuss your concern with your supervisor or report what you have observed, since you've seen enough to suggest that there may be a problem.

Q: OK, I reported the situation above. It turned out that Sandy's sister is getting married and that Sandy was purchasing china from her sister's registry as a wedding gift. Am I going to get in trouble because it turned out to be nothing?

A: No. You did the right thing by raising a genuine concern. If anything happens that you feel could be retaliation, report that immediately.

Is it okay to not speak up and raise concerns when I am uncomfortable doing so?

No, it is not okay. Integrity Always means doing the right thing, even when it makes us uncomfortable. By doing or saying nothing about actions we honestly believe are in violation of any Company policy, we are violating this Code and are subject to disciplinary action.

How should I use my voice to speak up?

Our Company tries hard to foster an environment of open and honest communications. Our Company's "open door" policy gives associates many options.

- Your supervisor – usually a good place to start.
- Your supervisor's supervisor.
- Your store manager or the head of your Department or location.
- Your HR Department.
- The Office of Solutions InSTORE
- The Law Department.
- ComplianceConnections.

Most issues can be resolved by direct conversations between the people involved. However, if an associate is unsure of where to go for answers, uncomfortable raising issues with individuals within the Company, or wishes to report a potential violation of Company policy anonymously, he or she may raise the concern by using ComplianceConnections.

ComplianceConnections is a toll-free telephone line that is answered by an operator, 24 hours a day / 7 days a week. To reach ComplianceConnections, call 1-800-763-7290. ComplianceConnections can also be reached online at www.macyscomplianceconnections.com. These contact details are the same as for the Office of Compliance Associate Hotline that we have had for over a decade to ask questions and report misconduct. The difference is that ComplianceConnections is operated by an independent third party, which is not a part of the Company.

What happens when I raise a concern via ComplianceConnections?

If an associate contacts ComplianceConnections by telephone, a live operator from our third party service provider will answer questions or will give guidance on how to obtain answers or will check with the right sources within the Company to get the associate's questions answered. This service is available 24 hours a day / 7 days a week.

If an associate calls to report suspected misconduct, the operator will guide the associate through the process and create a report with the details provided. The operator will promptly forward the report to the right sources within the Company for follow-up.

If an associate accesses ComplianceConnections online, via www.macyscomplianceconnections.com, to ask questions or report suspected misconduct the Company's third party service provider will promptly forward the web communication to the right Company sources for follow up.

In each case, the reporting associate will be told how feedback will be provided on the associate's questions or concerns. In some situations, however, because of the nature of the inquiry, the Company or ComplianceConnections may not be able to provide feedback on the investigation.

The Company will investigate concerns about compliance with Company policies as follows:

- The issue will be assigned for investigation to associates who are skilled and objective.
- The investigators will gather information and determine facts. The investigation will be prompt and thorough, and confidentiality will be maintained to the maximum extent possible.
- The investigators may recommend corrective action, if necessary, to appropriate managers for implementation.
- Where appropriate, the associate raising the concern will receive feedback on the outcome.

Can I request a waiver of any requirement of the Code?

Yes, we may request a waiver as described below.

- With respect to associates other than the Company's executive officers, any request for a waiver of the Code's requirements must be submitted to, and to be effective must be approved by, the Company's General Counsel.
- With respect to the Company's executive officers, any request for a waiver of the Code's requirements must be submitted to, and to be effective must be approved by, a majority of the disinterested members of the Company's Board of Directors. All such approved waivers of the requirements of this Code will be promptly disclosed to the Company's stockholders.

Being Respectful... Our Workplace

One of the most valuable assets our Company has is its workforce. Our Company's values – "You Count" and "Teams Win" – are the drivers of our Company's goal to provide a work environment that is inclusive, respectful, safe and healthy – one that fosters wellbeing, energy and creativity. Each one of us is responsible for ensuring that our actions and words help to build and maintain such an environment.

Diversity and Equal Opportunity

What To Know

Our Company embraces diversity and wants its workforce to be as diverse, inclusive and multifaceted as our customer base. Our Company's goal is to offer all individuals equal opportunities within our Company.

What To Do

We must not discriminate against any person on the basis of race, ethnicity, age, religion, gender, sexual orientation, gender identity, gender expression, national origin, physical or mental disability, genetic information, military status, marital status, medical condition or any other attribute that doesn't relate to the person's job.

Our Company's commitment to diversity and equal opportunity applies to all aspects of our employment – this includes recruitment, hiring, placement, promotion, transfer, compensation, training, recreational and social programs and the use of Company facilities.

We must, however, bear in mind that it is not harassment or discrimination for a supervisor to enforce job performance and standards of conduct equally without regard to any protected characteristics.

If we believe that discrimination has occurred, whether against us or against a co-worker, we must raise our concerns.

[All associates must use this link to access, read and understand our Company's EEO & Anti-Harassment Policy.](#)

Q: I consider myself a minority associate. My supervisor has passed me over several times for a promotion. He gave the position each time to associates who I believe are lesser-qualified, non-minority employees, whom I am then asked to train. I think this is discriminatory. What can I do?

A: Ask your supervisor why he/she hasn't selected you. If, however, you are uncomfortable discussing this with your supervisor, or do not get a satisfactory answer, discuss it with your HR representative, Solutions InSTORE, or raise your concern through ComplianceConnections.

Treatment of Co-workers

What To Know

We must treat co-workers as we would like them to treat us – with respect and dignity. There is zero tolerance for harassment of any kind – whether verbal, written, physical or sexual – or any form of workplace violence.

What To Do

We need to be sensitive and alert to the fact that harassment may take many forms. Sometimes conduct that is not intended to harass may be perceived as harassment by another person. We must avoid all such conduct.

Examples include:

- Making offensive or unwelcome remarks, jokes or gestures,
- Making unwelcome sexual advances, requesting sexual favors, making unwanted physical contact or comments, or distributing or displaying sexually explicit, racist or derogatory materials,

- Abusing physically or verbally, threatening, taunting or leering,
- Treating certain associates or customers differently because of race, religion, sex or other characteristic protected by law.

Q: I am a female employee. A male co-worker frequently makes personal comments about my appearance that make me uncomfortable. I've asked him to stop, but he won't. What can I do about it?

A: You should report this to your supervisor, your HR manager, Solutions InSTORE, or through ComplianceConnections.

Health and Safety

What To Know

Our Company strives to create workplaces that are safe, healthy and secure.

What To Do

It is not possible to eliminate every hazard in the workplace, just as it is not possible to prevent all accidents in the safest of homes. That said, we must do our best to avoid them by not creating hazardous conditions, monitoring our workplaces continually, and correcting or eliminating unsafe conditions, if they exist.

Similarly, we must guard against violence in the workplace. We must not tolerate acts or threats of physical violence, including the unauthorized possession of a weapon in a Company workplace. Each of us is responsible for reporting any violence or unsafe conditions that we may observe. And we must always take appropriate and prudent steps to protect our own health and safety.

We also need to maintain a healthy and secure work environment. This means that associates must not possess, consume, sell, purchase or distribute drugs or have open containers of alcohol in our workplaces, or engage in Company business (whether or not in a Company workplace), report to work or operate any Company equipment or vehicle while under the influence of drugs or alcohol. Alcohol may be served at Company-sponsored events, which is the only exception. Associates may take drugs that are prescribed by a licensed physician or are available over the counter. However, if a physician has prescribed medication that requires any accommodation or influences an associate's ability to perform his or her job duties, the manager or HR representative should be notified to discuss reasonable accommodations that are necessary.

Q: I have been asked to skip a routine inspection of a store's escalators, and instead help store management get the store ready for a major sales event. We rarely find a problem when we do this inspection, but it still does not seem right to skip it. I suggested rescheduling the inspection a few days later after the sale, but they want to skip it entirely.

A: Store management is not authorized to cut corners on safety matters. Immediately contact your supervisor, HR department or report this through ComplianceConnections.

Lawful Employment Practices

What To Know

Our Company is committed to complying with all laws regulating employment practices, including pay rates, overtime, meal periods, rest breaks, occupational health and safety, and leaves of absence.

What To Do

We must strive to properly categorize all associates as overtime exempt or non-exempt, and as employee or independent contractor, under employment and tax laws.

Those of us who record time worked, or manage associates who record time, or otherwise have access to time records must make sure that time records accurately reflect all time periods worked. We must not work or permit others to work off the clock. For example, we must not

- fail to record work performed at home,
- delete or conceal hours worked, including overtime hours, or move hours from one day to another to eliminate overtime,
- revise a correctly entered time record, or
- fail to take the required rest and meal breaks, or permit or require others to do so.

Q: I'm an hourly associate, I've been busy lately, but my supervisor does not want me to work more than 40 hours each week. To get my work done, I've been working for a half hour after I clock out each evening. Since this benefits the Company, have I done something wrong?

A: Yes. It is never OK for you to work off the clock. You must record accurately all time periods worked. Not doing so is a violation of Company policy. If you feel that you are not able to complete your work in 40 hours, please discuss your concerns with your supervisor or with your HR manager. As always, you can also bring your concerns to the Company through Solutions InSTORE or ComplianceConnections.

We must also ensure that our Company is in compliance with all laws governing employees with disability and employee leaves of absence, including the Family Medical Leave Act.

All associates must use [this link](#) to access, read and understand the form titled "Employee Rights and Responsibilities under the Family and Medical Leave Act."

Being Loyal... Conflicts of Interest

A conflict of interest exists when a personal interest or activity interferes – or appears to interfere – with the duties we perform for or owe to our Company. We owe it to our fellow associates, shareholders and other stakeholders to ensure that no activity of ours at work or home harms our Company's reputation or interests.

All business decisions should be made solely in the Company's best interest, and not for any personal gain. Similarly, when conducting our personal affairs and ourselves, we must avoid actions or situations that create, may create or reasonably appear to create, conflicts with the Company's interests.

Here are some common ways conflicts of interests could arise.

Certain Relationships

What To Know

A conflict of interest may arise if an associate or his or her family member (such as spouse, children, parents or siblings) has a relationship with a business partner or competitor of the Company.

- By "business partner" we mean anyone who does or seeks to do business with the Company. Examples are a supplier or purchaser of goods, services, equipment or real estate.
- By "competitors" we mean anyone in our geographic markets who sells merchandise that is the same as or similar to the merchandise we sell.

Examples of "relationships" that could present a conflict are below.

If one of us, someone in our family or someone with whom we have a significant relationship (including marriage, domestic partners, dating relationships, or family (such as sibling, parents, child))

- has a substantial amount of stock or other interest in a business partner or competitor,
- accepts an offer by a business partner or competitor to buy stock on terms not generally available to the public, or
- is an officer, director, employee, or consultant of a business partner or competitor.

What To Do

Not all relationships present a conflict of interest.

- **The questions we must ask ourselves are:**
Could the relationship cause or influence me to make a decision that is not in the best interest of the Company?
Or, could it look to others as if the relationship is influencing me?
- **Some investments are always wrong.** We must never personally invest in a business partner if we have any involvement in selecting or negotiating with the business partner or if we supervise anyone who has such responsibility.
- **We should carefully weigh a potential new relationship that could present a conflict of interest before entering into it.** Seek guidance and permission from our HR representative, who may consult with the Law Department.
- **We should disclose to the Company any conflict of interest (either when providing the annual conflict of interest sign off or promptly to our HR representative after becoming aware of a conflict of interest).**

Q: We need to hire a cleaning service for some stores. We could save our Company a lot of time and effort by hiring my brother's cleaning firm. They would also be the right choice because I would have control over them and they can be trusted to do the job right. And, they'll give us a special price. May I hire his Company?

A: No. Hiring a firm run by a family member is not a sound business practice and it violates our policies. It creates a conflict of interest between your desire to help your brother and your duty to select the most competitive supplier for our Company. Even if you have nothing but our Company's interests at heart, it may appear to others that you are being influenced by your relationship with your brother. However, if you make a full disclosure to your supervisor, HR representative and Law Department, and you remove yourself from the selection process (and no one who reports to you is involved), in certain situations the Company may permit your brother's firm to compete for the work with other bidders.

Q: A vendor of the Company that I do not directly work with is offering its stock for sale to the public. A friend of mine there tells me that the vendor has reserved shares to offer to its customers and business partners. He has offered me an opportunity to participate on this "favored" basis. May I buy some of the offered shares?

A: No. Accepting an offer to purchase a business partner's stock on terms that are not available to the general public violates our policy and must be avoided even if you are not directly involved in our Company's transactions with that vendor.

Gifts and Entertainment

What To Know

The Company does business on the basis of sound business judgment and seeks to treat all of its business partners fairly. Accepting a gift from or giving a gift to any business partner or competitor could create the expectation or appearance that they will be treated more favorably than others. We could also appear to be unfair and dishonest in our dealings.

Gifts or gratuities could take many forms - cash, merchandise, loans or non-cash gifts, such as gift certificates, discounts, gratuities, services, transportation, use of vehicles or vacation facilities, participation in stock offerings, tickets to sporting events or invitations to meals or events. The potential list is endless.

What To Do

Certain gifts and entertainment are permissible, while others are not. When receiving or offering gifts or entertainment, we must follow the Company's guidelines strictly and seek help when we are unsure.

Usually OK

Nominal Gifts

Gifts of "nominal" value (a combined retail value of \$100 or less) that are common courtesies in our business are usually okay to give or receive. When giving or receiving gifts of nominal value, remember these guidelines:

- The value of all gifts from a single source (including token gifts like pens, mugs and calendars) must not exceed \$100 in a calendar year;
- Gift baskets are to be shared with co-workers
- An associate must have the corporate authority to incur the expense of giving gifts; and
- Gifts that fall in the "Always Wrong" category below may not be given or received.

If the above guidelines are followed, gifts of nominal value do not require disclosure or approval. If there is any question about a gift, contact the Office of Compliance and Ethics (officeofcompliance@macys.com) for guidance.

Participation in Social Events with Business Partner

Participating in a social event with a business partner is the one exception to the \$100 limit on gifts. We may participate in events in which we are interacting with business partners or vendors. Follow these simple guidelines:

- We may accept an invitation from a business partner to a sporting, cultural, overnight outing or other event ("Social Event") in which the business partner also is participating, provided that the face value of the cost for

our participation (where it can be reasonably determined or estimated) does not exceed \$250. If the business partner is not personally participating in the Social Event, then the invitation is a gift and subject to the \$100 nominal gift limitation.

- We may not accept invitations to multiple Social Events from a single business partner if the aggregate face value of all invitations is more than \$250 in a calendar year, unless we obtain advance written clearance (electronically or otherwise) from the Office of Compliance and Ethics. Clearance will be based on, among other factors, the business development value of the Social Event(s).
- Unless clearance is obtained as provided above, an associate must (i) pay the business partner for the excess over \$250 of the aggregate face value of the cost of the Social Events in which the associate has participated at the invitation of a single vendor in any single calendar year; and (ii) disclose all such payments in the annual Code of Conduct acknowledgement.
- If there is uncertainty with regard to the dollar “value” or any other aspect of a Social Event, the associate should contact the Office of Compliance and Ethics (officeofcompliance@macys.com) for guidance.

Meals

Meals with current or prospective business partners are separate and distinct from gifts and social events. We may participate as the guest or host in occasional meals with our business partners if:

- It is a common business courtesy in our industry,
- It is not too frequent, extravagant or excessive in value, and
- There is mutuality in the “give and take” such that we and our business partners have a chance to both treat and be treated.

If we include business partners in meals that we host, the expense should be classified as “Entertainment” in our reimbursement requests.

Vendor Paid Trips

We may accept invitations to vendor sponsored events or meetings only in compliance with our Company’s Vendor Paid Trip Policy.

[Associates who have been or are likely to be invited to participate in events or trips that are paid for, to any extent, by current or potential vendors or business partners, including all associates in buying organizations, must use this link to access, read and understand our Company’s Vendor-Paid Trip Policy.](#)

Contributions to Charitable Causes

We may solicit contributions from our business partners to charitable causes ONLY in compliance with our Company’s policy on vendor solicitation. This policy may be found in the Policy Center on the MyMacy’s Portal.

Always Wrong

Some types of gifts and entertainment are **NEVER** permissible and no one can approve them. We may **NEVER**:

- Accept or give any gift or entertainment that is or could be illegal.
- Accept or give a gift of cash or cash equivalent (such as a check, money order or a gift certificate that is convertible to cash), loans, stock or stock options.
- Participate in any entertainment that is inappropriate, sexually oriented or otherwise violates our policy of mutual respect.
- Participate in any activity or accept or give any gift that you know would cause the person giving or accepting the gift or entertainment to violate his or her own employer’s policies.

Always Ask

It may not always be clear to us whether certain gifts and entertainment are permissible. In such situations we must not proceed without obtaining the written approval of our HR representative, who will consult with the Office of Compliance and Ethics.

When approval is requested, the Office of Compliance and Ethics will consider the following:

- whether the gift or entertainment would be likely to influence your objectivity,
- whether there is a valid business reason to attend the event,
- whether we would be setting a precedent by accepting or giving the gift or attending the event, and
- whether it could reasonably create a negative impression in the minds of our co-workers or outsiders.

Gifts and Entertainment Examples to Consider

Q: The sales representative for a business partner has offered me tickets to a baseball game. Can I accept them?

A: Possibly. If the sales representative is inviting you to attend the game with him/her, this may constitute a business function and may be appropriate. If the face value of the ticket is unclear or is above \$250, follow the guidelines provided above for attending Social Events with a business partner. If the sales representative is not attending the game, then the tickets would be considered a gift and must meet our standards for accepting gifts of "nominal" value.

Q: ABC Corp. has offered me an opportunity to attend an industry trade show in January at the expense of the ABC Corp., who is headquartered in Chicago. While our policy permits attendance at trade shows, the trade show is being held at a Disney World Resort in Orlando, Florida. We spend approximately \$4.0 million annually with ABC Corp. During the trade show, there will be a number of seminars applicable to our business and networking events that are available during the event days, including an all-attendee dinner at Sea World with a great keynote speaker scheduled to make a presentation. ABC Corp. is also giving each participant a two day hopper pass to Walt Disney World valued at approximately \$200. Is it acceptable for me to attend the trade show and related events?

A: Be careful. Before you can accept any vendor paid travel (transportation, lodging, registration, meals, etc.) you must make sure that you follow the Vendor Paid Trip Policy. That means you need written approval by an Executive Vice President in your pyramid prior to any travel. If approved, you then would need to contact the Office of Compliance & Ethics for additional approval, as the travel is not to the Vendor's main office. In this instance, since it is reasonable to hold a January trade show in Florida instead of Chicago, an exception to the policy likely would be granted and you would be able to attend the trade show at the Vendor's expense. While at the trade show, it would be acceptable to attend the group dinner. The hopper pass, however, requires additional information and consideration. Consider three possible alternatives:

1. If the hopper pass were given to you to enjoy by yourself at your own leisure, then it would be a gift, which exceeds our \$100 nominal threshold for a gift and, therefore, must be refused.
 2. If the hopper pass were given to you to enjoy with a business partner from ABC Corp., then it would be considered a Social Event and would meet our Social Event limitation of \$250. In this instance, the hopper pass could be accepted.
 3. If the hopper pass were given to all trade show attendees for a specific group event, then it should be analyzed as part of vendor paid travel to consider whether it is business related, or falls back under our Gift or Social Event policy. This requires additional information and should be discussed with the Office of Compliance & Ethics prior to the event.
-

Remember – always review the Vendor Paid Trip Policy before a vendor pays for any part of a trip and to ask the Office of Compliance and Ethics (officeofcompliance@macys.com) if you have any questions or concerns.

Fraternization

What To Know

While all of us have the right to associate freely and pursue personal relationships with our colleagues, a romantic, intimate, financial or family relationship in the workplace may create an uncomfortable work environment for others. It may also create – or appear to create – a conflict of interest if we have such a relationship with a subordinate or a supervisor.

What To Do

Associates in such relationships must use tact and good judgment. If the relationship is with a direct or indirect subordinate or supervisor, or with an employee, officer, owner, or director of a current or potential business partner, we must promptly tell our supervisor or HR representative, who will consult with the Law Department to determine if some action is needed.

Other Employment

What To Know

A conflict of interest exists if an associate works for or receives compensation for services from any competitor or current or potential business partner of the Company.

What To Do

An associate must not provide any services for a competitor or business partner for which he or she is paid either in cash or indirectly. (“Indirectly” includes a promise of future employment or other personal or family benefit), unless approved by the HR department. In addition, associates may not serve on the board or as an officer of another for-profit company, even if it is not a competitor or business partner, without the approval of the General Counsel of the Company.

All of us are encouraged to serve as a director, trustee or officer of non-profit companies in our individual capacities, but we must obtain the approval of our HR department before doing so as a representative of the Company.

Q: I need to make some extra money and I want to get a second job. Is this okay?

A: This may create a conflict of interest if your second job is with a competitor or business partner of our Company, or if it adversely affects your job performance. You should discuss any potential employment with your supervisor or your HR representative.

Being Honest... Company Assets and Information

Our Company's assets must be used, purchased or disposed of only for the Company's benefit. We are all obligated to protect the assets of the Company and use them appropriately.

In addition to merchandise, equipment, furnishings and other property, our Company's assets include Company information, the personal information of the Company's employees and customers, any work product we may develop in the course of our employment, and any business or financial opportunity that the Company could avail itself of.

Confidential Information

What To Know

Confidential information about our Company, its business, associates, customers and business partners should be protected. It can be used only to pursue the Company's business interests or to comply with the Company's legal or other obligations.

What is confidential information? It could be business or marketing plans, pricing strategies, financial performance before public disclosure, pending negotiations with business partners, information about employees, documents that show social security numbers or credit card numbers – in short, any information, which if known outside the Company could harm the Company or its business partners, customers or employees or allow someone to benefit from having this information before it is publicly known.

Just as our Company requires that its own confidential information be protected, our Company also requires that the confidential and proprietary information of others be respected.

What To Do

In performing our duties, we as associates may have access to confidential information relating to our Company, its business, customers, business partners or our co-workers.

We are all trusted to maintain the confidentiality of such information and to ensure that the confidential information, whether verbal, written or electronic, is not disclosed except as specifically authorized. Additionally, it must be used only for the legitimate business of the Company.

Here are some simple rules to follow.

Confidential information should:

- Be stored in locked file cabinets or drawers and not be left where others can see it,
- Be clearly marked as confidential whenever possible,
- Be shared only with those who need to see it for Company business purposes,
- Not be sent to unattended fax machines or printers,
- Not be discussed where others may hear,
- Be shredded when no longer needed.

Always respect the confidentiality of the information of third parties. We must not use or disclose any of it except as authorized under a written agreement approved by our Law Department.

[All associates must use this link to access, read and understand our Policy Regarding Confidentiality and Acceptable Use of Company Systems.](#)

Insider Trading

What To Know

As associates, we may from time to time become aware of “material inside information.” Associates must take care to avoid using “material inside information” for their own gain or to enable others to gain from it.

“Material inside information” generally means significant and confidential information about the Company’s business (which may include information relating to its business partners) that has not been disclosed to the public.

Examples of material inside information include information not yet announced to the public relating to earnings and financial performance information, business deals or plans, a change in the dividend, a stock split, a merger or acquisition, disposition or consolidation, changes in directors or senior executive officers and changes in control. Information is considered to be “inside” or “nonpublic” information unless it has been fully disclosed to the public, such as, for example, through public filings with the SEC or issuance of Company press releases.

What To Do

We may not buy or sell (including through the exercise of stock options) any stock or other security (such as warrants, debentures, puts or calls), whether of the Company or another entity, on the basis of material inside information. Nor may we disclose such information improperly, either intentionally or inadvertently, whether during business hours or in informal, after-hours discussions.

Trading in Company stock (or in the stock of any other company) on the basis of material inside information could result in civil and criminal charges against the person executing the trade and/or the person who provided the information to the person who traded. In addition, it would subject the Company to embarrassment and potential liability.

Q: My wife told our neighbor that I was working late on an important acquisition. A week later we announced the purchase of a major business and our Company’s stock price rose substantially. I learned later that my neighbor bought our Company stock before the public disclosure of the acquisition. I never had any conversation with this neighbor directly. Have I violated our Company policy?

A: Yes. By telling your wife, who then told your neighbor, about the nature of the assignment you were working on, you indirectly tipped your neighbor. Our Company takes a very serious view of such violation. So do the federal and state authorities. You should discuss the situation with the Law Department promptly.

Information Disclosure and External Communications

What To Know

Securities laws and stock exchange regulations regulate when, how and to whom our Company should disclose material inside information.

In order to comply with these regulations, our Company has strict guidelines for the release of material inside information to the public. Additionally, only a few associates are specially authorized to discuss any Company information with the media or the investment community.

What To Do

We must follow all Company policies governing the public disclosure of material information about the Company. Further, we must not

- discuss our Company or its affairs with the media, investors, financial or industry analysts, outside consultants, on Internet chat pages or in public forums, or
- use Company information in presentations to external audiences, such as college groups and industry conferences,

without obtaining specific approval from our Corporate Communications Department, Investor Relations Department or the Law Department.

Use and Protection of Personal Data

What To Know

The Company has certain personal data of its present and former associates, customers and vendors. It respects the privacy of this personal data and is committed to handling this data responsibly and using it only as authorized for legitimate business purposes.

What is considered personal data? It is information such as names, home and office contact information, social security numbers, driver's license numbers, account numbers and other similar data.

What To Do

We have a strict obligation to use such personal data in a manner that:

- respects the privacy of our co-workers and our Company's customers and vendors,
- complies with all applicable laws and regulations, and Company policies,
- upholds any confidentiality or privacy obligations of the Company in its contracts.

In addition, we must follow all policies and measures adopted by the Company for the protection of such data from unauthorized use, disclosure or access. If any of us becomes aware of any instance of data being accessed or being used in an unauthorized manner, we must report it immediately to our Divisional Security Administrator or the Law Department.

All associates must use [this link](#) to access, read and understand our Company's Associate Data Security Policy.

Q: I am a RTW buyer. My vendor rep asked me for information about our customers and further asked if the vendor could put out forms in our stores asking customers to join the vendor's email list. Is this OK?

A: No. We generally don't share customer information with our vendors or let them collect customer information themselves in our stores. If you get such a request, inform your DMM or GMM, who will contact the Law Department for guidance.

Q: I am the manager of the menswear department in a high volume store in New York. One of my successful sales associates asked if he could keep in his clientele book the contact and account information for certain clients who rely on him to ring up merchandise for them because they are too busy to come into the store. I am concerned that if I do not permit the associate to do this, we will lose valuable sales.

A: The Company recognizes the value of such client relations and customer service. However, the Company has strict guidelines on the protection and use of customer information. Our Company has provided both tools and guidance to our sales associates to help them to continue providing excellent service to their customers, while at the same time protecting their customers' personal information. You must immediately consult the policies that govern you and your associates and seek help from the Law Department to understand what is permissible and what is not.

Business or Financial Opportunities

What To Know

We as associates may discover during our employment a business opportunity that the Company may be interested in. All such opportunities belong to our Company and may not be diverted away for personal gain.

What To Do

If we know or could reasonably anticipate that the Company would have an interest in pursuing a business or financial opportunity we should not try to take advantage of that opportunity for ourselves or divert it to any other party.

Protection and Use of Company Assets

What To Know

Company assets belong to the Company. We must protect them and use them only for Company business.

Associates must not use merchandise, intellectual property, data, supplies, samples, software, equipment, fixtures and other assets of the Company for personal benefit.

Company computers, for example, are intended for Company business use. Only limited personal use is allowed. An associate's use of Company equipment, Internet access or email or voice mail systems is not private. The Company reserves the right to monitor our use, consistent with applicable laws.

Theft, fraud, carelessness and waste of Company assets directly affect our reputation and profitability.

What To Do

We should all protect our Company's assets by guarding against and reporting not only any suspicion we may have of theft or fraud, but also any waste or misuse we may observe.

We must not copy or inappropriately use software licensed to our Company, download unauthorized software onto our Company computers, or use our Company's trademarks or copyrights except as authorized by Company policy.

Similarly, we should not use Company assets, including merchandise, or funds for illegal, unethical or otherwise improper purposes. For example, we must not seek to advance the Company's business with any governmental authority by means of bribes or payments to any third party.

Q: Is it okay to take home samples or defective merchandise?

A: No. It is not ok, unless it is purchased in a Company-sponsored sample sale.

Q: I sometimes email my spouse to make personal plans, such as who will take the kids to their after-school activities. Am I allowed to use the Company's computer for this?

A: Yes, as long as personal use is reasonable and does not interfere with your work.

Q: I helped a co-worker duplicate a software application for the business he runs from his home. Did we violate Company policy?

A: Yes, you both violated Company policy by misusing a Company asset. In addition, the copying may have violated the terms of the license agreement under which the Company acquired the software. This creates potential liability for the Company under the license agreement as well as under federal copyright laws. And, you both could be personally liable under applicable laws.

Accuracy and Protection of Company Records

What To Know

Our Company's books and records must be clear and accurate, and must fairly reflect our Company's business transactions and assets. All our public disclosures must be full, fair, accurate, timely and understandable.

Accurate records are essential to conducting our business successfully. They are also the basis on which we make the required financial disclosures and other public statements about our business, financial condition and results of operations.

For these reasons, we maintain a comprehensive system of internal accounting practices and controls that is designed to help us meet our objective.

In addition, all Company records, in whatever format or media they exist, must be retained in accordance with the policies contained in the Company's Records Management Program.

What To Do

All Company accounting policies and internal controls must be followed. Some of these internal controls govern who may sign contracts that bind our Company and who has authority to incur expenses on behalf of the Company and to what limits. We must follow these controls strictly.

Additionally, we all must cooperate fully with our internal and external auditors. We may not, directly or indirectly, take any action to coerce, mislead or fraudulently influence any accountant or auditor engaged in an audit or review of our Company's records or procedures.

There is no tolerance for any deviation from this policy

If any of us becomes aware of any such wrongful behavior, or inaccurate recording or improper reporting of the Company's information, we should promptly report these matters to our immediate supervisor. If we believe in good faith that any such wrongful behavior, inaccurate recording or improper reporting is sanctioned by our immediate supervisor, it should be reported to a senior level manager, to HR, to the Law Department, or through ComplianceConnections.

In addition, if we become aware that the procedures for collecting and reporting information have not been strictly followed, or are flawed, we should similarly report that fact, even if that failure has not resulted in any inaccurate public disclosure.

If any of us has questions about accounting, internal accounting controls or auditing matters, we may submit them to the Audit Committee of the Board (which you may do anonymously and confidentially) through a secure website, at <http://www.macysinc.com/corporategovernance>. The Audit Committee will consider and act upon any questions and concerns regarding accounting, internal accounting controls or auditing matters submitted to the Audit Committee.

All Company records must be retained for the periods specified in the policies contained in the Company's Records Management Program, which can be accessed via the Policy Center on the MyMacy's Portal. If we are unable to access the document through the MyMacy's Portal, we may seek guidance from the Law Department.

Further, if we are told or otherwise become aware that certain records, whether in paper, electronic or other form, may be relevant to pending or anticipated legal action, they must not be destroyed without the approval of the Law Department.

Being Responsible... Legal Compliance and Social Responsibilities

Our Company is committed to conducting its business in full compliance with all applicable laws. This requires that we avoid not only any action that is clearly illegal, but also any action that may be technically legal, but is inconsistent with our core principle of “Integrity Always.”

Our Company also embraces its social responsibilities and seeks to support and enrich every community in which we work and live.

Being Responsible... Legal Compliance

It is not possible to cover all the laws that govern our business. However, each of us must recognize that certain laws apply to our jobs, and we must become familiar with them. When we are not sure if a particular action would violate applicable laws or our policies, we should ASK our Law Department. The sections below discuss a few principal laws that apply to our business.

Antitrust

What To Know

Antitrust laws are intended to promote vigorous competition. They prohibit agreements that seek to limit or restrain trade.

Our Company is firmly committed to competing fairly and ethically. It believes that a free market economy is in the best interest of both our customers and our Company.

What To Do

We may not enter into or try to enter into agreements, understandings or communications with **competitors**, whether written or unwritten and whether directly or through third party intermediaries, on matters such as prices, markups, markdowns, and any other terms or conditions on which we do business. Any such attempt on our part would not only violate the law, but is a bad business practice.

We must scrupulously avoid every situation, meeting, communication or conversation, which could be construed as involving an attempt to reach such an agreement.

Agreements with business partners, such as vendors, regarding the retail prices at which our Company will sell that vendor’s merchandise are prohibited. This includes agreements about sale, mark down or clearance prices, as well as the dates on which those prices will go into effect.

It is permissible to discuss markdown support, but we may not agree to sell an item at a certain price in exchange for a markdown allowance.

While it is not practical to discuss here all the “Dos and Don’ts” under Antitrust and Fair Competition laws, the following are helpful guides.

- Do compete vigorously, but ETHICALLY,
- Do not make agreements with respect to pricing with any business partner (vendor),
- Do not discuss **any competitor’s** pricing, clearance or markdown practices with a business partner,
- Do not engage in activity with a vendor or competitor that seeks to limit the vendor’s product distribution practices or control market prices, although asking for an exclusive on a newly introduced item is permissible,
- Do not induce a business partner to breach an existing agreement it has with a third party,
- Do inform all current and potential business partners of our Company’s commitment to maintaining the highest ethical standards as it competes vigorously to provide the best products at the best prices for its customers.

All merchants and planners must seek to understand and comply with our Company's Antitrust Guidelines. Ask the Law Department if additional guidance is needed.

Q: I am friends with some buyers of one of our Company's competitors. When I see them at trade shows, conferences or other events we often end up having lunch or dinner. We talk about industry trends, other retailers and other general topics. Is this a problem?

A: You should use caution in these situations. Do not discuss our Company's pricing, relationships with business partners, markup/markdown practices or other business practices or those of the competitor. If any anticompetitive topics come up in the conversation, you should refuse to participate and leave the conversation immediately.

Intellectual Property

What To Know

Trademarks, trade names, copyrights, trade secrets, rights of publicity and other similar proprietary information are considered intellectual property. Our Company owns many valuable intellectual property rights, such as our trademarks INC and Alfani.

Our Company may lose its rights in the intellectual property that it already owns, or risk lawsuits and other penalties if we fail to comply with certain laws.

Our Company also has the right to use the intellectual property of certain business partners under agreements. American Rag is one such example.

We must use our Company's or a business partner's intellectual property only as authorized.

If we violate the terms of these agreements, our Company may not only lose the right to use the licensed intellectual property, but may also be subject to substantial damage claims

What To Do

We must not use the intellectual property rights of others without their permission.

We may use the intellectual property of the Company only for the benefit of the Company, and should not allow others to use our logo or other intellectual property except in accordance with prescribed procedures.

Similarly, if and when the Company is permitted to use the intellectual property of its business partners, we must follow the reasonable usage guidelines provided by the business partner.

We must not provide to or accept from third parties any proprietary information or the right to use intellectual property without a written agreement that is prepared by our Law Department.

If any of us makes a discovery, or develops an invention, design, process, concept or idea in the course of our employment with the Company, the Company owns it. We should assist the Company's lawyers in documenting the Company's ownership.

Advertising

What To Know

Our Company's goal is "truth in advertising."

Our Company is committed to earning and keeping the trust of its customers by advertising in a clear and accurate manner.

Our Company's policy is to comply with all applicable laws, including those that govern pricing, product information, product availability and phone and mail order rules, among others.

What To Do

Our Company's advertising must be clear, accurate and helpful to our customers.

We must follow all our Company's advertising policies and guidelines.

When we say something about the products or services our Company sells, we must be able to substantiate it. That means we must have proof of what we say, before we say it. This is true even if we are just passing along what our vendor says about its merchandise.

All associates employed as merchants or planners or who work in marketing or advertising must seek to understand and comply with the Company's Retail Advertising Guidelines. Ask the Law Department if additional guidance is needed.

Product Integrity and Purchasing Practices

What To Know

Our Company acts upon its value "Customers First" by selling quality products and standing behind them.

Our Company's policy is to comply with all applicable laws governing production, testing, packaging and labeling of products.

When our Company procures products from vendors, it requires these vendors also to do the same, regardless of country of origin. Additionally, our Company is committed to fair purchasing practices and requires vendors to adhere to the Company's Vendor Code of Conduct.

Our customers trust us to take all the necessary safeguards to ensure that the products we offer for sale meet high standards for safety and quality, and are manufactured in a socially responsible manner.

What To Do

We must safeguard our Company's reputation and goodwill with our customers by ensuring that the products and services we sell are safe.

Product safety is the responsibility of each one of us.

Buyers and product developers must make every effort to ensure that the products or services our Company sells perform as we claim they do and are manufactured as we state they are.

Store associates must identify potential safety and quality issues and follow Company procedures to report them promptly.

In addition, store associates must follow Company guidelines in cases of returns or recalls of allegedly unsafe or defective products.

In all aspects of sourcing, production, sale investigations of claims or recalls, we should partner with our Law Department to ensure that we are in compliance with all applicable laws.

All associates in

- stores, including store managers, general and department managers and their staff,
- buying organizations, including buyers and planners, product developers and designers, as well as other associates who have or are likely to design or produce merchandise such as associates on special events teams or Corporate Marketing,
- customer service, including MCCS' Presidential and Retail Groups and Corporate Communications, and
- risk management, including claims adjustors

must use [this link](#) to access, read and understand our Company's Product Safety Policy and Procedure.

Government Investigations and Contacts

What To Know

Our Company's policy is to cooperate with appropriate governmental requests or investigation, and to comply with all applicable laws governing contacts with government officials. Our Law Department is responsible for managing all such requests, investigations or contacts and providing truthful and accurate information.

What To Do

If we are asked to provide information – verbal or written – for a government investigation, or if a government representative appears at our workplace, we must promptly notify our Human Resources representative or the Law Department and obtain approval for the release of any information. We must not obstruct, influence, mislead or impede the investigation.

Any contacts with government officials for the purpose of influencing legislation, regulations or decision-making may constitute lobbying. We must not contact or communicate with any government official for such purpose on behalf of the Company without having specific authorization. If a need arises to do so, we must contact the Law Department.

Political Activities

The use of Company funds for political activities is regulated heavily at the state and federal levels and the Company has established policies and procedures to comply with all applicable laws. No corporate funds may be used for political activity without compliance with those policies and procedures. Any questions regarding corporate political activities should be directed to the Group Vice President, Legislative Affairs.

Being Responsible... Social Responsibilities

Environmental and Social Responsibilities

What To Know

Our Company cares about the environment and complies with all environmental protection laws.

Our Company has implemented many sustainability programs that go several steps beyond the requirements of the law and are aimed at preserving and protecting the environment. These steps include measures to conserve energy, prevent the waste of valuable resources like water and electricity and recycle products.

Our Company seeks to live up to its value of "Giving Back" by caring for and enriching every community in which it participates through us. Our Company's long-established tradition of giving back to our communities is orchestrated through various Company-sponsored community service programs, such as "Partners In Time".

Our Company requires our Vendor's to comply with our Vendor Code of Conduct which includes a prohibition against child labor, slavery and human trafficking. The Company's Vendor Code of Conduct is located at www.macysinc.com under About Us / Policies/Positions.

What To Do

We must demonstrate our Company's commitment to preserving and protecting our environment in all our actions for the Company, including by complying with all applicable laws.

We must learn about our Company's sustainability programs and make a conscious effort to not waste valuable resources and dissuade others from doing so.

Additionally, our actions must uphold and demonstrate our Company's goal of giving back to every community in which we live or do business.




macy's inc

EEO & Anti-Harassment Policy

Equal Employment Opportunity

Macy's Equal Employment Opportunity Policy prohibits any form of discrimination in the workplace. The Company is committed to treating all associates equally on the basis of job-related qualifications, abilities and performance, regardless of race, ethnicity, age, religion, gender, sexual orientation, gender identity, gender expression, national origin, physical or mental disability, genetic information, military status, marital status, medical condition, or any other category protected by law or unrelated to job performance.

As part of the Macy's EEO & Anti-Harassment Policy, all associates should enjoy a working environment free from all forms of discrimination and harassment. It is against the Company's policy for any associate to harass another associate based on race, ethnicity, age, religion, gender, sexual orientation, gender identity, gender expression, national origin, physical or mental disability, genetic information, military status, marital status, medical condition, or any other category protected by law. Therefore, the Company will treat harassment as it does any other form of employee misconduct and it will not be tolerated.

Sexual Harassment

No associate, male or female, should be subjected to unsolicited and unwelcome sexual advances or conduct. Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, or other verbal, visual, or physical conduct of a sexual nature where:

- (i) Submission to such conduct is made either explicitly or implicitly a term or condition of an associate's employment;
- (ii) Submission to or rejection of such conduct by an associate is used as a basis for employment decisions affecting such an individual; or
- (iii) Such conduct has the purpose or effect of negatively interfering with an associate's work performance or creating an intimidating, hostile, or offensive working environment.

All associates are prohibited from offering, promising, or granting preferential treatment to any other associate or applicant for employment as a result of that individual's engaging in or agreeing to engage in sexual conduct. Likewise, all associates are prohibited from using any other associate's or applicant's refusal to engage in such conduct as a basis for an employment decision affecting that individual or others.

An intimidating, hostile, or offensive working environment may be created by such circumstances as pressure for sexual activities, unwanted and unnecessary physical contact with another associate, verbal abuse of a sexual nature, the inappropriate use of sexually explicit or offensive language or conversation, or the display in the workplace of sexually suggestive objects or pictures. This would include the placement of offensive materials on walls or bulletin boards or the circulation of offensive materials received electronically through the Company's email or other electronic systems.

This and other sets of circumstances provided in this policy are not exhaustive; they are intended as guidelines illustrating violations of Macy's Anti-Harassment policy.

Other Forms of Prohibited Harassment

Similarly, a racially hostile working environment may be created by circumstance such as verbal abuse based on race, including the use of racial epithets, racial slurs, racial remarks, racially derogatory terms, and racial jokes or insults.

Other hostile work environments may be created by the use of epithets, slurs or derogatory terms, insults, jokes, or teasing based upon another's ethnicity, age, religion, gender, sexual orientation, gender identity, gender expression, national origin, physical or mental disability, genetic information, military status, marital status, medical condition, or any other category protected by law.

Macy's will not tolerate harassment of any type based on race, ethnicity, age, religion, gender, sexual orientation, gender identity, gender expression, national origin, physical or mental disability, genetic information, military status, marital status, medical condition, or any other category protected by law. Engaging in harassment of others will lead to discipline, up to and including termination of the associate violating Macy's Anti-Harassment policy.

Complaint Procedure

Any associate who believes they have been subjected to or observed such behavior by another associate, either in or outside of the workplace, must report the situation immediately to:

- A manager or supervisor;
- A Human Resources representative;
- ComplianceConnections at 1-800-763-7290 or www.macyscomplianceconnections.com; or
- Solutions InSTORE at 1-866-285-6689

If a satisfactory response is not received from the person or office to whom a complaint was made, the associate should bring the complaint to the attention of another person or office listed above.

Macy's takes all complaints of harassment very seriously. All complaints will be promptly investigated and handled as confidentially as a thorough investigation allows.

Remedial Action

Following a complete review and thorough investigation of the complaint, appropriate remedial action will be taken and communicated to the parties involved. Any associate found to have engaged in harassment in violation of Macy's Anti-Harassment policy, will be subject to discipline, up to and including discharge.

No Retaliation

Retaliation in any form against an associate or applicant who complains of discrimination or harassment, or against anyone who participates in the investigation of such a complaint, is strictly prohibited and will itself be cause for disciplinary action up to and including discharge. Any form of retaliation must be reported immediately pursuant to the Complaint Procedure outlined above.

Employee Rights and Responsibilities Under the Family and Medical Leave Act

Basic Leave Entitlement

FMLA requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to eligible employees for the following reasons:

- For incapacity due to pregnancy, prenatal medical care or child birth;
- To care for the employee's child after birth, or placement for adoption or foster care;
- To care for the employee's spouse, son or daughter, or parent, who has a serious health condition; or
- For a serious health condition that makes the employee unable to perform the employee's job.

Military Family Leave Entitlements

Eligible employees with a spouse, son, daughter, or parent on active duty or call to active duty status in the National Guard or Reserves in support of a contingency operation may use their 12-week leave entitlement to address certain qualifying exigencies. Qualifying exigencies may include attending certain military events, arranging for alternative childcare, addressing certain financial and legal arrangements, attending certain counseling sessions, and attending post-deployment reintegration briefings.

FMLA also includes a special leave entitlement that permits eligible employees to take up to 26 weeks of leave to care for a covered servicemember during a single 12-month period. A covered servicemember is a current member of the Armed Forces, including a member of the National Guard or Reserves, who has a serious injury or illness incurred in the line of duty on active duty that may render the servicemember medically unfit to perform his or her duties for which the servicemember is undergoing medical treatment, recuperation, or therapy; or is in outpatient status; or is on the temporary disability retired list.

Benefits and Protections

During FMLA leave, the employer must maintain the employee's health coverage under any "group health plan" on the same terms as if the employee had continued to work. Upon return from FMLA leave, most employees must be restored to their original or equivalent positions with equivalent pay, benefits, and other employment terms.

Use of FMLA leave cannot result in the loss of any employment benefit that accrued prior to the start of an employee's leave.

Eligibility Requirements

Employees are eligible for leave if they have worked for a covered employer for at least one year, for 1,250 hours over the previous 12 months, and if at least 50 employees are employed by the employer within 75 miles.

Definition of Serious Health Condition

A serious health condition is an illness, injury, impairment, or physical or mental condition that involves either an overnight stay in a medical care facility, or continuing treatment by a health care provider for a condition that either prevents the employee from performing the functions of the employee's job, or prevents the qualified family member from participating in school or other daily activities.

Subject to certain conditions, the continuing treatment requirement may be met by a period of incapacity of more than 3 consecutive calendar days combined with at least two visits to a health care provider or one visit and a regimen of continuing treatment, or incapacity due to pregnancy, or incapacity due to a chronic condition. Other conditions may meet the definition of continuing treatment.

Use of Leave

An employee does not need to use this leave entitlement in one block. Leave can be taken intermittently or on a reduced leave schedule when medically necessary. Employees must make reasonable efforts to schedule leave for planned medical treatment so as not to unduly disrupt the employer's operations. Leave due to qualifying exigencies may also be taken on an intermittent basis.

Substitution of Paid Leave for Unpaid Leave

Employees may choose or employers may require use of accrued paid leave while taking FMLA leave. In order to use paid leave for FMLA leave, employees must comply with the employer's normal paid leave policies.

Employee Responsibilities

Employees must provide 30 days advance notice of the need to take FMLA leave when the need is foreseeable. When 30 days notice is not possible, the employee must provide notice as soon as practicable and generally must comply with an employer's normal call-in procedures.

Employees must provide sufficient information for the employer to determine if the leave may qualify for FMLA protection and the anticipated timing and duration of the leave. Sufficient information may include that the employee is unable to perform job functions, the family member is unable to perform daily activities, the need for hospitalization or continuing treatment by a health care provider, or circumstances supporting the need for military family leave. Employees also must inform the employer if the requested leave is for a reason for which FMLA leave was previously taken or certified. Employees also may be required to provide a certification and periodic recertification supporting the need for leave.

Employer Responsibilities

Covered employers must inform employees requesting leave whether they are eligible under FMLA. If they are, the notice must specify any additional information required as well as the employees' rights and responsibilities. If they are not eligible, the employer must provide a reason for the ineligibility.

Covered employers must inform employees if leave will be designated as FMLA-protected and the amount of leave counted against the employee's leave entitlement. If the employer determines that the leave is not FMLA-protected, the employer must notify the employee.

Unlawful Acts by Employers

FMLA makes it unlawful for any employer to:

- Interfere with, restrain, or deny the exercise of any right provided under FMLA;
- Discharge or discriminate against any person for opposing any practice made unlawful by FMLA or for involvement in any proceeding under or relating to FMLA.

Enforcement

An employee may file a complaint with the U.S. Department of Labor or may bring a private lawsuit against an employer.

FMLA does not affect any Federal or State law prohibiting discrimination, or supersede any State or local law or collective bargaining agreement which provides greater family or medical leave rights.

FMLA section 109 (29 U.S.C. § 2619) requires FMLA covered employers to post the text of this notice. Regulations 29 C.F.R. § 825.300(a) may require additional disclosures

For additional information:

1-866-4US-WAGE (1-866-487-9243)

TTY: 1-877-889-5627

WWW.WAGEHOUR.DOL.GOV

Vendor-Paid Trip Policy

Macy's may accept reimbursement (or payment in the first instance) from vendors for any charges relating to a Macy's associate's attendance at a vendor-sponsored business event, meeting or conference (such as travel, lodging, meals or registration costs) under certain circumstances. Any exception to this policy must be approved in advance in writing (electronic or otherwise) by the Office of Compliance and Ethics (officeofcompliance@macys.com).

Vendor-Paid Travel may be approved under the following circumstances:

- The trip must be approved in advance in writing (electronic or otherwise) by an Executive Vice President (or above) of the organization whose associates are attending the event. A copy of such written approval must be sent to the organization's HR Department for purposes of maintaining a record of vendor-paid trips as noted below.
- The purpose of the event is business and any recreational events sponsored by the vendor in connection with the event are incidental.
- Types of business-related events covered by the policy are seminars or education programs relating to a new vendor product or service, a new season's product line, a vendor manufacturing process, a vendor trade show or vendor sponsored industry conference.
- The event is held at the vendor's place of business (or in the same general geographic area in which the vendor is located) and is held in the continental United States.
- Reasonable trip-related charges payable by the vendor are airfare (coach fare), lodging (consistent with Macy's travel standards), meal and reasonable recreation expenses, conference registration costs and local transportation.
- NOTE – if during normal Macy's travel (i.e., expenses for the trip or conference are paid by Macy's and not paid by a vendor), a vendor wishes to take a Macy's associate out for a meal or attend a social event, then the Gifts and Entertainment Policy (which is contained in the Code of Conduct, available on InSite) would apply.
- Trip related charges (including meals) for a spouse or significant other may not be reimbursed or paid by the vendor.
- Only those Macy's associates for whom the event has demonstrable, direct business relevance may attend the event.
- The portion of the event attended by the Macy's associate may not exceed three business days (any part of a day during which the associate attends a business meeting associated with the event is considered one business day).
- The Human Resources Department in every organization will maintain a written record of all such vendor-paid trips taken during a fiscal year, recording all the particulars thereof (names of attending associates; venue, duration and purpose of trip; and amount of charges by associate by type (airfare, lodging, meals, local transportation, recreation) reimbursed by vendor), if known, and submitting the report to the Office of Compliance and Ethics within sixty (60) days following the end of the fiscal year.

Policy Regarding Confidentiality and Acceptable Use of Company Systems

Purpose

While working at or with Macy's, Inc., or one of its subsidiaries (the "Company"), you may have access to certain non-public information ("Confidential Information" or "Internal Use Only" Information, as those terms are defined in the Macy's Information Security Policy, collectively referred to as "Confidential Information" in this Policy, unless more specifically defined for the purposes of particular requirements). In addition, you may have access to Company systems and/or technology (including but not limited to computers, the computer network, voice mail, email, landline telephones, cellular telephones, fax machines, pagers, handheld email devices, and personal digital assistants (PDAs)) and systems connected to the Internet and/or intranet (collectively, the "Systems"), that are used to carry out the Company's business.

This policy governs your use of, and access to, all Confidential Information and the Systems either as an employee of the Company or as an independent contractor or licensee who provides services to the Company and/or uses the Systems. By using or accessing Confidential Information or the Systems, you are agreeing to abide by this policy, as well as all other applicable Company policies.

This policy may not address every issue or question that may arise. You must exercise good judgment, and if you have any questions or concerns (e.g., regarding whether information is confidential or materials are inappropriate or offensive), you should resolve them with your Company supervisor.

Your Responsibility

It is your responsibility to read and to follow this policy, as well as the Macy's Information Security Policy. If you violate any of these policies, you may be subject to disciplinary action, up to and including termination. In addition, access to the Systems may be suspended or terminated without prior notice.

A. CONFIDENTIALITY STANDARDS AND PROCEDURES

The following standards and procedures apply to your use of, or access to, all Confidential Information.

1. All Non-Public Information is Sensitive

Any information that is not generally available to the public that relates to the Company or the Company's customers, employees, vendors, contractors, service providers, Systems, etc., that you receive or to which you are given access during your employment or while you are performing services for the Company is classified as "Confidential" or "Internal Use Only" under the Macy's Information Security Policy. As is set forth in the Macy's Information Security Policy, internal access to Confidential Information should only be granted on a "need to know" basis, and such information should not be shared with third parties without prior approval from your Company supervisor and consultation with the Law Department.

2. Obligations to Maintain Confidentiality

The Company is often obligated under its contracts to maintain information received from or relating to third parties as confidential. Such information also constitutes Confidential Information for the purposes of this policy. Such information may not be disclosed or discussed outside the Company except with prior approval from your Company supervisor and consultation with the Law Department. Disclosing Confidential Information may cause serious and irreparable injury to the Company, and these policies apply to you both during and after your employment or termination of your relationship with the Company.

If you have any questions regarding whether information is Confidential Information, you should treat it as Confidential Information and seek guidance from your Company supervisor.

3. Use and Protection of Personal Data

Company maintains certain information regarding its present and former associates, customers and vendors. Company respects the privacy of this data where it includes personally-identifiable information ("Personal Data"). Personal Data includes names, home and office contact information, social security numbers, driver's

license numbers, account numbers and other similar data. Company is committed to handling Personal Data responsibly and using it only as appropriate for legitimate business purposes. This commitment requires that all Company employees, contractors, and third parties who are granted access to Personal Data by Company follow all policies adopted by the Company for the protection of such data against unauthorized use, disclosure or access. Such policies, including those set forth in the Macy's Information Security Policy, may vary depending on the sensitivity of the Personal Data at issue.

Personal Data may not be shared with any third party without the written approval of your senior Sales Promotion executive or, for support organizations, your Chief Executive Officer.

4. Special Handling for Highly Sensitive Personal Data

You must not send or require others to send certain "Sensitive Personal Data" (including, but not necessarily limited to, social security numbers or other tax identification numbers, credit card numbers, bank account numbers or other account information, passport numbers, or medical information) over the Internet unless the connection is secure and the data is encrypted prior to transmission using the Company approved encryption method. Any transmission, storage, disposal, or other handling of Sensitive Personal Data should be carried out in compliance with the Macy's Information Security Policy, which prohibits the storage of Personal Data on any portable removable storage device (including, but not limited to, USB drives, CDs, etc.). More information regarding storage can be found in Section A.7 - Confidential Data on Public Drives.

5. Sharing Email Addresses

Your email address itself is not considered confidential information but should only be shared with appropriate contacts outside the Company. Customer email addresses are considered Confidential Information, and should not be shared with third parties without prior approval from your Company supervisor and consultation with the Law Department.

6. Email Confidentiality

When transmitting Confidential Information via email, be certain that it is only addressed to the intended recipients. Keep in mind that email may be readily printed or forwarded by the recipient, and be careful to only include content that is appropriate, business-related, and that is not likely to be misunderstood or taken out of context by the recipient or any others to whom it may be forwarded. Information subject to attorney-client privilege (i.e., communications with a lawyer about a legal matter) should be communicated by email only with appropriate disclaimers.

- A message subject to attorney-client privilege should include the following heading: "ATTORNEY-CLIENT COMMUNICATION: PRIVILEGED & CONFIDENTIAL".

If information communicated outside Macy's (external) includes Sensitive Personal Data (defined above), it must be encrypted prior to transmission using the Company approved encryption method. In the event the Company approved encryption method is not an option, the Sensitive Personal Data must be removed from all parts of the email before sending or replying to a recipient. Sensitive Personal Data included in internal email communications also must be encrypted or sent in the form of a password protected attachment. If you are uncertain of the appropriate method of communicating certain information, consult with your Company Supervisor or the Law Department.

Unless you have been instructed to keep messages for a legal matter, all voicemail or email messages no longer needed should be promptly deleted. For more information on email retention, email purges, and email standards, see Section C.3.

7. Confidential Data on Public Drives

Do not put Confidential Information, sensitive data, or privileged documents on public drives or the MyMacy's Portal since these drives may be available to anyone with access to that network. If business requires you to temporarily store Confidential Information on a public drive or MyMacy's Portal, you must

take steps to protect the document from being viewed or altered by unauthorized parties. This may involve password protecting the document, designating it as “read only,” or placing a “write reservation” password on the document. Sensitive Personal Data or privileged documents must not be stored on public drives. In the event business requires you to temporarily store Sensitive Personal Data on a public drive, you must password protect the document.

8. Laptops, Cell Phones, Handheld Email Devices, and other Portable Devices (“Mobile Devices”)

Caution must be exercised when communicating Confidential Information or information subject to attorney-client privilege over portable drives, including, but not limited to, laptops, cellular phones or handheld email devices. Storage of Confidential Information on Mobile Devices should be limited to those instances where such storage is justified by applicable business requirements, and where appropriate security controls, as established in the Macy’s Information Security Policy, have been implemented. Laptops and Mobile Devices may be lost or stolen, and the storage of Confidential Information on such devices creates a security risk that must be mitigated. Sensitive Personal Data should never be communicated using or stored on Mobile Devices.

9. Disclosure of Systems Security Methods

All information and documentation relating to Company security, including but not limited to Company security policies, procedures, audits and risk assessments, constitute Confidential Information. No such information may be disclosed or distributed to any employee without a “need to know” in the normal course of his or her assigned work duties. “Need to know” means that the person needs the information to carry out his or her job duties and, even then, only covers the specific pieces of information needed to do the job. Furthermore, no such information may be disclosed or made available to any third party, except with the approval of an appropriate senior Company executive (Vice President level or above).

B. COMPANY SYSTEMS

The Systems include all systems, applications, media and services that are

- Provided by the Company or accessed on or from Company premises, OR
- Accessed using any Company equipment or service, or via any Company-paid or Company-provided access methods (e.g., remote VPN access or email access on PDA), OR
- Used in a manner that identifies the individual with the Company (e.g., through a domain name or email address on the Internet that is tied to the Company)

Such Systems specifically include but are not limited to: hardware, software, computer networks, email, voice mail, phones, fax machines, intranet systems, and the Internet when accessed using Company equipment or any Company-provided access method.

C. ACCEPTABLE USE OF COMPANY SYSTEMS

This policy applies to your use of, or access to, any Systems. By accessing or using any Systems, you are agreeing to abide by this policy, as well as any additional policies or procedures that may be required by the Company.

1. Use of the Systems for Business Purposes

- a. The Systems are provided to serve business purposes only. They should be used to further the Company objectives that fall within the scope of your duties as an employee, independent contractor or licensee.
- b. Limited occasional use for personal purposes is allowed only if the System is used (i) responsibly, (ii) during your own personal time, (iii) without any expense, burden, or risk to the Company or the Systems, (iv) not in connection with an alternative business enterprise, for financial gain (other than in connection with employee benefits), or for any purpose that is illegal, inappropriate, or contrary to Company policies or procedures, and (v) with the approval of your Company supervisor.

2. No Expectation of Privacy When Using the Systems

You have no expectation of privacy when using the Systems, including voicemail, email, Internet, Intranet, and word processing. Subject to applicable laws, your use of the Systems may be monitored, and all information on the Systems may be monitored, accessed, duplicated, deleted or disclosed at any time without notice to you and without your permission. The Company further has the right to limit, block, monitor, remove, and/or record access by any employee, contractor, or licensee when using the Systems and when accessing any information on the Internet or Intranet.

3. Corporate Email Retention Policy, Automatic Deletion of E mail, and Your Obligations During Lawsuits

You must comply with the Corporate Email Retention Policy. Under that policy, emails are automatically deleted from the Systems after 60 days. If you have a critical business need to keep email for more than 60 days, you must move it to your Business Critical folder or print a copy. Items will be retained in the Business Critical Folder for 1 year from the date they are moved there. Use the Business Critical folder only for emails that are needed for critical business reasons (e.g., meeting notes for ongoing projects, budgets, etc.); do not use it as a storage device for non-critical emails. In the event that you are identified as someone who has information related to ongoing litigation, you will be instructed not to delete any emails related to that case, and the law department will place your email account on a separate litigation server to ensure that your emails are backed up and saved until they are no longer needed for that case. Following all instructions provided in such cases and preserving all records, including emails, is critical.

4. Systems Access Restrictions

a. Non-employee access to the Systems is restricted and may be given only for Company business purposes (e.g., for the development of software or an Intranet page) and only with appropriate approvals and the issuance of a separate user identification and password in compliance with the Macy's Information Security Policy.

Any non-employee who is permitted access to the Systems must agree to abide by this policy and the Macy's Information Security Policy through signature or Company contract.

b. Except for authorized Company representatives, no person may access any other person's voice mail, email, files, or other Systems, and no person may use or access any Systems using another person's user id and/or password. However, in appropriate circumstances where there is a sound business need (for example, to access information needed for an internal investigation or to copy files after an employee is terminated), an Organizational Security Administrator may grant authorization to an appropriate executive to access another employee's voice mail, email, files, or other Systems. NOTHING IN THIS SECTION CREATES ANY EXPECTATION OF PRIVACY OR RESTRICTS COMPANY'S RIGHT TO MONITOR ANY USE OF COMPANY'S SYSTEMS AS DESCRIBED ELSEWHERE IN THIS POLICY.

c. When you are away from your computer, you must either log off or use the Control-Alt-Delete function to lock your computer and prevent any other person from accessing the Systems using your log on.

d. Accessing information, data, and/or files without a legitimate business reason and proper authorization is prohibited. You must not attempt to obtain unauthorized access to any Company System or any protected or restricted file or area on any Company System without approval from the Chairman, President, or CFO of Macy's Systems and Technology, or the General Counsel of the Company. Furthermore, the Systems may not be used to gain unauthorized, illegal, or improper access to any other computer, system, or Web site outside the Company. All access to Company information must comply with the Macy's Information Security Policy.

e. Vendors and independent contractors authorized to access the Systems may only access information on such Systems that has been specifically approved by Company management.

5. Password Management

- a. Passwords are used to secure the Systems. Passwords are not intended to assure employees that messages or information on these systems will be kept confidential or private. The Company reserves the right to reset your password without notice and to revoke your access to some or all of the Systems at any time.
- b. You must protect the confidentiality of your password and change it on a regular basis. You must change it immediately if you think the confidentiality of your password has been breached. You must not share your password with anyone else. In an emergency or when otherwise appropriate, your supervisor may have your password reset.

6. Restrictions Regarding Email and Internet Use

- a. The Systems may not be used to access, create, post, upload, download, or send any information, files, programs, messages, email, or other material that may potentially be inappropriate, offensive, abusive, defamatory, disruptive, illegal, threatening, obscene, or harassing. In addition, Systems may not be used to create or transmit any information or files that may potentially contain sexual implications, racial slurs, or any comments that may offensively address age, gender, race, sexual orientation, religious or political beliefs, national origin, or disability. If you inadvertently access an inappropriate site or information, promptly notify your supervisor and HR representative in writing so that both you and they have documentation reflecting that your action was not intentional in the event that you later are asked about the site or information you accessed.
- b. If you receive any emails from people inside or outside the Company (including, for example, unsolicited emails containing sexually explicit or derogatory materials) that you feel are harassing, offensive, threatening, or inappropriate, notify your supervisor and/or HR so that appropriate steps may be taken to stop such emails in the future.
- c. No employee may send or authorize a third party to send marketing emails without prior authorization from Company's senior management. All marketing emails are approved by properly authorized executives using approved email service providers and following legal requirements for commercial email.
- d. The Systems may not be used in a manner that overloads the Systems (e.g., by sending email to a large group of users unless appropriately authorized and required in the performance of your work duties).
- e. The Systems may not be used for solicitations for commercial ventures, religious or political issues, or outside organizations, except with prior authorization from your CFO or appropriate senior public relations or HR executive.
- f. The Systems may not be used to distribute or publish chain letters or copyrighted or otherwise protected materials. If you receive any chain letters, delete them and do not forward them to anyone else. They overload the Systems and may make others uncomfortable.
- g. The Systems may not be used to participate in Internet discussion groups or chat rooms unless such participation is authorized and is related to your job.
- h. Only the Macy's Corporate Communications Department and designated public affairs executives may make, or authorize others to make, public statements on behalf of the Company.
- i. Do not send emails or other electronic communications that attempt to hide the identity of the sender or represent the sender as someone else.
- j. Only employees who have a business purpose for using the Internet and/or Social Media will be granted access, and that access may be limited. You may apply for Internet and/or Social Media access using the designated electronic form.
- k. Unless authorized by the holder of the copyright, no copyrighted information (e.g., news articles or pictures) may be transmitted or posted on or downloaded from the Internet. Similarly, all non-public information on the Company Intranet is considered Confidential Information and is subject to copyright protection; therefore, it may not be shared outside of the Company without appropriate authorization.

I. Any message or information you send by Company email or on the Internet/Intranet may identify you with the Company; therefore, all such communications must comply with this and other Company policies.

7. Restrictions on Hardware and Software Installation

Only authorized Macy's Systems and Technology (MST) personnel may purchase or authorize the purchase of hardware or software for any the Systems. Only authorized technical support personnel may install hardware, software, or shareware, or copy or delete any software from any Systems. In addition, MST must approve any direct software downloads.

All software and other equipment must be used in accordance with applicable licensing agreements and Company policies. Individual drives may be audited at any time to determine whether unauthorized software has been installed, and, if so, it will be deleted. If you are aware of any misuse of any Systems or software, you must report such misuse to your Company supervisor or MST.

8. Other Restrictions on Copyrighted Material

You may not download, copy from a CD or DVD, or otherwise transfer onto the Systems (including the hard drive of your Company-provided computer) any music, video or picture files or data that is protected by copyright. This includes but is not limited to MP3 files of songs, JPEGs of photographs (other than personal photographs), images from an outside websites, and video clips (other than video clips or streaming video provided by the Company or personal to you). Whenever you need such files or data to perform your job, you must ensure that you have all necessary licenses to any creative work you are transferring to the Systems and using. For assistance, consult with the Law Department.

9. Intellectual Property Rights

Any business procedure, software, program, system, application, Web page, methodology, design, drawing, or other creative work developed by you while you are working as an employee, independent contractor, or licensee at the Company is the property of the Company unless completed on your own non-work time and demonstrably unrelated, as determined by the Company in its reasonable judgment, to the subject and methodology of the areas of your employment, contract or license. The Company shall have the intellectual and other proprietary rights (including patent and copyright rights) in all such works, and you agree to protect the Company's intellectual and other proprietary rights in any such works. You agree that each such work shall be a "work made for hire" under the United States Copyright Act of 1976, as amended. If any such work does not qualify as a "work made for hire," you hereby assign to the Company, absolutely and forever, all rights, title, and interest in and to all copyrights, patents, trade secrets, and other proprietary rights in and to such works throughout the world and agree to record such assignment and enforce such rights.

10. Suspected Computer Viruses

If you learn of any computer virus or other IT security problem, you should contact the MST Help Desk to address it. If you receive a suspicious email and are concerned that it may contain a virus, do not open it; delete it.

11. Caring for Company Equipment

- a. You must maintain the Systems and equipment in good working order. You must contact the MST Help Desk to address any problems or for necessary maintenance.
- b. If possible, label handheld equipment with your contact information (if it's not otherwise obvious) so that it may be returned to you if you misplace it.
- c. When you leave the Company, you must return all Company-provided equipment, as well as Systems access mechanisms or software

12. Reporting Loss of Equipment or Security Breaches

- a. You must protect the physical security of the Systems and equipment and must immediately notify your Divisional Security Administrator and your HR department if you lose or misplace any Company equipment (e.g., a laptop, handheld email device, storage device or cell phone). If any Personal Data was stored on or accessible through those devices, our Security Incident Reporting Procedure must be followed.
- b. If you suspect or learn of any breach or vulnerability in our Systems security (e.g., someone has or potentially has inappropriately accessed any Company System or data) or if you suspect or learn of any loss of customer, employee or vendor information (whether that information is on paper or on a System), immediately report it to your Organizational Security Administrator using the Macy's Security Incident Reporting Procedure. Immediate action is necessary to investigate the incident, address any issues and restore the integrity of our Systems.

13. Blogging and Social Media

You may not blog or access external social media sites while on Company time, unless doing so is part of your job responsibilities. And while what you do on your own time generally is your affair, your conduct, even while off-duty, can reflect on and affect the Company. Although you can engage in legally protected conduct, keep in mind that the rules regarding safeguarding Confidential Information and professional behavior apply. Do not use or disclose any Confidential Information (i.e. trade secrets, business or sales plans, etc.) or violate others privacy rights. Also, never make discriminatory, retaliatory, defamatory, harassing, abusive or obscene comments with respect to the Company, its associates, business partners, customers or vendors. Do not infringe copyright or intellectual property of others. You may be invited to become a friend or associate of someone on social media sites. Feel free to remain silent or say no. You may be asked to provide a testimonial for a friend or associate. If you choose to do so, make sure you are clear that you are expressing your own views and opinions, and that you do not speak on behalf of the Company. And keep in mind that only authorized individuals may speak for the Company on social media. If you choose to interact with postings by or about the Company on external social media sites on your own time, be upfront about who you are, that you work for the Company, that you are expressing your own opinion, and that you are not speaking for the Company.

D. DISCIPLINARY ACTION

Any employee, contractor, or licensee who violates any of the standards, policies, or procedures contained in this Policy may be subject to disciplinary action, up to and including termination of employment or termination of relationship with the Company.

Associate Data Security Policy

In the course of conducting business, you may need to collect and use associates' sensitive personal information. Sensitive personal information refers to data that can be used (or misused) to validate a person's identity or commit fraud, e.g., the associate's name along with his or her home address, telephone number, social security number, date of birth, driver's license or other government-issued identification/passport number, bank, credit or debit card account number, or mother's maiden name. The Company recognizes and requires that reasonable protections must be taken to maintain the confidentiality of sensitive personal information. To that end, the following guiding principles serve as the standards and procedures that you must apply when handling such information. However, these guiding principles cannot address every situation or issue. In some instances, therefore, you must exercise good judgment, and partner with your supervisor and/or Human Resources as needed.

Guiding Principles about Collection and Use of Information

- Only gather sensitive personal information if necessary for an express business purpose. For example, a business license application specifically requests the personal information of an individual. Do not provide more information than an application may require by furnishing a template that includes sensitive personal information that is not requested, or that includes the names of more individuals than requested. This also means reducing the number of officers or agents listed on certain filings, if appropriate.
- Human Resources should be notified in advance of the initial request to gather sensitive personal information from an associate. If appropriate, Human Resources should contact the associate to explain why such collection is necessary.
- Prior to collecting and/or distributing sensitive personal information, determine whether the process can be completed without the information. For example, if a third party process requires the disclosure of sensitive personal information, contact the third party to determine if the Company can be excused from the disclosure, or if alternate information may be provided instead.
- Do not collect or transmit sensitive personal information electronically (i.e., via Lotus Notes, the Internet) unless the connection is secure. Do not move secured information to an unsecured, unprotected format.
- Personal information should be shared on a business "need-to-know" basis only.

Guiding Principles about Maintenance of Information

- Maintain any hard copy records containing sensitive personal information in a manner that ensures confidentiality. For example, records should not be kept in unsecured areas such as desktop or unlocked file cabinet; instead, records must be stored in locked file cabinets or locked offices. If records are not in a locked cabinet, then when leaving the office, even if only for a short while, the office should be locked.
- Maintain any electronic records containing sensitive personal information in a manner that ensures confidentiality. For example, electronic records should be stored on a non-public drive and should be password protected.
- As a customary practice, sensitive personal information should not be stored on portable electronic devices, including, but not limited to, laptops, blackberries or memory sticks. In those rare instances where it is necessary to receive and/or store such information on a portable device, you must apply appropriate safeguards to protect the data and the device. If the device is lost or stolen, you must immediately notify Human Resources.
- Access to and use of any records containing sensitive personal information should be restricted to those on a "need-to-know" basis.

Guiding Principles about Storage and Destruction of Information

- Ensure that records with sensitive personal information that are sent to off-site storage are properly secured. For records containing personal information, on the packaging label designate the department as Confidential Information. Also, ensure that the containers are properly sealed prior to shipping off-site.
- Follow the Company's record retention guidelines and timely destroy all records containing sensitive personal information.
- When sensitive personal information is destroyed, ensure that it is totally destroyed and not recoverable. Paper records must be shredded. Electronic records must be purged from computers, servers and back-up drives. The disposal of sensitive personal information as ordinary garbage, without first shredding, burning, pulverizing, erasing or otherwise destroying the material or medium, is prohibited.
- If the sensitive personal information of multiple associates is maintained in a single electronic document (e.g., a spreadsheet) if an associate's employment ends, the sensitive personal information of that individual should be deleted from the document. Individual's names should also be removed if the person withdraws consent and as officer slates change.

Guiding Principles about Loss, Theft, Improper Access and Inadvertent Disclosures

- In the case of any loss, theft, improper access or inadvertent disclosure of sensitive personally identifiable information, you should immediately notify Human Resources. You may learn of an inadvertent disclosure or theft by a third party, e.g., a letter from an agency to whom the Company transmits personal information. You may also become aware of missing files. If you believe that data within your control has been compromised, you should notify Human Resources immediately.
- If a portable electronic device containing sensitive personal information is lost, stolen or misplaced, notify Human Resources immediately.

Product Safety Policy and Procedure

This is a summary of product safety policies and procedures for complaints about unsafe products reported at our stores.

Customer complaints about products are generally handled by either (1) Risk Management or (2) the Stores and/or Macy's Credit and Customer Service (MCCS). How complaints are handled depends on whether the complaint involves safety. As a general matter, (1) Risk Management handles safety complaints involving bodily injury or damage to personal property, and (2) the stores and MCCS handle all other product complaints or inquiries (e.g., routine returns, quality issues, questions about the product).

The Law

Section 15 of the Consumer Product Safety Act requires that a company report to the U.S. Consumer Product Safety Commission (CPSC) a product that (1) fails to comply with a consumer product safety rule, (2) contains a defect that could create a substantial product hazard, and/or (3) creates an unreasonable risk of serious injury.

Processing Product Safety Complaints At The Stores

When a customer (1) reports a product safety incident as defined above or (2) complains that a product allegedly caused or could cause bodily injury or personal property damage, the sales associate must immediately contact and/or escort the customer to a store manager or the designated Store Executive/Duty Executive. Complaints received through the Company's internet retail sales sites should be referred to the Internet Customer Service team at MCCS.

The designated Store Executive/Duty Executive will handle the complaint by:

- Obtaining and retaining the product in a secured location until the complaint has been resolved. The Security Manager may be required to secure the item.
- Filling out a Product Safety Incident Report and emailing the report to General.Liability.RiskMgt@macys.com or faxing the report to 866-908-2396. Go to the Risk Management section of the MyMacy's Portal for more information: <http://mymacys/sites/enterprise/Stores/Profit/RMHome/Pages/GeneralLiability.aspx>
 - NOTE: If the product is Macy's Private Label Merchandise such as Tools of the Trade, Charter Club, I.N.C. International Concepts, Green Dog, etc., email a copy of the Product Safety Incident Report to the MMG Product Evaluation Team at producttesting@macys.com. Copies of a claim concerning Bloomingdale's Private Label, such as Aqua, should be emailed to Bloomingdale's Risk Management at BlmProductSafety@bloomingdales.com.
- If the customer wishes to return the product, the designated Store Executive/Duty Executive must handle the return transaction. The Sales Associate will NOT process the return.

Processing All Other Product Complaints NOT Involving Safety

The Sales Associate should follow the Company organizational procedures for handling general customer complaints involving non-safety related issues such as routine returns, quality, or product information. Such complaints are handled at the store, by the designated store executives, or referred to the designated Customer Service team at MCCS.