CODE OF CONDUCT

macy's inc

To: Macy's, Inc. Colleagues

Dear colleagues,

At Macy's, Inc., we live by our company values every day. And those values of acceptance, respect, integrity and giving back are instilled in our DNA.

Our Code of Conduct guides us and defines what it means to be a Macy's, Inc. colleague. This important document describes the laws and policies we have in place to ensure the highest standards across our business. It also provides direction on where to go with questions when issues arise, and leads colleagues to the resources and tools needed to ensure we can support one another.

It is imperative for all of us to familiarize ourselves with this Code of Conduct and use it as a guide for our daily work and decision-making. Please speak with your People Leader if you have any questions or concerns.

Thank you for your dedication to our business.

Jeff Gennette
Chairman & CEO

macy's inc

Table of Contents

About This Code **4**

Being Respectful... Our Workplace **7**

Diversity and Equal Opportunity 7

Treatment of Co-Workers 7

Accommodating Disabilities 8

Leave of Absence 8

Health and Safety 8

Lawful Employment Practices 9

Being Loyal... Conflicts of Interest **10**

Certain Relationships 10

Gifts and Entertainment 11

Fraternization 14

Other Employment 15

Being Honest... Company Assets and Information **16**

Company Data and Confidentiality 16

Consumer Data Privacy Laws 18

Insider Trading 19

Information Disclosure and External Communications 19

Business or Financial Opportunities 20

Protection and Use of Company Assets 20

Accuracy and Protection of Company Records 21

Being Responsible... Legal Compliance and Social Responsibilities **22**

Antitrust 22

Intellectual Property 23

Advertising 24

Product Integrity and Purchasing Practices 24

Government Investigations and Contacts 25

Sustainability: Environmental, Social and Governance 25

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

Colleague 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 colleagues, 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 colleagues work. ALL colleagues at ALL levels, referred to here as "we" or "us", are governed by this Code.

What are our responsibilities as colleagues?

Each of us should:

- follow all company policies, including those discussed in this Code and in other materials distributed by the company, such as colleague 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 policies, and
- make the necessary disclosures of any personal conflict of interest as described later in this Code.

Do People Leaders have additional responsibilities?

Colleagues who are People Leaders are responsible for creating a culture in which all colleagues 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 colleagues 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.

Nothing in the Code or the policies it incorporates, is intended, or will be applied, to prohibit employees from exercising their rights protected under federal labor laws, including concerted discussion of wages, hours or other terms and conditions of employment. This Code is intended to comply with all federal, state and local laws, including but not limited to, the Federal Trade Commission Endorsement Guidelines and the National Labor Relations Act, and will not be applied or enforced in a manner that violates such laws.

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 People Leader, AskHR or the Law Department.

As a rule of thumb, when acting on behalf of our company, colleagues 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 on social media?

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 colleagues, 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 AskHR or the Colleague Support Center (1-800-234-6229), 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 colleagues from using their discount for others?

A: Yes, it is a violation of company policy for colleagues 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 People Leader 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 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 colleagues many options.

- Your People Leader – usually a good place to start.
- Your People Leader's Manager.
- Your store manager or the head of your Department or location.
- AskHR or the Colleague Support Center (1-800-234-6229).
- The Office of Solutions InSTORE.
- The Law Department.
- ComplianceConnections (1-800-763-7290).
- Office of Compliance and Ethics (**officeofcompliance@macys.com**)

Most issues can be resolved by direct conversations between the people involved. However, if a colleague 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.

What happens when I raise a concern via 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**.

If a colleague contacts ComplianceConnections by telephone to report suspected misconduct, a live operator from our third party service provider will guide the colleague 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 a colleague 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 report to the right company sources for follow up.

In each case, the reporting colleague will be told how feedback will be provided on the colleague'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 colleagues 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 colleague raising the concern will receive feedback on the outcome.

Being Respectful ... Our Workplace

One of the most valuable assets our company has is its workforce. We strive 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.

What To Do

We must not discriminate against any person on the basis of race, color, ancestry, ethnicity, age, religion, sex (including pregnancy and pregnancy-related conditions), sexual orientation, gender, gender identity, gender expression, national origin, physical or mental disability, genetic information, military and veteran 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 People Leader 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 someone else, we must raise our concerns.

All colleagues must use this link to access, read and understand our company's EEO & Anti-Harassment Policy.

Q: I consider myself a minority colleague. My People Leader has passed me over several times for a promotion. He gave the position each time to colleagues 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 People Leader why he/she hasn't selected you. If, however, you are uncomfortable discussing this with your People Leader, or do not get a satisfactory answer, discuss it with the Colleague Support Center, 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, or
- Treating certain colleagues 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 People Leader, AskHR, Solutions InSTORE, or through ComplianceConnections.

Accommodating Disabilities

The Americans with Disabilities Act protects employees and applicants who have disabilities or pregnancy related conditions and requires that employers provide reasonable accommodations to enable performance of the essential functions of the job. People Leaders are responsible for recognizing when they are on notice of a disability and escalating these issues to Colleague Support. The People Leader Policy Insight on Reasonable Accommodations can be found in AskHR under the Knowledge tab. In addition, People Leaders are encouraged to open an AskHR ticket if they have further questions regarding accommodations. Discrimination and/or retaliation against an individual with a disability is strictly prohibited.

Leave of Absence

If a People Leader becomes aware that a colleague needs time away from work because of a medical issue, a family member's medical issue or any other issue that is not vacation or personal time, the People Leader has an obligation to escalate these issues to Colleague Support. People Leaders must never grant or deny a request for a leave of absence themselves.

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 and Medical Leave Act.

All colleagues must use this link to access, read and understand the form titled "Employee Rights and Responsibilities under the Family and Medical Leave Act."

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, taking safety training as directed (including training related to asbestos containing material) and correcting or eliminating unsafe conditions, if they exist. In the event a colleague becomes injured or ill as a result of their job, we want them to receive prompt medical attention. All colleagues must promptly report any work-related accidents or illnesses to their People Leader.

We also 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 to the appropriate member of the management team or the senior manager on duty at your facility or location.

To maintain a healthy and secure work environment, colleagues 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. Colleagues 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 a colleague's ability to perform his or her job duties, the manager or AskHR 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 People Leader, AskHR 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, accommodations and leaves of absence.

What To Do

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

Those of us who record time worked, manage colleagues 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 or any other offsite location,
- delete or conceal hours worked, including overtime hours, or move hours from one day and/or week to another to eliminate overtime,
- revise a correctly entered time record, or
- fail to take the required meal period and rest breaks, or permit or require others to do so.

Q: I'm an hourly colleague, I've been busy lately, but my People Leader 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 People Leader or contact AskHR. As always, you can also bring your concerns to the company through Solutions InSTORE or ComplianceConnections.

Being Loyal ... Conflicts of Interest

A conflict of interest exists when a personal interest or activity interferes –appears to interfere, or may interfere – with our job duties or our duty of loyalty to our company. We owe it to our fellow colleagues, 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 a colleague or a colleagues family member 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 at the national and local level 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, or someone with whom we have a significant relationship (including relatives by blood, marriage or domestic partnership, individuals who share a household, or individuals who are in a dating relationship)

(i) has a substantial amount of stock or other interest in a business partner or competitor,

(ii) accepts an offer by a business partner or competitor to buy stock on terms not generally available to the public, or

(iii) 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 by contacting AskHR, who may consult with the Office of Compliance and Ethics.
- **We should disclose to the company any conflict of interest (either when providing the annual conflict of interest sign off or by promptly notifying the Office of Compliance and Ethics (officeofcompliance@macys.com) 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 People Leader, make your disclosure to the Office of Compliance and Ethics, and 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 is offering its stock for sale to the public. Although, I do not work directly with the vendor, my friend who is employed by the vendor, 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. Can 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 public violates our policy. Accordingly, you may not accept such an offer even if you are not directly involved in our company's transactions with that vendor.

Gifts and Entertainment

What To Know

We use sound business judgment when making business decisions, and we seek to treat all our 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. It could also cause us to appear to be unfair and dishonest in our dealings.

Gifts or gratuities can take many forms – cash, merchandise, loans or non-cash gifts, such as gift cards, 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
- A colleague 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 $300. If the business partner is not personally participating in the Social Event, then the invitation is a gift subject to the $100 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 $500 in a calendar year, unless we obtain advance written authorization (electronically or otherwise) from the Office of Compliance and Ethics and the colleague's pyramid head. Clearance will be based on, among other factors, the business development value of the Social Event(s).
- Unless authorization is obtained as provided above, a colleague must pay the business partner for the aggregate face value of the Social Events to the extent it exceeds $300.
- If there is uncertainty with regard to the dollar "value" or any other aspect of a Social Event, the colleague 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.

Colleagues 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 colleagues 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.

Bribes and Anti-Corruption

At the extreme end of conflicts of interest are bribery and corruption, which involve offering value with the intent of illegally or unethically influencing behavior. Bribes typically involve government officials. All colleagues and all third parties acting on the company's behalf are strictly prohibited from offering, giving, or receiving a bribe under any circumstances. This applies to every colleague - at every location and at every level. A bribe isn't just a cash payment – bribes can include gifts, discounts, charitable contributions, travel, excessive meals or lavish entertainment. And bribery is also against the law, most notably under the Foreign Corrupt Practices Act, which involves foreign government officials.

It is imperative that we abide by the company's Anti-Corruption Policy and make sure we are following the guidelines of the Gift and Entertainment and Vendor Paid Travel Policies as well. The company's Anti-Corruption Policy is located on the MyMacy's Portal under Legal / Compliance and Ethics / Compliance and Ethics Reference Materials. If you have any questions or concerns, you should contact the Office of Compliance & Ethics (**officeofcompliance@macys.com**).

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 card 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 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 $300, 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 are subject to the $100 limitation.

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 The Magic Kingdom 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 $275. 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 the Office of Compliance & Ethics , as the travel is not to the Vendor's main office. In addition, you should advise your pyramid head of the trip. 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 $300. 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 personal relationship with a colleague or a People Leader with whom we also have a direct or indirect reporting relationship.

What To Do

Colleagues in such relationships must use tact and good judgment. If you have a relationship with a direct or indirect subordinate or People Leader, or with an employee, officer, owner, or director of a current or potential business partner, you must promptly disclose the relationship by contacting the Office of Compliance (officeofcompliance@macys.com), AskHR, or the Colleague Support Center (1-800-234-6229) to determine if some action is needed.

Other Employment

What To Know

While a conflict of interest generally exists if a colleague works for or receives compensation for services from any competitor or current or potential business partner of the company, there are certain exceptions.

Most hourly colleagues in our stores and central/support organizations are allowed to work for competitors while employed by the company. Similarly, commission colleagues are allowed to work for competitors as long as the other employment does not involve commission or incentive-based selling of merchandise similar to that sold at our stores or online. However, colleagues may not work for a current or potential business partner of the company.

Generally, People Leaders, Executives, Human Resources colleagues and Asset Protection colleagues may not work for competitors while employed by the company.

What To Do

The company may conduct an individual review of the circumstances relating to other employment before making a final determination. All questions or concerns about other employment should be discussed with AskHR, the Colleague Support Center (1-800-234-6229) or the Office of Compliance (**officeofcompliance@macys.com**).

In addition, you 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 first getting the approval of the Chief Legal Officer of the company.

All of us are encouraged to serve as a director, trustee or officer of non-profit organizations in our individual capacities, but you must obtain the approval from the Office of Compliance and Ethics before doing so as a representative of the company.

Q: I am a commission cosmetics colleague and would like to make some extra money. I want to get a second job. Is this okay?

A: A second job may be fine, depending on your responsibilities in the other job. For example, a commission cosmetics colleague may work as a cashier at a competitor, but may not sell merchandise on commission if that merchandise is similar to merchandise we sell at our stores or online. Also, you may not work for a current or potential business partner of the company. Finally, there may be a conflict of interest if your second job adversely affects your job performance for the company. You should discuss any potential other employment with your People Leader.

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 colleagues and customers, any work product developed in the course of our employment, and any business or financial opportunity that the company could avail itself of.

Company Data and Confidentiality

What To Know

Data is a critical corporate asset. We use data every day to drive value for our business, our customers, our shareholders, and our employees. As a company, we must ensure our data quality, protect our sensitive data, and collect, maintain and use data responsibly in a manner consistent with our brand values. Failure to handle and protect our data responsibly creates significant risks for the company, such as: loss of customer trust, risk of lawsuits and adverse regulatory actions.

All of the company's data is considered "confidential." This could include business or marketing plans, pricing strategies, financial performance before public disclosure, pending negotiations with business partners, documents that show personal data from present and former colleagues, customers and vendors, social security numbers or customer credit card numbers – in short, information, that if known outside the company, could harm the company or its business partners, customers or colleagues or allow someone to improperly benefit from having this information before it is publicly known. This data can be used only to pursue the company's business interests or in compliance with law or other obligations.

What To Do

All data should be collected, used, maintained, stored, transferred, retained and destroyed in accordance with Macy's, Inc. Data Handling Protection Policy (DHPP), the Data Security Policy, and the Records Management Policy. These polices can be accessed via the Policy Center on the MyMacy's Portal.

The DHPP explains:

- How the company classifies data according to the level of data sensitivity;
- The basic rules governing each class of data; and,
- The requirements on how to handle company data, such as saving files on company public drives.

In performing our duties, we may have access to company data relating to the business, our customers, partners or our colleagues.

We are all trusted to maintain the confidentiality of such company data, whether verbal, written or electronic, and to ensure that this data is not disclosed except as specifically authorized.

Here are some simple rules to follow:

Company data should:

- Follow the "clean desk" standard ensuring confidential information is not left out and is stored in locked file cabinets or drawers when you leave your work area,
- Be clearly marked as "confidential" or following the Attorney-Client Privilege standards where appropriate,
- Be shared only with those who need to see it for legitimate company business purposes,
- Not be sent to unattended fax machines or printers,

- Not be emailed without password protecting or encrypting attached files containing sensitive data,
- Not be discussed where others may hear, and
- Be properly disposed of according to the company's Shred All Policy. For paper, this means shredding. For electronic files, this means proper purging techniques must be used.

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

Nothing in the Code or the policies it incorporates, is intended, or will be applied, to prohibit associates from exercising their rights protected under federal labor laws, including concerted discussion of wages, hours or other terms and conditions of employment. This Code is intended to comply with all federal, state and local laws, including but not limited to, the Federal Trade Commission Endorsement Guidelines and the National Labor Relations Act, and will not be applied or enforced in manner that violates such laws.

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 local technical support team and the Enterprise Information Security Team and/or the Law Department.

All colleagues must use this link to access, read and understand our Policy Regarding Confidentiality and Acceptable Use of Company Systems, as well as, our company's Colleague Data Security Policy.

Q: I am a RTW buyer. My vendor representative 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 Divisional Business Manager or Group Business Manager, 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 colleagues asked if he could write down the credit card numbers for certain clients in a personal notebook for quick reference, with the intent to destroy the notebook at a later point in time. These clients rely on him to ring up merchandise because they are too busy to come into the store. I am concerned that if I do not permit the colleague 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. It is against our Shred All Policy to write customer information down on a piece of paper and subsequently throw it in the trash as this is an insecure collection and destruction method. In addition, credit card information must never be stored on paper, or in any system other than those company systems specifically used for that purpose. Our company has provided both tools and guidance to our sales colleagues to help them to continue providing excellent service to their customers, while at the same time protecting their customers' personal data. You must immediately consult the policies that govern you and your colleagues and seek help from the Law Department to understand Data Handling Protection Policy to understand what is permissible and what is not.

Consumer Data Privacy Laws

What to Know

New international and state data privacy laws such as the California Consumer Privacy Act are in effect. These laws provide customers and colleagues with rights to:

- Know the Personal Information (PI) that the company collects or holds;
- Say no to certain data shares or sales of PI data;
- Request deletion of certain PI.

A customer cannot be discriminated against for exercising these rights. There are significant penalties for an organization's failure to honor these rights. Each colleague has a role in ensuring the company meets our data privacy law obligations.

What to Do

Any colleague that handles customer or colleague data should understand the following; if you are responsible for any system containing customer or colleague data you must:

- Know what PI are in the systems, including your PCs and collaboration platforms.
- Know the type and sensitivity level of data according to the Data Classification Table.
- Follow the Macy's, Inc. Data Handling & Protection Policy (DHPS).
- Complete a Risk Assessment before collecting customer or colleague data or sharing data with any 3rd party. For more information on Risk Assessments, see the Macy's, Inc. Risk Assessment Process on the Macy's, Inc. portal or contact riskassessments@macys.com.
- Limit data collection to what is necessary and approved through a Risk Assessment or policy exception.
- Dispose of data in the approved manner per company Records Management Policy and DHPS .

Responding to Customers about Privacy

If you are asked about customer privacy rights, refer them to the Notices of Privacy Practices available on our websites.

Insider Trading

What To Know

As colleagues, we may from time to time become aware of "material inside information." Colleagues 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, business deals or plans, a change in the dividend, a stock split, a merger or acquisition, disposition or consolidation, changes in directors or senior People Leader officers and changes in control, as well as unfavorable events such as a significant cybersecurity incident or breach. Information is considered to be "inside" or "nonpublic" information until 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 specify 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 colleagues 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 social media 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 Law Department.

Business or Financial Opportunities

What To Know

We as colleagues 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.

Colleagues 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. A colleague'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 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. They form the basis on which we make the required financial disclosure and other public statements about our business, financial condition and results of operations. All such public disclosures must be full, fair, accurate, timely and understandable.

We maintain a comprehensive system of internal accounting practices and controls 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 Policy.

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 People Leader. If we believe in good faith that any such wrongful behavior, inaccurate recording or improper reporting is sanctioned by our immediate People Leader, it should be reported to a senior level manager, 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) by sending an email to **directors@macys.com**. 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 Policy, which can be accessed via the Policy Center on the MyMacy's Portal.

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, we must retain them and must consult with the Law Department on their disposition.

Being Responsible ... Legal Compliance and Social Responsibilities

Our company is committed to conducting its business in full compliance with all applicable laws. We must 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."

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, certain laws apply to our jobs, and we must become familiar with them. Where it is unclear if a particular action would violate applicable laws or our policies, ASK the 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. We believe 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 indirectly, on matters such as prices, markups, markdowns, or any other terms or conditions on which we do business. Such an attempt would not only violate the law, but is also a bad business practice.

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

Agreements with vendors, regarding the prices at which we will sell that vendor's merchandise are prohibited. This includes agreements about sale events, mark downs or clearance prices, as well as the dates on which those prices will go into effect. We also cannot try to get a vendor to agree to stop selling or not sell an item to a competitor though we can try to negotiate exclusives.

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. We can only agree that we won't get our markdown support if we choose to price differently.

While it is not practical to discuss here all of the "Dos and Don'ts" under Antitrust 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 assets 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.

We must use our company's and others' intellectual property only as authorized.

If we violate this, our company may be subject to substantial damage claims.

What To Do

We must not use the intellectual property of others without their permission. This applies to everything from social media posts to the art hanging in our stores.

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

Similarly, if and when the company is permitted to use others' the intellectual property, we must follow the reasonable usage guidelines provided.

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 reviewed by our Law Department.

If any of us makes a discovery, or develops an invention, design, process, creative work, 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. This does not apply if an invention is unrelated to the company's business and did not result from your work for the company. Even in that case, it must be developed entirely on your own time, without using the company's equipment, supplies or facilities.

Advertising

What To Know

Our advertising must be truthful. We want to earn and keep our customers' trust by advertising clearly and accurately, and substantiating our product claims and comparison prices.

Our policy is to comply with all applicable laws, including those that govern pricing, product quality, product information, product availability and shipping, among others.

What To Do

Our offers should be clear, and any restrictions or limitations should be prominently disclosed so that customers get what they expect when they visit our stores or websites.

We also follow our company's advertising guidelines and policies, including the Retail Advertising Guidelines. All members of the Merchants, Planning and Marketing teams and others who deal with pricing must understand and comply with those Guidelines.

Product Integrity and Purchasing Practices

What To Know

We put our customers first by selling quality products and standing behind them and requiring our vendor to do the same, regardless of country of origin.

Our customers trust us to take all the appropriate steps to ensure that the products we sell meet high standards for safety and quality, and are manufactured in a socially responsible manner. To that end, we require vendors to adhere to our Vendor and Supplier Code of Conduct.

What To Do

To safeguard our company's reputation and customer goodwill we must ensure 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 colleagues must identify potential safety and quality issues and follow company procedures to report them promptly. In addition, store colleagues must follow company guidelines related to recalls and returns of allegedly unsafe or defective products.

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

All colleagues 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 colleagues who have or are likely to design or produce merchandise such as colleagues 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 investigations, 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 accurate and truthful formal company responses.

What To Do

If asked to provide information or a response – verbal or written – on behalf of the company for a government request or investigation, promptly notify the Law Department. This helps ensure the company responds timely (information often is needed quickly) and appropriately. Only certain people may formally represent the company, and we must never obstruct, influence, mislead or impede an 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, contact the Law Department

Political Activities

The use of company funds for political activities is heavily regulated 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 Law Department.

Being Responsible... ESG Responsibilities

Sustainability: Environmental, Social and Governance

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, recycle materials, and prevent the waste of valuable resources like water and electricity.

Our company seeks to live up to its value of "Giving Back" by caring for and enriching every community in which it operates. Our 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 Vendors to comply with our Vendor and Supplier Code of Conduct which includes a prohibition against child labor, slavery and human trafficking. The company's Vendor Code of Conduct is located at **https://www.macysinc.com/vendors/code-of-conduct**.

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.

EEO & Anti-Harassment Policy

Equal Employment Opportunity

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

As part of the Macy's, Inc. EEO & Anti-Harassment Policy, all colleagues should enjoy a working environment free from all forms of discrimination and harassment. It is against the company's policy, and the law, for any colleague, People Leader, manager or third party to harass or discriminate against others in the workplace based on race, ancestry, color, ethnicity, age, religion, sex (including pregnancy and pregnancy-related conditions), sexual orientation, gender, gender identity, gender expression, national origin, physical or mental disability, genetic information, military and veteran 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 colleague 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 a colleague's employment;

(ii) Submission to or rejection of such conduct by a colleague 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 a colleague's work performance or creating an intimidating, hostile, or offensive working environment.

All colleagues are prohibited from offering, promising, or granting preferential treatment to any other colleague or applicant as a result of that individual's engaging in or agreeing to engage in sexual conduct. Likewise, all colleagues are prohibited from using any other colleague'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 colleague, 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 includes 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, Inc.'s EEO & Anti-Harassment policy.

Other Forms of Prohibited Harassment

Similarly, a racially hostile working environment may be created by circumstances 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 race, ancestry, color, ethnicity, age, religion, sex (including pregnancy and pregnancy-related conditions), sexual orientation, gender, gender identity, gender expression, national origin, physical or mental disability, genetic information, military and veteran status, marital status, medical condition, or any other category protected by law.

Macy's will not tolerate harassment of any type based on race, ancestry, color, ethnicity, age, religion, sex (including pregnancy and pregnancy-related conditions), sexual orientation, gender, gender identity, gender expression, national origin, physical or mental disability, genetic information, military and veteran 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.

Complaint Procedure

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

- A People Leader or manager;
- AskHR or Colleague Support Center (1-800-234-6229);
- 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 colleague should bring the complaint to the attention of another person or office listed above.

People Leaders must immediately report any complaint of harassment or discrimination to a Human Resources representative by submitting a case via AskHR, or calling the Colleague Support Center at 1-800-234-6229.

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. Any colleague found to have engaged in harassment in violation of Macy's, Inc's EEO & Anti-Harassment policy, will be subject to discipline, up to and including discharge.

No Retaliation

Retaliation in any form against a colleague 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 whose spouse, son, daughter, or parent is on covered active duty or call to covered 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 unpaid 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 colleague'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 the Office of Compliance and Ethics (**officeofcompliance@macys.com**) with a notice to the pyramid head of the organization whose colleague is attending the event.
- The purpose of the event is business and any recreational events sponsored by the vendor in connection with the event are incidental. Attendance at extraordinary recreational events paid for by the vendor (e.g., Super Bowl, NCAA Final Four, US Open, Sundance Film Festival), even in connection with company business, must be approved in advance in writing by the Office of Compliance and Ethics.
- 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 colleague 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 colleagues for whom the event has demonstrable, direct business relevance may attend the event.
- The portion of the event attended by the Macy's colleague may not exceed three business days (any part of a day during which the colleague attends a business meeting associated with the event is considered one business day).

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, and personal devices) 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 People Leader.

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

Information that is not generally available to the public that relates to the company or the company's customers, associates, 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. This includes, for example, customer names, associate social security numbers, vendor terms, account numbers and driver's license numbers. 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 People Leader after 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 People Leader after 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.

Nothing in the Code or the policies it incorporates is intended, or will be applied, to prohibit associates from exercising their rights protected under federal labor laws, including concerted discussion of wages, hours or other terms and conditions of employment. This Code is intended to comply with all federal, state and local laws, including but not limited to, the Federal Trade Commission Endorsement Guidelines and the National Labor Relations Act, and will not be applied or enforced in manner that violates such laws.

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

3. Use and Protection of Personal Data

The company maintains certain information regarding its present and former customers, associates, and vendors. The company respects the privacy of this data where it includes personal information ("Personal Data"). Personal Data includes, for example, customer names, colleague social security numbers, account numbers, driver's license numbers and other similar data – anything that identifies or could be used to identify an individual or household. The company is committed to handling Personal Data responsibly and using it only as appropriate for legitimate purposes. This commitment requires that all company associates, contractors, and third parties who are granted access to Personal Data by the 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 containing customer information or sensitive colleague information, such as social security numbers, may NOT be shared with any third party without first being approved through the Risk Assessment process and approved by the Law Department. A colleague's own wage data and employee data lawfully obtained by association with co-workers is not covered by this policy unless such employee data was surreptitiously obtained from the company's private or confidential records.

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 be not be shared with third parties without prior approval from your People Leader, completion of a Risk Assessment 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 directly 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 People Leader 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 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, Personal Devices, and other Portable Devices ("Mobile Devices")

Caution must be exercised when communicating Confidential Information or information subject to attorney-client privilege over mobile devices, including, but not limited to, laptops, cell phones or handheld 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. Generally, those devices should only be used to access data on Company Systems, and not for direct storage. 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 People Leader (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 People Leader.

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 company-provided programs. 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 Systems, including 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 Enterprise Information Security Team 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 Chief Technology Officer or the Chief Legal Counsel of the Company. Furthermore, the Systems may not be used to gain unauthorized, illegal, or improper access to any other computer, system, or website 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 People Leader 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 abusive, harassing, defamatory, illegal, threatening or obscene, or may otherwise violate the company's Diversity or EEO & Anti-Harassment Policies. For example, 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, gender identity, race, sexual orientation, religious or political beliefs, national origin, or disability. If you inadvertently access an inappropriate site or information, (e.g., pornographic, sexually explicit, gambling, promotes unlawful discrimination or hate, etc.) promptly notify your People Leader and AskHR 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 abusive, harassing, defamatory, illegal, threatening or obscene, or may otherwise violate the company's Diversity or EEO & Anti-Harassment Policies, notify your People Leader and/or **bademail@macys.com** or **bademail@bloomingdales.com** 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 People Leaders 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 Corporate Communications.

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 (i.e. blogs or social media, etc.) unless such participation is authorized and is related to your job.

h. Only the Macy's Corporate Communications Department and designated government 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 Social Media will be authorized to do so, and that authorization may be limited.

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.

l. 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 Technology (MTech) 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, MTech 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 People Leader or MTech.

8. Other Restrictions on Copyrighted Material

You may not download 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 any 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. This does not apply if you develop an invention entirely on your own time, without using the company's equipment, supplies or facilities, that is unrelated to the company's business and did not result from your work for the Company.

10. Suspected Computer Viruses

If you learn of any computer virus or other IT security problem, you should contact the MTech Help Desk to address it. If you receive a suspicious email, do not open it. Please report it either using the Report Phishing button in Outlook, or by forwarding to **bademail@macys.com** or **bademail@bloomingdales.com**.

11. Caring for Company Equipment

a. You must maintain the Systems and equipment in good working order. You must contact the MTech 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 local technical support team, the Enterprise Information Security Team and/or your HR department if you lose or misplace any company equipment (e.g., a laptop, handheld 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 Enterprise Information Security Team 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 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. Contractors or licensees who violate this Policy may be removed from their assignment with the company.

Colleague 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 People Leader 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 a colleague. 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 Microsoft Outlook, 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 a colleague'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.
  - For Bloomingdale's – go to the PNP (Policies and Procedures) tab under the Safety section of the Asset Protection Portal for more information: http://mybloomingdales.net/sites/AP/safety.
  - For Macy's – go to the Risk Management section of the MyMacy's Portal for more information: http://mymacys.net/sites/stores/support/risk-management/GeneralLiability/Forms/AllItems.aspx

  NOTE: If the product is Macy's Private Label Merchandise such as Hudson Park or I.N.C. International Concepts, etc., email a copy of the Product Safety Incident Report to the MMG Product Integrity Team at productsafety@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.