

Business Practices Policy

Ethical Business Practices Policy

This **Ethical Business Practices Policy** was prepared to provide employees, as well as those with whom we do business and the general public, with a formal statement of [name of organization] commitment to the standards and rules of ethical business conduct for its staff. The references to [name of organization] in this document extend to all full time, part time, or contract employees of [name of organization] operating divisions, units and subsidiaries.

All [name of organization] employees are expected to review this policy, and in doing so, agree to comply with the principles of this important policy statement. No policy can cover all of the circumstances or anticipate every situation, therefore, employees encountering situations not addressed by this policy, should apply its overall philosophy and concepts to the situation. If a question still exists in your mind after so doing, the particular circumstances should be reviewed with your supervisor, the Human Resources Coordinator or the President.

Use of Company Funds and Assets

The assets of [name of organization] are to be used solely for the benefit of the Company. Each employee is responsible for assuring that [name of organization] assets are used only for valid company purposes. The assets of [name of organization] include much more than its cash, real estate, furniture, fixtures, equipment and office supplies. [name of organization] assets also include technologies, concepts, business strategies and plans, financial data and other important information about, and related to, our business. These assets may not be improperly used to provide personal gain for employees or others.

Confidential Information

You have already agreed to [name of organization] non-disclosure policy. The protection of confidential business information, including membership-related information and trade secrets, is vital to the interests and the success of [name of organization]. Such confidential information includes, but is not limited to, the following examples:

1. member, customer, purchaser, exhibitor, advertiser, subscriber and prospect data
2. financial data
3. business and marketing material and plans
4. compensation information
5. pending projects and proposals
6. personal and financial information on members, customers, purchasers, exhibitors, advertisers, subscribers and prospects

Employees must dispose of information about [name of organization] members, customers, purchasers, etc., using the secure document disposal (Shred-It) receptacles. Employees must use the utmost care and discretion when handling, working with or filing financial and personal information about its members, customers, purchasers, etc.

Employees who improperly use or disclose trade secrets or confidential business information will be subject to disciplinary action, up to and including termination of employment. In addition, because this information is proprietary to [name of organization], it may not be copied, taken, or used by any employee upon or following termination or resignation.

All employees have agreed that:

1. During the tenure of his/her employment, he/she shall access and use trade secrets only as required to perform the requirements of employment with [name of organization];
2. During the tenure of employment and for a period of five (5) years thereafter, he/she will not disclose, divulge, share, sell, or transfer to any person, including future employers, any trade secrets;
3. Upon the termination of employment with [name of organization], he/she will not retain or take any trade secret, or any copy thereof, from [name of organization].
4. For a period of five (5) years following termination of employment, he/she will not make use of any trade secret of [name of organization].

All employees, as a condition of employment, have acknowledged that breaching the confidentiality of the information described in this section will cause harm and damage to [name of organization], including but not limited to the loss of competitive advantage, loss revenue, increase in costs, and other harm not yet ascertainable. Because the harm to [name of organization] will be material and irreparable, [name of organization] can seek equitable relief, including restraining orders and preliminary and permanent injunctions, in addition to monetary relief for damages.

Conflict of Interest

Since its inception, it has been the intent of [name of organization] to carry on its activities in accordance with the highest ethical standards. This policy is, therefore, a reaffirmation of [name of organization's] expectation that its employees practice the highest ethical standards and exercise complete loyalty to the pursuit of its goals. Any activities which do not serve the best interest of [name of organization] or which favor the personal advantage of another person or business entity are inconsistent with the duties and responsibilities required by [name of organization].

[name of organization] recognizes and respects the right of employees to take part in financial, business and other activities outside of their jobs, provided that these activities are lawful and free of conflicts with their responsibilities as [name of organization] employees.

No [name of organization] employee will take personal advantage of his or her employment by allowing a situation to exist that may be construed as a conflict of interest.

All [name of organization] employees shall scrupulously avoid any conflict between their own respective individual interests and the interests of the [name of organization] organization and its family of companies in any and all actions taken by them on behalf of the [name of organization] in their respective capacities.

Conflicts of interest are, but are not limited to:

- direct financial or those of an immediate family members' interests in a business entity,
- service or product which could be affected by a business decision made by [name of organization], acceptance of any personal gift, services, loans, or promises of future benefits from any person or organization that might benefit because of the employee's or an immediate family member's connection with [name of organization].

All [name of organization] employees will immediately disclose any direct or indirect relationships with any individuals, entities or organizations, either for-profit or not-for-profit, that may be involved with [name of organization] in a formal or informal capacity. Examples of such a relationship may include, but is not limited to, employer-employee relationships, governance relationships, shareholder relationships, contractor-contractee relationships, etc.

In the event any employee and/or an immediate family member may stand to derive a personal gain or benefit from a transaction with [name of organization] or proposes to render or employ services, personal or otherwise, to [name of organization] or may be seen as competing with the interests or concerns of [name of organization], the employee shall immediately give [name of organization] notice of such interest or relationship.

Simply stated, this means that in the case of any transaction involving [name of organization] and a company or organization in which an employee and/or an immediate family member has any financial interest, the employee must do two distinct things:

- 1) he/she must fully disclose any interest in the proposed transaction, and,
- 2) he/she must refrain from any involvement, if so requested, with the transaction.

The disclosure should be made in writing to the [name of organization] President and will be retained in the employee's file. Any changes to the relationship should also be disclosed.

Commissions and Rebates

Purchases or sales of goods and services must not lead to employees or their families receiving personal commissions or rebates. Commissions or rebates can take many forms and are not limited to direct cash payments or credits. In general, if you stand to gain personally through the transaction, it is prohibited. Such practices are not only unethical but are in many cases illegal.

Gifts or Gratuities

Employees may not accept gifts of money under any circumstances nor may they solicit non-monetary personal gifts, gratuities, or any other personal benefit or favor of any kind from suppliers, vendors, customers or members. Employees may accept unsolicited, non-monetary gifts from a business firm or individual doing or seeking to do business with [name of organization] only if the gift is of nominal value -- within the bounds of normal, acceptable business parameters -- or if the gift is primarily of an advertising or promotional nature (logo items). Thank you gifts, intended to be shared with co-workers (such as treats and cookies) are acceptable if they are within the bounds of normal, acceptable social parameters.

Gifts of more than nominal value may be accepted if protocol, courtesy or other special circumstances exist, such as on trips abroad where the exchange of gifts is a customary business practice. All such gifts must be reported to both a department manager and the President, who together will determine if the employee may keep the gift, return it, or whether it should more appropriately become company property.

Entertainment

Employees may not encourage or solicit entertainment from any individual or company with whom [name of organization] does business. From time to time, employees may offer and accept entertainment, but only if the entertainment is reasonable, occurs infrequently, and does not involve lavish expenditures. Offering or accepting entertainment which is not a reasonable adjunct to a business relationship, but is primarily intended to gain favor or influence, should be avoided.

Penalties

Employees who violate the standards of this Ethical Business Practices Policy and object to the disciplinary action or decision, may request a meeting with the Treasurer, Human Resources Coordinator and President. Disciplinary action may range from a written warning to termination of employment.

Travel Policy

The purpose of this policy is to define [name of organization] policies and procedures for the expenditure and accountability of company funds for business related travel expenses incurred by employees traveling for [name of organization] business purposes at the request of [name of organization]. It is expected that anyone traveling at the request of [name of organization] for business purposes exercise prudent judgment when spending [name of organization] funds. In that expectation, this policy is administered in an atmosphere of trust and conservatism.

Travelers are responsible for following the guidelines established in this policy including:

- Travel should be carefully planned in advance and insure the most cost effective use of travel dollars. All travel costs must be conducted within the parameters of the annual budget.
- Requests for reimbursement should be submitted on an [name of organization] expense report form.
- All requests for travel reimbursement must be submitted within 30 days of the date incurred in order to be eligible for reimbursement.

Transportation

Air Travel: All air travel tickets must be purchased using the lowest coach class fare available. Airline selection should not be influenced by traveler premiums. Because well-planned travel is more cost effective, airline tickets must be purchased at least 21 days in advance of travel.

Train Travel: All train travel must be at the coach class fare. The cost of reimbursable train travel may not exceed the cost of a 21-day advance purchase coach class airline ticket.

Car Travel: Travel by personal automobile is reimbursed at the prevailing allowable rate as set by the IRS for distances up to 500 miles. Automobile trips in excess of 500 miles are reimbursable at the equivalent of a 21-day advance purchase coach airfare.

Car Rental: Necessary car rental fees are reimbursable.

Parking, Tolls and Taxis: Parking, tolls and taxi expenses are reimbursable. Travelers should be judicious when selecting a parking garage, avoiding costly short-term or daily parking lots. Since they are more cost effective, shuttle or van services should be used when available and practical.

General Expenses

Meals: Expenses for meals and related expenses, including gratuities, are reimbursable for legitimate business purposes. Every receipt must list the number and names of people the meal expense covers. If the meal was for business purposes, the receipt should also describe the business purpose. No reimbursement will be made for the purchase of alcoholic beverages consumed outside of a regular business meal.

Valet and Laundry: Valet and laundry services are reimbursable only on trips exceeding five days.

Telephone: Only [name of organization] business-related telephone expenses incurred while on funded travel for the Association are reimbursable.

Extending Travel: Travelers on [name of organization] business are expected to conduct business in a reasonably efficient manner, limiting the cost. If the traveler extends a business trip for vacation, pleasure, or personal reasons, only those expenses related to the original business purpose are reimbursable.

Receipts: Receipts should be submitted for all expenses, but are required to be submitted for any one expense totaling \$25.00 or more. Expenses for gratuities and tips should be reasonable in nature and be supported by receipts when possible.

Documenting Expenses: Receipts are needed for all expenses reported on employee expense reports or reimbursement requests. In an instance where a receipt is missing, employees are expected to create a receipt (in memo format) that details the amount, what the purchase was, the date of purchase, and sign it. Your signature on the documentation of the created receipt "stands in" for the receipt; please do not simply note that "receipt is missing" on MBNA statements or expense reports.

For general receipts, please relate the expense to a function, event, conference or department. For meal receipts, please write the names of those present and the event or business meeting that the meal relates to. If the purpose is customer relations, please note that. If the meal receipt is part of a conference expense, please note the conference name and the number of participants. If you have purchased a gift (for a speaker or vendor), please detail the recipient's name and the event that the cost of the gift relates to.

Outside-In Documentation

Check Requisitions forms are no longer used at [name of organization] and do not serve as an acceptable form of documentation to authorize the production of an accounts payable (AP) check. Appropriate *outside documentation* is necessary for the production of an AP check.

Examples of appropriate forms of documentation are:

an Invoice

Vendor's (outside party's) email request, with internal approval

Contracts - copy the page that contains: Payee, dollar amount, remittance address
Simply write the appropriate general ledger (GL) account codes on any invoice/contract/vendor email, sign the document and send it to the Accounting department for payment.

For travel advance requests, please forward your request to your manager for approval. Managers will then forward the approved request to AP.

For postage checks for conference mailings, please email the conference mailing information (meeting name, location, date of conference, calculation of costs, GL account) to [name of organization] Accounts Payable representative. Please be sure to complete the transaction by supplying the Accounts Payable representative with the final statement received from the mail house. That statement details the cost of the postage, [name of organization] advance payments for postage and details either the balance due or credit due back to [name of organization].

For any new vendor (including speakers) used an IRS W-9 form is required. Please provide contact information such as a phone number or email address to Accounts Payable along with the documentation for payment requests.

Technology Policy

Technology continues to play an ever-increasing role in today's office environment. From hardware to software to the Internet, you use technology to help you do your job better. And who is responsible for the technology and how you use it? You are!

The intent of this guide is to provide you with a better understanding of the technology you use every day and the policies you need to be aware of.

Technology covers more than just the machine that sits on top of your desk. It covers the software that runs your machine, the network you are attached to and the Internet that you access. It also encompasses email, your telephone, printers, fax machines and copiers.

Please be sure you understand your responsibility when using technology. If you have any questions, comments or concerns, contact the IT department.

Security

In today's world of viruses, worms and spammers, everyone needs to be aware of security. Security is not the sole responsibility of the technology department. We play a big role in keeping our PCs and network clean, but we need everyone's help. The more you understand about the security, the safer our work environment will be.

Passwords play an important role in today's security. And as you all know, you need a password for just about everything today. When dealing with passwords you will probably have many questions: How do you come up with a password that is both secure and easy to remember? How often do you change your password? Who should have access to your password?

When trying to develop a password, there are several things you should keep in mind:

- Your password should always be more than 7 characters long.
- You should try to use both alpha and numeric characters.
- Never use a family name, nickname, pet's name or anything else that might be guessed by another person, and your password should never be the same as your username!
- Never write your password down and leave it near your computer.
- Never use the same password for both your work and personal account.

Try to use a phrase to help you remember your password. For example, "My dog Kimmie had 12 puppies in May" (mdkh12pim)

Once you have a password, it is very important that you do not keep it forever. This is just asking for trouble. If someone obtains your password, they can cause all kinds of problems. This is why it is important that you change your password on a regular basis. Everyone is strongly encouraged to change his or her password every 3 months. We also suggest that you never share your password with anyone.

Computer Hardware and Software

Staff members are issued a PC and software configured appropriately to match job requirements. Staff members also have access to printers, copiers and fax machines. All hardware and software is the sole property of National Association of Credit Management ([name of organization]) and should only be used for work directly related to [name of organization]. When using hardware and software, please keep in mind the following:

- The hard drive on your machine is never backed up. If for some reason you store any type of file on your hard drive and your machine crashes, all of your files would be lost.
- Do not install any software on your machine. There are licensing issues with software and we need to be sure we have all the appropriate documentation. If you need software, contact the IT department.
- Do not download any files, patches or software from the Internet. Internet files can sometimes contain viruses that could infect our network.
- Never change any settings within your PC's BIOS. The BIOS is the basic input/output system for your PC.

These rules also apply to those of you who have or travel with laptops. When traveling with a laptop, never leave it unattended, even briefly. Due to their size, laptops can be easily stolen. Some of the most common places for laptop theft are airport security checkpoints, hotel lobbies, restrooms, and registration lines. When leaving a laptop in a hotel room, store it away in a secure place like a locked suitcase.

Currently there are desktop and network printers. The network printers are centrally located and are configured to match its components as well as interface with the network. You

should never attempt to change any settings on any printers, as that could affect the printer's ability to function properly. If there is a paper jam, and you are comfortable in your ability to clear it, please do so. If not, please consult with a co-worker who is familiar with the printer or contact the IT department. If an error message appears on the LCD display, please write down the error and then contact the IT department. If your printer displays "low toner", please contact the office manager or the IT department.

Telephones

In addition to a computer, each staff member has a telephone on his or her desk. The telephone is for official [name of organization] use only. One area that is often overlooked is telephone security. How secure is access to your personal voicemail? Without a strong password, not very! As with computer passwords, telephone passwords are equally important. Things to remember:

- Never set your telephone password to the same number as your extension or to a number that might be easily guessed by someone else.
- Remember to change your password every three months.
- Never give your password out to anyone.

If there is a need for you to host a conference call, please make IT aware of your plans. All bills relating to conference calls, excluding teleconferences, are sent from accounting to IT. We need to know who initiated the call, so the bill can be coded by the appropriate department director.

Email

Although your [name of organization] email account is personalized with your name, the email address is the sole property of [name of organization], and is subject to review at any time. Your email can also be subpoenaed as part of a lawsuit.

Email is a convenient and easy way to communicate with people both internally and externally. It's very easy to type a message, attach a document and send it off. One of the major problems with email is SPAM. Things to remember about SPAM:

- If your email address is on a web site or you respond to a newsgroup, your email has been captured by a SPAMMER.
- Never open a message you suspect is SPAM. Doing so confirms to the SPAMMER that your email is valid.

When it comes to your email account, you may have many questions: How long should I keep an email? Why do we have limits on the size of our email account? What can I do to prevent my account from filling up? Some guidelines for email are:

Everyone has a maximum account size for 350 MB. Your mailbox size is made up of your Inbox, Sent Items and Deleted Items.

Your account limits are as follows:

At 250 MB you will receive a warning saying your account is over its limit. What this

actually means is your account is at a critical limit

At 275 MB, you will not be able to send any email.

At 350 MB, your account will be closed. This means you will not be able to send or receive email.

What happens when an employee leaves [name of organization]? Each department manager should ask the departing employee to clean up his or her mailbox before leaving. The employee is the best person to know what needs to be kept and what can be trashed. On the first business day, after the employee leaves, the department head, or someone within the department, must do the following:

- Create an out of office message stating that the employee is no longer with the company and list a contact person who should receive future communications
- Begin to clean out or transfer all relevant emails and contacts to another staff member

Erase and record a new voice mail message stating something similar to the out of office message.

After a period of two months, IT will delete the employee's account.

[name of organization] reserves the right at all times to monitor email.

Mass Email – Outbound

In order to comply with the CAN SPAM Act, before any email is sent, containing advertisements or solicitations of any kind, a hard copy of the finalized email must be given to IT for review to ensure it meets the CAN SPAM requirements. IT will then file that hard copy to ensure we have records of what has been sent, should anyone claim we were not in compliance with the FCC regulation. The hard copy you give to IT should have the actual email being sent out, the target date of the emailing, who it is being sent to, and which email box the email will be sent from.

In an effort to streamline this process, help spread out our large email broadcasts, and have an up-to-date calendar of all these emails to prevent bottlenecks at the Copia machine, please get the hard copy to IT no less than 48 hours prior to the target email date.

Your email broadcasts will then be scheduled. Every effort will be made to hit your target delivery date. However, based on previously scheduled emails, your delivery may be delayed.

Internet Usage

Your use of the Internet is strictly for the sole use of conducting [name of organization] business. [name of organization] reserves the right to monitor, at all times, staff use of the Internet. The following apply to [name of organization] staff when using the company Internet:

- Each [name of organization] employee using the Internet access shall identify themselves honestly, accurately, and completely when corresponding or participating in interactive activities.

- [name of organization] Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or local jurisdiction in any material way.
- Employees have no right of ownership or expectation of personal privacy as to their [name of organization] Internet usage. It is possible to monitor Internet usage, and [name of organization] reserves the right to inspect any and all network traffic and files stored on [name of organization] resources. [name of organization] reserves the right, without notice, to limit or restrict any employee's Internet usage.
- Offensive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using the [name of organization] network, printing, or computing resources. Offensive content includes, but is not limited to, pornography, sexual comments or images, profanity, racial slurs, gender-specific comments, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability, veteran status or any protected status of an individual or that individual's relatives or associates. Any content that may be interpreted as libelous, defamatory or slanderous is prohibited.
- [name of organization] Internet access shall not be used to conduct personal business, play computer games, gamble, run a business, conduct political campaigns, for personal gain, or to take part in any prohibited or illegal activity.
- No employee may use [name of organization] Internet access to post a message to an Internet message board, chat room, "weblog," "listserv," or other Internet communication facility, except in the conduct of official business. Any opinions expressed must include a disclaimer stating that the opinions are those of the author and not necessarily those of [name of organization].
- No employee may use [name of organization] facilities knowingly to download or distribute pirated software or data.
- No employee may use [name of organization] Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program code or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- No employee may install, remove, or otherwise modify any hardware or software for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security measures [name of organization] may have in place.