Information Systems Usage

Overview

This policy defines the appropriate use of various forms of electronic communication at [Company] including, but not limited to computers (personal, lap-top), e-mail, telephones (cellular), voicemail, fax machines, and all online services paid for by the [Company], including the internet and intranet. All electronic communications, including all software and hardware, are and remain at all times the sole property of [Company]. This may also include policies regarding electronic monitoring and recording and computer video cameras.

[Company] property, including computers, electronic mail and voice mail, should only be used for conducting company business and the use of these systems at all times is subject to this policy. This Policy applies to all employees, contractors and others who use the Company's information and communication systems. Not complying with this policy is grounds for corrective action up to and including termination.

Incidental and occasional personal use of company computers and our voice mail and electronic mail systems is permitted, but information and messages stored in these systems will be treated no differently from other business-related information and messages, as described below.

Computers, Electronic Mail & Voice Mail Usage Policy

Although [Company] provides certain codes to restrict access to computers, voice mail and electronic mail to protect these systems against external parties or entities obtaining unauthorized access, employees should understand that these systems are intended for business use, and all computer information, voice mail and electronic mail messages are considered company property.

Information Access & Disclosure

In addition to the policy section, "Access & Disclosure" under "Workplace Policies," [Company] specifically reserves the right to access and disclose the contents of any part of the any communication systems used by a [Company] employee at any time when, in the company's sole discretion and judgment, such actions are warranted. Examples of situations in which the company might elect to seek access to such communications include, but are not limited to, the need to solve technical problems, investigation of possible employee misconduct, harassment or sexual harassment, prevention of unauthorized disclosure of [Company] proprietary information, concerns about personal abuse of any communication systems, and review of communications upon the departure or death of an employee/user. The [Company] may use information regarding the number, sender, recipient and address of such communication for any business reason.

Communication Etiquette

Users of any company communications systems should make their electronic and telephone communication courteous, professional and business-like. Also, it is important to keep in mind that "deleting" a message may not mean that it is deleted entirely from computer or voicemail memory since the sender's or the receiver's network has backup/memory systems in place.

Email

Employers should formally advise their employees that electronic mail (e-mail) is considered the property of the company and, as such, is not considered confidential material to the employee.

An employee's right to privacy is vague at best. The Electronic Communications Privacy Act of 1986 generally bars unauthorized access to electronically stored communications. The Act renders "unauthorized" access or exceeding the scope of authorized access a federal crime. However, the Act expressly permits conduct which has been authorized by an individual who communicated or is the intended receiver of the message and is a user of the voice-mail or e-mail. Thus, one method of limiting potential legal exposure is to conduct only "authorized" searches and retrievals, and to limit the scope of search-and-retrieval efforts to those that are business-related. A well-established written policy regarding the employer's ability to search and retrieve voice and e-mail messages also will assist employers in demonstrating that their conduct is "authorized."

An employer who wishes to retain the ability to access all electronic communication systems - including computers, employee voice mail and electronic mail messages -- should have a clear written policy providing that these systems are company property and should only be used for business purposes.

For better or worse, email is not private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. You must take into account the fact that any email you send may be read by a person (or many people) other than your intended recipient.

Any attachments which contain important or confidential material should be encrypted or password protected.

All messages and files are automatically scanned for viruses before being introduced into the [Company] network, but this does not provide a complete guarantee of protection. All employees have an obligation to be cautious when opening emails and attachments to emails from unknown sources. If you have any doubts about opening an email or attachment, please talk with your [Manager]. Employees may not download software as it may contain viruses that can be harmful to the Company. Employees must contact the [CEO or manager] if they identify any software programs that would be beneficial to the organization prior to any downloads. Any employee who downloads software without prior authorization is subject to disciplinary action up to and including termination.

The next time you see this document, it may be stamped "EXHIBIT A" at the top!

Contracts can be entered into by email in the same way as they are by letter or on the telephone. You must at all times take care to assure that you do not inadvertently enter into contracts which bind the Company by email, and you should be aware that contracts

must only be entered into according to our normal legal procedures.

The use of the [Company] email system may not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job related activities. Furthermore, our email system is not to be used to create any offensive or disruptive messages, for example, sexual implications, racial slurs, gender-specific comments, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability. In addition, the email system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

You must not under any circumstances send messages or attachments whether within [Company] or outside [Company] which are…

- Abusive including the use of foul language
- Bullying or intimidating in content
- Defamatory about any other person or organization
- Discriminatory in any sense (e.g. age, disability, gender, race, religion, sexual or sexual orientation)
- Malicious
- Sensitive or confidential

Any attachments which contain important or confidential material should be encrypted or password protected.

If you receive any such messages from outside the Company, you immediately bring these to the attention of your manager or [CEO]. Sending emails or messages that include any of the above will result in disciplinary action up to and including termination.

Any employee who violates this policy or uses the electronic communication systems for improper purposes may be subject to discipline, up to and including termination.

Internet

The [Company] has put technical measures in place to prevent access to internet web sites which contain explicit, illegal or other inappropriate materials. If you need to access a site which contains such materials for the purposes of your job you must obtain the express permission of the Company.

Much of the information that appears on the internet is protected by copyright. Unauthorized copying or modifying of copyright-protected material, including software, breaches copyright law. Therefore, down-loading software or copyright protected information is not permitted, as it may make you and/or [Company] liable to legal action. If you must download and reprint text from the internet, you must include an active hyper-link back to the authors' website for proper credit.

Confidential Information

Users of any company communication systems must adhere to [Company]'s "Confidential Information & Inventions" Agreement.

You must not use [Company]'s information and communications systems whether alone or in conjunction with any other device to make any unauthorized disclosure or copy of any confidential information belonging to [Company]. The unauthorized disclosure or copying of information belonging to [Company] is likely to be treated as a disciplinary offense and could be reason for termination.

Such confidential information shall include without limitation details of:

- Accounts, invoices, statistical information and other financial reports
- Business contacts, associates, lists of customers and suppliers and details of contracts
- Corporate and marketing strategy, business development plans and forecasts, sales reports and research results
- Details of the employees and officers of [Company] and of the compensation and other benefits paid to them
- Identities of potential customers, partners and suppliers
- Information regarding acquisitions, contemplated developments, joint ventures, offers, presentations, or projects offered or undertaken by [Company]
- Proposals, plans or specifications for the development of the existing products and of new products to be sold or developed
- Sales, expenses, buying and pricing policies including details of percentage mark-up, or profit and discount data

Monitoring & Data Protection

It would be great if you had the capabilities to do all of these things… Delete what you don't need (or leave them in there as a possible bluff to keep your people honest!)

In order to protect the interests of [Company] and to maintain the effectiveness, integrity and security of [Company]'s network, the Company has tools in place to monitor and intercept telephone and email communication and internet use by staff ensuring endpoint security

Monitoring is undertaken using the following automatic procedures:

- Automatic blocking and recording access to certain files and pages on the internet
- Automatic blocking of the connection of unauthorized devices to the network
- Automatic checking of emails and attachments for viruses.
- Automatic measures to prevent software from being downloaded to, installed on or deleted from the Company's computers

- Automatic recording of telephone and mobile telephone call destination numbers
- Monitoring the content of emails, internet use or telephone calls is not routinely carried out but may be carried out in some situations. For example (this is not an exhaustive list):
- Where [Company] has reasonable grounds to believe an employee is breaching this or any other policy of the Company
- Where there is a suspected breach of contract or under-performance
- For the purpose of assisting in the investigation of wrongful acts
- To comply with any legal obligations
- For the purpose of defending or prosecuting any legal action brought against the Company

You should not expect that your personal use of the Company's information and communication systems to remain private.

The holding, processing and disclosure of personal data in electronic form is regulated by the provisions of data protection legislation. Personal information relating to a living individual who can be identified from that information should not be sent by mail unless proper checks have been made to ensure that this will not involve any breach of that legislation.

You must also comply with the [Company]'s Protection Policy.

Security

Employee access to [Company]'s information and communication systems is subject to satisfactory security checks being carried out in the reasonable discretion of the Company.

If you are provided with a portable computer, mobile phone, personal organizer and/or any related or similar equipment, you must ensure its security at all times. You must in particular…

- Always lock mobile equipment when not in use so that it cannot be used without entering your log-on ID.
- Keep your passwords confidential and change them regularly.
- Lock your terminal if you leave it unattended so that it cannot be used without entering your log-on ID, in order to prevent unauthorized users using it in your absence.
- Never leave computer equipment including thumb drives, etc. unattended

If your computer equipment is lost or stolen you must report the incident to the police immediately, and notify your [Manager] as soon as possible. The incident will be fully investigated, and may be treated as a disciplinary issue if you have failed to take adequate

steps to safeguard the security of equipment in your possession.

Passwords

The security and protection of individual passwords is a prime responsibility of the individual owner of the password. ***Passwords should not be shared***. Therefore, if any material is authored out of password-protected system, the presumption will be that the owner of the password is the author of such material.

You must not attempt to gain access to any part of the network to which you are not permitted access.

Software

This may seem redundant, but it's worth repeating and having a clear policy in place to protect the company just in case…

For more information on the issues surrounding software copying, please contact either The Business Software Alliance, at 800 688-2721, or The Software Publishers Association at 202-452-1600

All software used on [Company] communication systems must be purchased and/or approved for use in writing by the [CEO or Information Technology Department]. When software is to be used on [Company] communication systems the [CEO or Information Technology Department] has sole responsibility for the installation and maintenance of same, as well as all registration and licensing matters, and will be the primary contact with the manufacturer or reseller.

[Company] does not condone the illegal duplication of software. The copyright law is clear. The copyright holder is given certain exclusive rights, including the right to make and distribute copies. Title 17 of the U.S. Code states that "it is illegal to make or distribute copies of copyrighted material without authorization" (Section 106). The only exception is the users' right to make a backup copy for archival purposes (Section 117).

The law protects the exclusive rights of the copyright holder and does not give users the right to copy software unless a backup copy is not provided by the manufacturer. Unauthorized duplication of software is a federal crime. Penalties include fines up to and including $250,000, and jail terms of up to five (5) years.

Even the users of unlawful copies suffer from their own illegal actions. They receive no documentation, no customer support and no information about product updates.

- [Company] licenses the use of computer software from a variety of outside companies. [Company] does not own this software or its related documentation and, unless authorized by the software manufacturer, does not have the right to reproduce it.
- With regard to use on local area networks or on multiple machines, [Company] employees shall use the software only in accordance with the software publisher's license agreement.

- [Company] employees learning of any misuse of software or related documentation within the company must notify their [manager / supervisor / team leader / designated company representative] or [Company] legal counsel immediately.
- According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages and criminal penalties, including fines and imprisonment. [Company] employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination.

Computer & Other Equipment Not Provided by Company

See also the section on BYOD (Bring Your Own Device) in the *Manager's Procedures Guide*

You must not connect or attempt to connect any device to the network without express authority from the information systems manager and you should be aware that [Company] has in place automatic measures to prevent this. In particular you should not attempt to connect any of the following devices to the Company's network:

- An unauthorized file or information storage device
- A mobile phone or PDA not issued by the Company
- An MP3 Player or similar device
- A gaming device
- A camera or flash memory card

A breach of the prohibition contained on connecting devices to [Company]'s network is likely to be treated as a disciplinary offense and could be cause for disciplinary action up to and including termination.

Personal Use

Note that a company may/may not allow use of the company email system for personal use. If the company allows limited use the policy below provides sufficient information.

A limited amount of personal use of [Company]'s system is permitted subject to the following rules:

- All personal email messages must make it clear that they are sent in a personal capacity and not on behalf of [Company] and must include in the subject field a statement that the email is "Private"
- All personal emails should be deleted as soon as read or sent.
- Any personal use of email or communications systems must not delay or interfere with the proper performance of the duties of any other employee.

- Where you are in receipt of personal emails you should advise the sender that these may be monitored.
- Work on [Company]'s business must always take priority over your personal use of Company's systems.
- You may not subscribe to any non-job related Internet service or access any web based personal email accounts using [Company]'s systems.
- You may not use the [Company]'s systems to transfer, store or download information and files for your personal use including (but not limited to) MP3, AVI, WMV files and other similar formats.

If your personal email use is excessive or you do not comply with these rules, your access to the system may be curtailed and you will be subject to disciplinary action -- up to and including termination.

Prohibited Uses of [Company] Information Systems

Other prohibited uses of the company information or communication systems include, but are not limited to:

- Accessing pornography or any other illegal material on the Internet and/or circulating it
- Any use that might compromise the operation or security of [Company]
- Connecting an unauthorized device to the network
- Engaging in any communication that is unlawful or in violation of [Company] policy, including (but not limited to) communication that is defamatory, obscene or prohibited by [Company] Harassment Policy;
- Excessive personal use of the company communication systems;
- Excessively visiting non-job related internet sites during normal working day;
- Gambling or engaging in other activities via internet sites in violation of local, state or federal law;
- Introducing a virus to the computer system by downloading an Internet file;
- Sending, forwarding, redistributing or replying to "chain letters";
- Using unauthorized passwords to gain access to another user's information or communications;
- Accessing any [Company] e-mail account (authorization must be given by the [Manager Title]);
- Copying or modifying copyrighted material without authorization;
- Downloading software or files without authorization;
- Using any communication systems for electronic "snooping" i.e., to satisfy idle curiosity about the affairs of others, with no business or legal reason for obtaining access to the files or communications of others (this prohibition applies to users, including [Company] Communication System administrators and managers);

- Using any communication systems to interfere with normal business functions in any way;
- Using any communication systems to solicit or conduct business other than the business of the Company.

Consequences of a Breach of this Policy

Breach of this Policy in your use of the Company's information and communication systems will be considered a serious disciplinary matter and may result in disciplinary action up to and including termination.

Social Media

[Company] encourages employees to participate in Social Media which may include; LinkedIn, Facebook, Twitter, blogging, etc.

Every day, we strive to develop meaningful relationships and look for ways to improve the services we provide. In the past, we've connected with our customers in person, through telephone calls, or in e-mail conversations. Today, social networking tools provide [Company] the opportunity to start a whole new type of dialogue with our current and future clients, and even with each other.

Nothing in these guidelines should be construed as restricting any state or federal rights, including those under the National Labor Relations Act - NLRA. Remember that while social networking is valuable, there are some risks you should keep in mind. In the social media world there often is no line between what is public and private, personal or professional. Non work-related social media is prohibited during work hours.

Policy

These guidelines include a list of things to avoid when communicating with the public via social media.

All social media accounts, blogs, Web pages and related content carrying the [Company] brand identity are and will be owned and licensed by [Company] as appropriate. Personal accounts, blogs, Web pages and related content that do not carry the [Company] brand identity can be owned, licensed and operated by any [Company] employees and/or contractor. However, any and all use of Company's name, logo and/or related marks requires prior, express, written consent of Company. If [Company] is referenced in any media, all social media guidelines apply.

These guidelines should be applied to any online medium where information may reflect back on the image of Company, any Company's employees and/or customers. This Social Media Policy applies to all forms of social media including, but not limited to: blogs, Facebook, Flickr, LinkedIn, MySpace, Pinterest, Twitter, Wikipedia , or other wikis, YouTube, etc. These guidelines apply to any comments [Company] employees may leave on others' social media pages.

Guidelines

- **Be professional**

You represent [Company] at all times. Review the [Company] Employee Handbook. The rules for employee conduct also apply to you in the social world.

- **The Internet knows who you are**

Everything written on the Internet can easily be traced back to its author. Write only things you would say out loud to all parties involved.

- **Promoting other brands with the [Company] brand**

Never promote personal projects or endorse brands, causes or opinions when posting from a [Company] account. Be sure to respect third party copyrights. If a personal opinion must be posted, clearly state to all readers that it does not represent the opinions of Company.

- **Maintain confidentiality**

Respect the privacy of your colleagues and customers. Do not disclose any confidential or proprietary information in regards to [Company] or its customers (e.g., Company's financial information, innovations, marketing strategies, customer information, etc.). This also includes any personal information of employees and others associated with [Company] products / services not be shared or disclosed through social media.

Never mention customer names or talk about specific about projects without first getting permission from your manager. Acknowledging a customer relationship may violate a client privacy agreement. Communications inside Company, including emails among employees, are proprietary to Company. Sharing internal communications outside of [Company] may result in disciplinary action up to and including termination. Never engage in social media on behalf of a customer without their permission, and always abide by our customers' policies. Check with the sender before forwarding or posting any information. Never discuss numbers, sales figures, strategies, forecasts, legal issues, customer names, or future activities online.

- **Respect copyrights**

Confirm that any information you are posting, including work products on document-sharing sites, has been approved for public information and does not violate copyright laws. Do not post any images or content from another source unless you are sure it is in the public domain or that the owner has granted permission. When reposting or referencing a post on one of Company's online sites, you must provide an active link back to the original post or story. Check website terms of service to see if the site has rules about when you may reproduce content.

- **Identify yourself**

When relevant; identify your affiliation with [Company] and your area of concentration, exercise full disclosure.

- **Do not provide public relations related information**

Do not report Company's results or outcomes. Please communicate with your

[Manager/CEO] to identify information to be shared for outside of the company.

- **Private & Personal Information—Yours, [Company] Customers & Co-workers**

To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.

- **Be careful of any offers of advice**

We must not give legal, medical or other professional advice using social media.

When you want to overhaul your employee polices manual...

Whether you're writing your first employee policy manual or updating your previous handbook, EmployeeManualBuilder provides the easiest and fastest way to produce a comprehensive and current HR policies and procedures manual for your company.

Menu-driven from start to finish, EmployeeManualBuilder's organized system gives you a complete employee policies and procedures handbook that has been thoroughly proven by thousands of users and in every state. The text and guidance are all right here, ready for you to easily edit into a customized employee policy handbook for your company. (No copying, pasting or reformatting needed.) You can use Employee Manual Builder as-is, revise any part of it, or copy and paste from other documents. Click to learn more…