[redacted]

[redacted] Enterprise-Wide Electronic Communications Policy

Purpose

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

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

[redacted] expects all users to communicate in a professional and respectful manner.

Scope

This policy applies to all Company associates in every Banner, Region, Office and subsidiary, as well as to contractors, temporary associates and any other persons authorized by the Company to access its electronic communications systems. This policy supersedes all previous versions and any related local Banner or Region-level policies.

Policy

Usage

The Company's electronic communication systems are intended primarily for use in connection with the Company's business. The Company permits occasional personal use of email, telephone, facsimile and the Internet; however, associates should understand that personal use (a) must not in any way interfere with or impede the Company's business, (b) must not interfere with an associates' job performance, (c) must be occasional and minor, (d) must be promptly discontinued at the request of Company management, and (e) is expressly subject to all of the provisions in this Policy, as well as all other applicable Company policies and guidelines.

Associates are responsible for ensuring that the Company's electronic communications systems are not used for any unethical, illegal or improper purpose and will be held accountable for any misuse. The Company's systems should not be used to create or transmit offensive or disruptive messages such as chain letters or jokes or messages containing sexual implications, racial slurs, gender-specific comments or other comments that offensively address a person's age, sexual orientation, religious or political beliefs, national origin or disability. Further, they should not be used to disseminate or intentionally access material that could potentially be defamatory, sexually oriented, pornographic, harassing, threatening, illegal, fraudulent, and offensive or unwelcome to anyone who may view it.

Usage of the Company's electronic communication devices, other than facsimile services, must be authenticated with a username and password or other authentication item, such as a token. The Company utilizes an asset management system to track all devices and personnel having access. Electronic devices will have an asset tag identifying the owner and contact information.

Modem usage must be strictly controlled. Modem will be set to timeout after a specific period of inactivity. Modems used by vendors must be active only when needed with immediate deactivation after use, unless authorized business exception is on file with Enterprise Security.

Privacy/Monitoring

Associates should have no expectation of privacy when using the Company's electronic communication systems and are expected to follow the Electronic Mail Standards set forth in Appendix A to this policy. The Company reserves and intends to exercise the right to monitor, review, electronically scan, audit, intercept, access and disclose all electronic communications and data that are created, sent, received, stored and/or accessed using Company provided electronic communication systems, and does from time to time examine the content of electronic communications. The source of any e-mail message is clearly identifiable and the message may remain part of the Company's business records long after it has supposedly been deleted.

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

Security

Associates must obtain management approval to use the Company's electronic devices using the appropriate request process, check with your management for the correct form. Associates must take appropriate care to safeguard the security and integrity of the Company's electronic communication systems and not deliberately interfere with the Company's access to data stored on the systems or deliberately circumvent the Company's security procedures. Associates are prohibited from using the Company's electronic communication systems in any manner that creates an unreasonable risk of permitting unauthorized outside access to the systems or in a manner that compromises the security and integrity of the Company's network, such as allowing intruders or viruses into the Company's network. Users wishing to download any documents, file or software from non-Company sources must observe the Company's procedures for virus checking and system security. They should also refrain from downloading anything onto the Company network that is not part of the licensed product that [redacted] has paid for. This includes but is not limited to music files, software, or other media. Uploading of Company information to non-Company owned sites, including but not limited to chat rooms, bulletin boards, etc. is prohibited without prior written approval of the Investor Relations Department or the Corporate Communications Department. Persons not employed by the Company may not be given access to, and are not permitted to use the systems unless such access or use has been approved in advance, via the appropriate request process, check with your management for the correct form. If approved by management, then those persons (including contractors and temporary associates) are subject to this Policy.

Unauthorized Copying

Use of the Company's electronic communications' system for unauthorized copying of copyrighted software or content is expressly prohibited. Similarly, proprietary information belonging to other companies must not be placed on the Company's systems without the prior written approval of the Enterprise Information Security Department.

Administration

Administrative decisions and interpretations of this policy are the responsibility of the Company's Human Resources Department and Enterprise Information Security Department and IT Compliance Management. Please contact these departments if you have any questions or concerns regarding this policy.

Related Documents / References

[redacted] Enterprise Wide Information Security Policy

[redacted] Internet Discussion Forum Policy and Internet Usage Standards

APPENDIX A

Subject: ELECTRONIC MAIL STANDARDS

The Company recognizes that electronic mail (e-mail) plays a significant role in the Company's business communications. The standards set forth in this document govern the creation, transmission, duplication, retention and deletion of electronic mail messages and the overall use by associates, contractors, customers and vendors of the Company's electronic mail system. These standards are a part of and should be read in conjunction with the Company's Electronic Communications Policy.

Appropriate Electronic Communication Usage Standards

1. You should structure your electronic communications as you would any professional business communication and in such a manner as to ensure that they do not adversely affect the Company, its public image or that of its customers. Messages must be courteous and respectful. Messages that are derogatory, vulgar or offensively suggestive are prohibited. Personal comments that may be construed as religious, sexual, racial or political commentary are against Company policy and are strictly forbidden.
2. You should not misrepresent, obscure, suppress or replace a user's identity. The user name, electronic mail address, organizational affiliation and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.
3. You should include your signature at the bottom of e-mail messages when communicating with people who you do not know you personally or any time you are sending an email to someone outside of the Company. The signature footer should include your name, position, email address and phone number.
4. To prevent unauthorized parties from obtaining access to e-mail systems, choose passwords that are difficult to guess, change passwords on a regular basis and whenever the password may become known by another person. Regardless of the circumstances, individual email passwords must never be shared or revealed to anyone else besides the owner of the password.
5. Except as otherwise specifically provided, you may not intercept or disclose, or assist in intercepting or disclosing, e-mail communications.
6. E-mail is not private and can be forwarded, intercepted, printed, and stored by others.
7. Always enter a descriptive subject line to enable the recipient to prioritize messages.
8. Check your messages at least daily when in the office.
9. Since every network message takes time to transmit and read, be sure the person receiving the message really needs it.
10. DON'T SHOUT. Don't whisper. Messages in all upper case are hard to read and may be perceived as impolite. Messages in all lower case are hard to read as well. Messages should be grammatically correct and spell check should be run before email is sent.
11. Messages should be deleted after they have been read. Important messages should be saved outside of the electronic mail system for long-term retention.
12. Follow chain of command procedures for corresponding with superiors. For example, don't send a complaint via e-mail directly to the "top" just because you can.
13. Be professional and careful about what you say about others. Email is easily forwarded.
14. Be selective in using high priority designations for e-mail. Remember that email is not always read immediately. If your message really is urgent, a phone call may be more appropriate.

15. The Company email directories will contain addresses for non Company entities. Make sure you do not inadvertently send a message meant only for company associates to outsiders.
16. If you receive a message that has been misaddressed, stop reading as soon as you have realized that the message was not intended for you. Inform the sender and the system administrator of the error immediately and delete the email.
17. Use caution when sending messages to mail groups. Make sure that everyone in the group really needs to review the material you are sending.
18. Be careful when replying to a message that was addressed to a mail list group. Make sure that a response that was intended for the sender only is not inadvertently sent to the entire group.
19. All Internet mail will be scanned for viruses.
20. There is a 25 MB enforced limit on all internal email, 10 MB for external, which includes the attachment, body and header of the email.

Inappropriate Electronic Communication Usage Standards

1. Chain letters may not be sent or forwarded.
2. Jokes that are disruptive or offensive may not be sent or forwarded.
3. Do not provide others with the Company e-mail addresses other than your own. If someone asks for the e-mail address of a specific associate, suggest that they contact the person to obtain the information.
4. Large file attachments (anything over 10MB external/25MB internal) should not be sent via electronic mail. Store the attachment in a LAN group directory and send a message to users indicating where the file can be found. This way you make sure that the recipient really needs this information before network time and server disk space is committed to delivering them.
5. Do not routinely transmit messages without meaningful content.
6. Credit card, protected health information, or confidential or sensitive data should never be sent unencrypted over the Internet.
7. The Internet is a public domain and thereby sharing of any information about the company could be a breach of the Internet Standards and could be subject to disciplinary actions, up to and including termination. Comments about or information on [redacted] may not be posted on Internet sites, including but not limited to chat rooms, bulletin boards, and [redacted] supplied email platforms. Please see the Internet Discussion Forum Policy and Internet Usage Standards.

Email Archive, Retention And Restoration; Size And Attachment Limits

1. Only business critical email messages that are required for business purposes may be archived. Email archives must be stored on the individual's local PC.
2. Deleted email messages will be retained in the mailbox for 7 days from the deletion date, and can be retrieved from the "Deleted" folder. Mailbox data will be backed up for 7 days and stored for disaster recovery purposes only. Individual mailbox data will not be recovered from tape back up.
3. Users of the Company e-mail systems must utilize file servers and local hard disks for long-term storage of e-mail messages that are required for business purposes. Attachments received via electronic mail systems should be immediately detached and stored in a file server directory.
   Email messages will be retained for 60 days unless approved by the Legal and IT Messaging Departments'.Mailbox data will be retained for 60 days from the received date. Exceptions require approval by the Legal and IT Messaging Department.
4. Email file size will be a maximum of 400mb.