

GOLDEN TULIP

ELECTRONIC COMMUNICATION POLICY

Policy Purpose

To maximize the benefits of electronic communications to Golden Tulip and its employees, while protecting the Company and its employees from liability and/or performance challenges due to improper or unauthorized use of the systems made available to facilitate the business of the Company.

Company Property

As a productivity enhancement tool, the Company (including all subsidiaries) provides and encourages the business use of electronic communications (notably the Internet, voice mail and electronic mail). Electronic communications systems owned by the Company and all messages generated on or handled by these electronic communications systems, including back-up copies, are considered the property of the Company. Any attempt to violate, circumvent, and/or ignore these policies could result in corrective action, up to and including termination.

Authorized Usage

The Company's electronic communications systems must be used solely to facilitate the business of the Company. Users are forbidden from using the Company's electronic communications systems for private business activities, personal, or amusement/entertainment purposes. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use. Inappropriate use might result in loss of access privileges and disciplinary action, up to and including termination.

Proper Usage

Employees are strictly prohibited from using Company computers, e-mail systems, and Internet access accounts for personal reasons or for any improper purpose. Some specific examples of prohibited uses include, but are not limited to:

- Transmitting, retrieving, downloading, or storing messages or images that are offensive, derogatory, off-color, sexual in content, or otherwise inappropriate in a business environment.
- Making threatening or harassing statements to another employee, or to a vendor, customer, or other outside party.
- Transmitting, retrieving, downloading, or storing messages or images relating to race, religion, color, sex, national origin, citizenship status, age, handicap, disability, sexual orientation, or any other status protected under federal, state, or local laws.
- Communicating confidential Company information to individuals inside or outside the Company or to other organizations, without specific authorization from management.
- Sending or receiving confidential or copyrighted materials without prior authorization.
- Soliciting personal business opportunities or personal advertising.
- Gambling, monitoring sports scores, or playing electronic games.

User Identification

Where electronic communications systems provide the ability to identify the activities of different users, these facilities must be implemented. For example, electronic mail systems must employ personal user-IDs and

GOLDEN TULIP

ELECTRONIC COMMUNICATION POLICY

associated passwords to isolate the communications of different users. Fax machines that do not have separate mailboxes for different recipients need not support user separation.

User Accountability

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone besides the authorized user or senior management. To do so exposes the authorized user to responsibility for actions the other party takes with the password. Violation could result in discipline of both the authorized user and the person receiving the password, up to and including termination. If users need to share computer resident data, they should use message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (for example, not a dictionary word, a personal detail, nor a reflection of work activities).

No Expectation of Privacy

Employees should expect that the Company might access all information created, transmitted, downloaded, received, or stored in Company computers at any time, without prior notice. Employees should not assume that they have an expectation of privacy or confidentiality in such messages or information (whether or not this content is password-protected), or that deleted messages are necessarily removed from the system.

No Default Protection

Employees are reminded that Company electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. Users should have no expectations of privacy using Company equipment. Unlike written communications, e-mail does not usually have an 'envelope.' Unless the e-mail message is encrypted, you're sending a postcard, not a letter.

Regular Message Monitoring

Contents of electronic communications might be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. The Company reserves the right to disclose any electronic messages to law enforcement officials without prior notice to any employees who might have sent or received such messages. Users should structure their electronic communications recognizing the fact that the Company will, from time to time, examine the content of electronic communications. Because all messages are company records the Company reserves the right to access and disclose any message sent over its electronic messaging systems. The Information Technology Department and Department Supervisors have the right to review the electronic communications of the employees they supervise to determine whether there have been any breaches of security, violations of company policy, or unauthorized actions on the part of the employee.

Statistical Data

Consistent with generally accepted business practice, the Company collects statistical data about electronic communications. For example, call detail reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, Information Technology personnel monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems. If during the collection and review of such information they find questionable, inappropriate or illegal use of electronic communications, they must report their findings to management.

GOLDEN TULIP

ELECTRONIC COMMUNICATION POLICY

Contents of Messages

Workers must not use profanity, obscenities, or derogatory remarks in electronic messages discussing employees, customers, competitors, or others. Such remarks; even when made in jest; might create such legal problems as trade libel, defamation of character, or harassment/discrimination claims. Special caution is warranted because backup and archival copies of electronic mail might actually be more permanent and readily accessed than traditional paper communications. Therefore, transmission of obscene or harassing messages to any individual is strictly prohibited.

Message Forwarding

Recognizing that some information is intended for specific individuals and might not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive Company information must not be forwarded to any party outside the Company without the prior approval of management. Blanket forwarding of messages to parties outside the Company is prohibited unless such permission has been obtained.

Handling Information About Security

Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to an appropriate manager. Users are prohibited from utilizing Company systems to forward such information to other users, whether these users are internal or external to the Company.

Public Representations

No media advertisement, Internet home page, electronic bulletin board posting, e-mail message, voice mail message, or any other public representation about the Company can be issued without prior approval by management.

Archival Storage

All official Company e-mail messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, must be archived/copied to individual user archive files within the Company e-mail facility.

Purging Electronic Messages

Messages no longer needed for business purposes must be periodically purged by users from their electronic message storage areas (including outboxes, in-boxes, and file folders). It's recommended that individual users delete electronic messages stored on the Company's e-mail systems after 90 days. After seven days e-mail which has been sent to 'Trash' will automatically be purged in order to increase scarce storage space and simplify records management and related activities. Voice mail messages are saved for 30 days, then purged. Undeliverable messages are automatically deleted.

Harassing or Offensive Materials

The Company computer and communications systems are not intended and must not be used to exercise employees' right to free speech. Sexually explicit words and images, ethnic slurs, racial epithets, religious or political statements, or anything else that might be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, religious beliefs, or political beliefs may not be displayed or transmitted. Unwanted telephone calls, e-mail, and internal mail messages are strictly prohibited, with violators subject to disciplinary action including termination. Users are encouraged to respond directly to

GOLDEN TULIP

ELECTRONIC COMMUNICATION POLICY

the originator of such messages. If the originator does not promptly stop sending offensive messages, users must report the communications to their manager and the Human Resources department. The Company retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Establishing Electronic Business Systems

Although the Company seeks to aggressively implement Electronic Data Interchange (EDI) and other electronic business systems with third parties, all contracts must be executed by paper documents prior to purchasing or selling via electronic systems. EDI, e-mail, and similar binding business messages must be released against blanket orders, such as a blanket purchase order. All electronic commerce systems must be approved prior to usage.

As an employee of Golden Tulip, I recognize and understand that company's communication equipment and services are to be used for conducting company's business only.

I acknowledge that I have read and understand Golden Tulip's Electronic Communication Policy. I acknowledge that I have read and that I understand this notice.

Employee Name

Employee Signature

Date Signed
