ELECTRONIC COMMUNICATIONS & SECURITY POLICIES (B/D December 15, 2005)

PURPOSE

Banner Corporation and Banner Bank (hereafter Banner) encourage the business use of electronic communications by employees as productivity enhancement tools. Electronic communications include: Banner’s intranet; the Internet; electronic mail (email); voice mail, regardless of what phone system used, including a Banner-owned phone system as well as all phones used for Banner business; facsimile; and any other electronic device, including but not limited to personal digital assistants (PDAs) and flash drives that hold or may hold Banner information. These policies cover matters of company property and ownership of information; authorized usage, including primary usage, Internet usage, and cell phones; privacy and monitoring, recordkeeping, contracts and signatures, security, and employee training among other important issues related to electronic communications and security.

COMPANY PROPERTY AND OWNERSHIP OF INFORMATION

Electronic communications systems, and all messages generated on or handled by electronic communications systems, including back-up copies, are the property of Banner. All information obtained by employees is the property of Banner. As a result, Banner reserves the right to review email and information downloaded from the Internet and to check web sites visited by the employee.

IMPORTANT: All employees and other authorized users should specifically read the section of this policy titled “Privacy and Monitoring” which appears below.

Use of Personally-Owned Computers or Other Electronic Communications Devices for Business Purposes: Banner provides computers, computer access, and/or electronic communications devices, and related resources for employees whose jobs require their use for business purposes. Banner understands that, from time to time, some of these employees may want to use a personally-owned computer or other electronic communications device for business purposes. Such use is allowed subject to these rules:

- Since employees who need to use a computer or other electronic communications device(s) for business purposes are provided them by Banner, any damage, destruction, theft, viruses, etc., to a personally-owned computer or other electronic communication device(s) is a risk (and potential liability or loss) for which Banner will not be responsible.
- Employees who want the ability to remotely log in and access Banner information systems or sensitive information using a personally-owned computer or other electronic communications device must obtain advance permission from their appropriate supervisor and the Banner Bank Support Center.
- No remote access is allowed after a separation from employment.
- At termination of employment, any Banner sensitive information, programs, correspondence, etc., in a personally-owned computer or other electronic communications device(s) shall be copied and returned to Banner and then deleted or destroyed from the personally-owned computer or other electronic communications device(s).
Any questions concerning this policy should be directed to the Banner Bank Support Center. As with Banner’s other policies concerning the use of electronic communications or other property, violations may result in discipline up to and including termination of employment as well as appropriate legal action.

**AUTHORIZED USAGE**

**Primary Usage:** Banner permits the use of electronic communications primarily for business purposes.

**Personal Usage:** Occasional personal use is permissible so long as (a) it does not consume more than a trivial amount of resources, (b) does not interfere with employee productivity, (c) does not preempt any business activity, and (d) does not reduce the performance or response of any business system or Internet access.

Employees should not use Banner’s electronic communication systems for personal charitable endeavors, private business activities, for amusement or entertainment purposes including the download of any files, including but not limited to music, pictures, applications or movies, or for on-line computer journals also known as “weblogs” or “blogs”. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

**Internet Usage:** Employees permitted to use Banner’s resources to access the Internet are representing Banner. As a result, Employees are expected to conduct all activities on the Internet in a professional business manner.

Banner views Internet access as a resource owned and provided by Banner to enhance productivity and communication between employees, business partners, vendors, suppliers and customers. Therefore, Banner permits the use of the Internet primarily for business purposes. Occasional use for personal purposes is permissible, but use of any Internet-based or delivered “pay for use” system is permissible only with your supervisor’s advance written permission. Nevertheless, certain restrictions regarding the use of the Internet will be implemented.

Employees using the Internet to send email must follow all Banner email and electronic communications policies and guidelines.

All Employees must comply with any and all applicable laws and regulations, including but not limited to copyright and trademark laws, as well as Banner’s ethics policies.

Employees must not misrepresent Banner through chat rooms, other public forums, or through email communication or any type of posting, including on-line computer journals. Employees must not publish non-public, confidential Banner material or other sensitive information on any publicly accessible computer system, either through email or the Internet, including on-line computer journals.

As with any Banner record, email/Internet records are subject to disclosure to law enforcement or government officials or others through subpoena or other legal process. Thus, employees should ensure that business information in such messages is accurate, appropriate and lawful.
Employees may not advertise Banner products via the Internet, unless permitted to do so using approved advertising copy.

Before and after joining lists, monitoring news groups, signing up for interactive web sites or web sites with frequent updates, employees should give thought to how much time and Banner resources these activities absorb.

Internet-Based Services – If an Internet-based service requires a User to read and agree to a statement of usage terms and conditions, the Internet-based service should not be utilized before permission is obtained from the employee’s supervisor.

Email Spam – Email “Spam” may consist of advertisements or other messages that are sexual or otherwise offensive in nature. Banner’s email spam filter automatically stops most spam. However, employees are expected to delete any spam messages they may otherwise receive without reading or responding to them. Employees who continue to receive email Spam should contact the Banner Bank Support Center so that Banner can take steps to block the Spam.

**Cellular Phones:** The use of cellular phones to conduct Banner business is permitted; however, safety should always come first. All cellular phone use must be consistent with any federal, state, or local laws or regulations. Employees are strongly encouraged to limit cellular phone use while driving, and particularly in slow, congested or stopped traffic, bad weather, or in unfamiliar areas, and whenever possible only hands-free cellular phones should be used for business purposes.

Traffic or related citations resulting from the use of cellular phones are an employee’s responsibility and are not subject to reimbursement as a business expense.

The use of cellular phones is covered by all Banner policies or rules on electronic communications and security.

**Message Forwarding:** Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, employees using electronic communications should exercise caution when forwarding messages.

Banner’s sensitive information must not be forwarded to any party outside Banner without the prior approval of a Banner officer.

Blanket forwarding of messages to parties outside Banner is prohibited unless the prior permission of an appropriate senior/executive officer has been obtained.

**Use, Copying, or Dissemination of Software or Other Materials:** Users may not use Banner email or electronic communications systems to download software unless they comply with established policies. Users may not install software (except software supplied by Banner or on any Banner approved list), games, or screen savers on their computers without first receiving authorization from the Banner Bank Support Center and their immediate supervisor.

Use, copying, or dissemination of software or materials, including but not limited to articles, books, music, or movies, in violation of any license agreement, copyright or other legal
restrictions is absolutely prohibited. Employees with any questions on this subject should check with the Banner Bank Support Center and their immediate supervisor before putting Banner at risk — and subjecting themselves to possible disciplinary or other action.

**Harassing or Offensive Materials:** Employees must not use profanity, obscenities, or derogatory remarks in electronic mail or voice mail messages discussing employees, customers, competitors, or others. Such remarks – even when made in jest – may create legal problems such as trade libel and defamation of character. Special caution is warranted because back-up and archival copies of electronic mail or voice mail may actually be more permanent and more readily accessed than traditional paper communications.

Employees are prohibited from using the Internet to inappropriately discuss confidential Banner information; access pornographic or obscene materials; express personal opinions on political, social, inflammatory, or volatile subjects; exchange taunting, threatening, or otherwise hostile language with another Internet user; or exchange language which is racist, sexist or inappropriately sexually explicit.

Banner computer and communications systems are not intended to be used for, and must not be used for the exercise of the employee’s right to free speech. Sexual, ethnic, and racial harassment – including unwanted telephone calls, electronic mail and internal mail – is strictly prohibited and is cause for disciplinary action including termination. Employees shall report any communication of harassing or offensive material to the Human Resources Director or another member of the Watch Committee. Banner retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Put simply, these computer and communications systems should not be used in any manner and/or for any purpose that would violate the letter and/or spirit of our policies titled “Equal Employment Opportunity and Unlawful Harassment Policy: No Tolerance”.

**Public Representations:** No media advertisement, Internet Home Page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about Banner may be issued unless it has first been approved by the Marketing Director or an appropriate member of Executive Management.

Although an employee may not intend to represent Banner with personal email, phone calls, or facsimiles, the “@.com” suffix, caller ID, or facsimile address may suggest such a representation to some. Therefore, the standard for communication is the same as Banner would expect for customer interactions on the floor, over the phone, or on Banner letterhead. Banner may initiate disciplinary action if an employee misuses this power to speak with the voice of Banner.

**PRIVACY & MONITORING**

**Electronic Communications – No Privacy:** No employee has any right or expectation of privacy in any information file maintained in or on Banner property or accessed, transmitted, downloaded, or stored in its computer systems, voice mail, email, Banner service provider owned systems or other technical resources. Employees have no personal privacy rights in any
material created, received, stored or sent through these systems. Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications.

**Intrusion or Attempted Intrusion:** Intruding or trying to intrude into folders, files, work, networks or computers of others or intercepting communications intended for others without appropriate authorization normally will result in disciplinary action, up to and including immediate termination, and may also result in civil or criminal prosecution.

**Electronic Communications Monitoring:** To ensure that the use of electronic communications systems and equipment is consistent with business purposes and these policies, Banner has the absolute right to monitor, access, retrieve and/or review these files or records at any time without advance notice or permission. Banner is also responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications. Banner reserves the right to access and disclose as it deems necessary and appropriate all messages sent over its email or voice mail system, without regard to content. Thus, employees should not send – or allow others to send them – messages that they would not want read by a third party and/or which could violate any Banner policies. Further, electronic communications may be subject to review by third parties, including but not limited to Banner’s legal counsel, accountants, consultants and regulatory agencies.

**Statistical Data:** Consistent with generally accepted business practice, Banner may collect statistical data about electronic communications. As an 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, technical support personnel monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.

**Incidental Disclosure:** It may be necessary for technical support personnel to review the content of an individual employee’s communications during the course of problem resolution. Technical support personnel may not review the content of an individual employee’s communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

**RECORDKEEPING**

**User Back-Up:** If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a Banner management decision, it should be retained for future reference. Most electronic mail messages will not fall into these categories and accordingly can be erased after receipt.

Electronic mail systems are not intended for the archival storage of important information. Important stored electronic mail messages can be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.
Archival Storage: All official Banner electronic mail messages, including those containing a formal management approval, authorization, delegation, or handling over of responsibility, or similar transaction, must be printed and retained as hard-copy records.

Purging Electronic Messages: Messages no longer needed for business purposes must be periodically purged by users from their personal computers. The systems administration staff, with approval of the Chief Information Officer, may delete electronic message storage in multi-user systems.

CONTRACTS & SIGNATURES

Establishing Electronic Business Systems: Although Banner seeks to implement Electronic Data Interchange (EDI) and other electronic business systems with third parties; all contracts must be formed by paper documents prior to purchasing or selling via electronic systems. EDI, electric mail, and similar binding business messages must therefore be released against blanket orders, such as a blanket purchase order. The Chief Information Officer and Chief Operations Officer in consultation with legal counsel as appropriate must approve all electronic commerce systems contracts prior to usage.

Written Confirmation of Contracts: All contracts formed through electronic offer and acceptance messages (EDI, electronic mail, etc.) must be formalized and confirmed with executed written documents within thirty days of acceptance.

Scanned Signatures: Employees must not employ scanned versions of hand-rendered signatures to give the impression that the sender signed an electronic mail message or other electronic communications.

SECURITY

Handling Information About Security: Employees must promptly report all information security alerts, warnings, suspected vulnerabilities and the like to the Banner Bank Support Center. Employees are prohibited from utilizing Banner systems to forward such information to other users, whether the other users are internal or external to Banner, with the exception of their immediate supervisor, Banner’s Security Officer or the Internal Audit Department.

User Separation: Where electronic communications systems provide the ability to separate the activities of different users, these facilities must be implemented. For example, electronic mail systems shall employ personal user ids and associated passwords to isolate the communications of different employees.

Fax machines that do not have separate mailboxes for different recipients need not support such user separation.

User Accountability: Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Security token Personal Identification Numbers (PINs) should not be shared with anyone except with authorized user security administrators within the Banner Bank Support Center. To do so exposes the authorized user to responsibility for actions the other party takes with the password. If employees need to
share computer resident data, they should utilize 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, employees must choose passwords, which are difficult to guess (For example, not a dictionary word, not a personal detail, and not a reflection of work activities.)

**User Identity**: Misrepresenting, obscuring, suppressing, or replacing a user’s identity on an electronic communications system is forbidden. 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 posting. Banner reserves the right to assign a pseudonym if appropriate.

**No Default Encryption/Password Protection**: Banner’s electronic communications systems are not encrypted by default. Any electronic communication or other transmission that contains customer or corporate information and is being sent to destinations outside of Banner’s control should be encrypted or password protected.

Fax and voicemail communications are excluded from this policy; however, care must be taken to ensure confidential information is being sent to the intended destination.

**Removable Storage Media - Compact Discs/Floppy Disks/Other Removable Storage Media**: In order to protect our system against a virus or other malware, all removable storage media from outside our enterprise or from Banner laptops must be checked by virus detection software prior to usage.

**Internet Security**: The Board of Directors and Management recognize that the Internet is inherently insecure. By design, it is an open network that facilitates the flow of information between computers. Furthermore, the Board understands that Internet risks will not remain static. As technologies evolve, security controls will improve, however, so will the tools and methods used by others to compromise data and systems. The Board is committed to implementing comprehensive security controls and updating them to guard against current and emerging threats and will continue to operate Banner in a safe and sound manner.

The Board also recognizes that use of the Internet presents numerous issues and risks that must be addressed. While many aspects of system performance will present additional challenges to Banner, some will be beyond its control. The reliability of the Internet continues to improve, but situations including delayed or misdirected transmissions and operating problems involving Internet Service Providers (ISP's) could also have an effect on related aspects of Banner’s business.

The Board appoints the Chief Information Officer as the officer responsible for Internet security.

The Information Security Oversight Committee will develop policies and procedures subject to review and approval by Senior Management and by the Board that will include, but are not limited to the following areas:

- Data Privacy and Confidentiality
- Data Integrity
• Authentication
• Non-repudiation – Non-rejection of Validity
• Access Control/System Design

It is Banner’s policy to use a monitored firewall and Internet security systems provided by a third party vendor.

All Employees must take great care when accessing information of any kind from the Internet. It is Banner’s policy to employ anti-virus and anti-Spyware software that continuously monitors all files accessed. It is also Banner’s policy to employ encryption and firewall software on laptops. Employees will be personally accountable for accessed information. Employees are prohibited from disabling their virus and Spyware protection software as well as encryption and firewall software on laptops.

Employees who suspect that their computers are infected must contact a supervisor and the Banner Bank Support Center immediately and cease use of the suspected infected computer.