Banner Health

Title: **IT Acceptable Use Policy**	
Number: 504, **Version**: 6	**Original Date**: 07/12/2017
Effective: 04/24/2023	**Last Review/Revision Date**: 04/24/2023
Next Review Date: 04/24/2024	**Author**: Cybersecurity GRC
Approved by: PolicyTech Administrators	

Discrete Operating Unit/Facility:
Banner Baywood Medical Center
Banner Behavioral Health
Banner Boswell Medical Center
Banner Casa Grande Medical Center
Banner Churchill Community Hospital
Banner Del E Webb Medical Center
Banner Desert Medical Center
Banner Estrella Medical Center
Banner Fort Collins Medical Center
Banner Gateway Medical Center
Banner Goldfield Medical Center
Banner Heart Hospital
Banner Ironwood Medical Center
Banner Lassen Medical Center
Banner Ocotillo Medical Center
Banner Payson Medical Center
Banner Thunderbird Medical Center
Banner—University Medical Center Phoenix
Banner—University Medical Center South
Banner—University Medical Center Tucson
East Morgan County Hospital
McKee Medical Center
North Colorado Medical Center
Ogallala Community Hospital
Page Hospital
Platte County Memorial Hospital
Sterling Regional MedCenter
Torrington Community Hospital
Washakie Medical Center
Wyoming Medical Center

Banner Corporate

Ambulatory Services
Banner Health Clinics
Banner Imaging Services
Banner MD Anderson Cancer Center
Banner Surgery Centers
Banner Urgent Care Centers
Occupational Health/Employee Services
Rural Health Clinics
The Orthopedic Clinic Association (TOCA)

Banner Home Care and Hospice

Insurance
Banner Health Network
Banner Plan Administration
University Physicians Health Plans

Banner Pharmacy Services

Post-Acute Care Services

Research

Table of Contents

I. Purpose

A. The purpose of this policy is to outline the IT, Cybersecurity and Privacy requirements for the acceptable use of Banner Health ("Banner") Information, electronic and computing devices, and network resources.

B. Banner established this Policy to:

- Protect against inappropriate use of Banner's Assets.
- Reduce exposure to risks, including Virus and Ransomware attacks, and compromise of network systems and services, as well as comply with regulatory requirements.

II. Scope/Population

A. **Scope**: This policy applies to Workforce Members who use Banner Health computing devices, data, or network(s) to conduct business or interact with internal networks and business systems.

B. **Population**: The population applies to the entire Banner Workforce.

III. Definitions

A. The definitions of terms and acronyms that are used in this document may be found in the IT Glossary.

IV. Roles and Responsibilities

Roles	Responsibilities
Cybersecurity	• Refer to Banner IT Roles and Responsibilities Guide
Service Desk	
Workforce Members	

V. Policy

A. General Acceptable Use

1. Banner Information will be protected from unauthorized access with appropriate safeguards, as defined by IT.

2. Workforce Members are responsible and accountable for their use of Banner Resources. Workforce Members will:

   a. Acknowledge Banner's policies and Banner's Code of Conduct prior to, or within ninety (90) days of, commencement of employment or engagement, and comply with such policies and Code.

   b. Sign the appropriate confidentiality agreement(s) before accessing Banner Information. These may include a Non-Disclosure Agreement (NDA), a Business

Associate Agreement (BAA), or other agreements as required by Banner, its counsel, regulations, and/or local, state, or federal laws.

c. Comply with applicable Banner policies when accessing Banner Information and Banner Business Tools (Business Tools).

3. Use Business Tools for official business purposes; limited personal use of Business Tools is acceptable, provided this use does not interfere with the performance of one's job duties, the efficient operation of Banner networks or devices, or otherwise violate Banner policy or introduce risk.

4. Ensure the confidentiality of Banner Information that may be displayed on their screen in public locations by using discretion and privacy screens,. Banner does not currently provide privacy screens to all users so it is the responsibility of the user to obtain a privacy screen from Banner if accessing Banner data in public locations.

5. Ensure Business Tools are not left unattended in unsecured areas to avoid theft or loss of the device.

6. Report potential IT, Cybersecurity and Privacy issues to the Service Desk immediately. Examples include, but are not limited to:

   a. Detected viruses or malware.

   b. Phishing emails.

   c. Loss of Banner's Assets, including Personally-owned Devices that may contain Banner Information.

   d. Evidence of improper viewing, modification, or inappropriate or unauthorized access to Information or Business Tools.

7. Be aware of, understand, and acknowledge that Banner reserves the right to monitor Banner-owned devices, Business Tools, Electronic Communication, and network traffic for security, compliance, performance, or for other business reason , subject to compliance with applicable privacy laws and regulations.

8. Acknowledge and accept that Banner reserves the right to disconnect, modify, wipe/delete, secure, create backups, or perform eDiscovery/forensics analysis on a device, whether Banner-owned or not, that contains Banner Information.

9. Banner Information stored on hardware or electronic media, whether leased or owned by Banner, a Workforce Member, or a third-party remains the sole property of Banner.

10. When electronic Confidential Information is printed, the paper copies will be treated with an appropriate level of security based on the document's classification level, as outlined in the IT Data Classification Standard, and securely disposed of when no longer needed.

11. Workforce Members are prohibited from engaging in prohibited use of data using Business Tools, devices, or network.

Reference: NIST 800-53 CM-11, PL-4, PS-6

B. Working in Secure Areas

1. Banner Workforce Members will adhere to the following while working in secure areas:

    a. Understand the specific instructions for secure areas to which they are granted access.

    b. Question and/or report anyone not wearing an ID.

    c. Remain vigilant while within the secure area.

    d. Always escort their authorized visitors after confirming that they have signed in.

    e. Inspect their deliveries as soon as possible.

    f. Check that doors and windows are secure before leaving if they are the last ones out of the secure area.

    g. Not disclose information relating to the secure area other than on a need-to-know basis and as authorized.

    h. Not allow anyone to tail-gate behind through a secure entry point.

    i. Not keep secure doors open for longer than necessary.

    j. Not allow its guests to work in the secure area on their own without appropriate management authorization.

    k. Not lend anyone their ID cards.

    l. Not expose their ID cards to possible theft or loss.

    m. Not tell or share with anyone their passwords, Personal Identification Number (PIN) or One Time Password (OTP) codes.

    n. Not write down passwords, PIN or OTP codes.

    o. Not use photographic, video or audio recording equipment within the secure area unless there is a business need approved by Banner Security and/or IT leadership.

Reference: NIST 800-53 PE-3

C. Banner-Owned Computer Use

1. User Adherence

    a. Workforce Members will surrender Banner-owned devices and property (including, but not limited to computers, mobile devices, and access badges) and/or remove Banner data from personally-owned devices upon transferring within or leaving the company: provided, however, that, Banner reserves the right to remotely wipe and delete all data (including personal data) on Banner-owned computers and other

Banner-owned devices; and all Banner data on personally-owned devices that have access to Banner Information.

b. Administrator privileges on Banner-owned devices will be allowed only if required by business needs, documented, and approved by the Head of Department and Banner's IT.

c. Banner may at any time and without notice:

   i. Audit the Workforce Member's Banner-owned device and data, to include network security requirements, to investigate compliance and legal issues, to investigate and preserve information relevant to litigation or potential litigation, and other legitimate business reasons deemed appropriate by Banner; and

   ii. Require the return of a Banner-owned device and associated equipment.

d. Workforce Members will lock their workstations (Windows key + L for Windows) when they are away from their workstations.

e. Workforce Members will save data to network drives where it will be automatically backed-up for them.

f. Files received from anywhere outside Banner will be virus-checked before they are opened. This includes files on CD or USB drive. This will be performed by automated tools such as anti-virus software or other security software already installed on the assigned workstation.

g. If Workforce Members suspect that their computers may have a virus, they will leave the computer on, unplug the network cable, or disconnect from the wireless connection and call Banner's Information Technology Service Desk.

h. Workforce Members will ensure that computers are supported via an approved anti-virus system. Workforce Members may receive the latest updates by connecting to the Banner network. Workforce Members will contact Banner's Information Technology if they are unsure whether their computer has received relevant updates.

i. Incidents of virus/malicious code detected by anti-virus software will automatically be reported to Banner's Information Technology.

j. Authentication (e.g., passwords, security tokens, biometrics) and encryption (where available) to protect access to Banner's Information Systems and electronic documents is required.

k. Workforce Members will not allow anyone else to use their Banner computers at any time.

l. Workforce Members will never install software on a Banner-owned device, with the exception of some business-related software to participate in vendor or other Banner business partner meetings. For example, Banner computers will allow certain meeting web-based temporary access to software (not downloaded to the device) such as Zoom and Cisco Webex. Installation of all software on a Banner computer will be blocked and can only be installed by Banner's Information Technology.

m. Workforce Members will not disable or uninstall the software that is installed on a Banner-owned device by Banner's Information Technology.

n. Unless specifically authorized by IT, inherently allowed by the Banner computer configuration, or a specific exception, Workforce Members will not connect any personally-owned devices to a Banner computer for any reason.

o. Workforce Members will not play music CDs on a Banner computer because they can install unwanted software on the computer.

p. Workforce Members will not store non-business-related data such as personal photographs, music, and video files on a Banner-owned device or in Banner-owned storage facilities.

q. Immediately notify the Service Desk of lost, stolen, or potentially compromised Banner-issued and owned devices.

2. Security Safeguards

    i. Computers and applications with access to Banner's network and/or Information will be configured to time out in accordance with Cybersecurity thresholds. Workforce Member computers will be configured to automatically lock after 15 minutes of inactivity unless there is an applicable Federal or state regulatory requirement that is more restrictive, determined and communicated by IT.

    ii. For applications accessing Confidential Information, session timeout will be 15 minutes.

    iii. Banner applications that contain Banner Confidential data such as electronic Protected Health Information (ePHI)/Cardholder Data (CHD) and similar, as well as Banner web email will timeout (wherein the browser closes) after 15 minutes of inactivity.

3. Information Storage and Protection

    a. Banner prohibits the copying, moving, or storing of PHI/ ePHI and/or CHD onto local hard drives (c:\drive), unencrypted removable Media Devices, and non-approved Banner cloud storage.

    b. Banner Information (other than PHI or CHD) stored on local hard drives or other removable data storage media (e.g., external hard drive, etc.) will have appropriate administrative, technical, and physical safeguards applied, including use of Banner-approved encryption methods, in accordance with Banner's Cybersecurity Encryption Standard.

    c. The only cloud-based storage solutions (e.g., Microsoft OneDrive) that can be used to store Banner Information must be approved by IT.

    d. Workforce Members will store Non-Public Information in approved designated network storage locations.

4. Removeable Media

    a. Use of Removable media may be permitted only where there is a clear business case for use and this case has been approved by the Director (or above) for the applicable Workforce Member and Banner Information Technology.

    b. If use of removable media is approved, the Workforce Member authorized to use such media:

        i. Must use such removable media in a secure manner in accordance with this policy;

        ii. Must return the removable device to IT per policy; and

        iii. Must take special care to physically protect the removable media device and stored data from loss, theft and/or damage.

    c. Workforce Members will not copy Banner Information from a removable media to third-party computers or to their personal computers.

    d. The usage of removable media will be monitored by IT and data loss prevention software tools.

5. Unacceptable Use

    a. Computers will not be used for solicitation of activities or distribution of material that does not further Banner's mission or that would violate Banner's Solicitation and Distribution of Literature Policy.

    b. Workforce Members may send, upload, or download a third-party's copyrighted materials, trade secrets, proprietary financial information, or similarly protected business materials only in accordance with local, state, or federal law.

    c. Authorized devices accessing the Banner network will not be used for any non-Banner activity that could cause network congestion and/or disruption of networks and systems.

    d. Storage of non-Banner Information/data on Banner IT assets that does not directly assist workforce members in performing their job.

Reference: NIST 800-53 CM-11, SC-43

D. Internet Use

1. User Adherence

    a. Workforce Members will be responsible for the activity they conduct on Banner-provided internet connections.

    b. Banner wireless access points will be configured in accordance with Cybersecurity specifications.

c. Guests and Workforce Members using personally-owned devices or non-Banner Assets that have not been approved to access the Banner business production wireless Service Set Identifier (SSID) and wired networks are only permitted to access the Banner-defined guest wireless network Service Set Identifier (SSID), and are prohibited from connecting to the Banner business production wireless SSID and wired networks.

2. Unacceptable Internet Usage

a. Workforce Members may not give the impression that they are representing or providing opinions on behalf of Banner unless specifically authorized.

b. Social networking sites, such as Facebook, Twitter and LinkedIn will not be used to store, share, or disseminate Banner Information in violation of Banner's Social Media Policy.

c. Accessing websites with adult/sexually explicit material, gambling, illegal drugs, peer-to-peer file-sharing, personals and dating, violence, and hate based information and other content that violates Banner's policies is prohibited.

d. Websites determined to be compromised or that potentially contain a virus, worm, Trojan horse, or malicious code or software will be blocked by Cybersecurity.

e. Use of Banner-provided Internet services (including guest networks) for fraudulent or illegal purposes or uses is prohibited.

f. The use of anonymized network routing protocols is prohibited on the Banner Network.

g. Workforce Member's personally-owned devices authorized to access the Banner network are prohibited from connecting to the guest network for business purposes, unless required for specific business functions or service(s) (e.g., wireless team troubleshooting or configuration changes).

h. Banner managed devices are prohibited from connecting to the guest network to bypass security controls, including accessing blocked websites.

Reference: NIST 800-53 CM-11, AC-18

E. Software Use

1. User Adherence

a. Software usage will be in compliance with applicable user licenses, contracts, and agreements.

b. Banner reserves the right to conduct software audits at any time, not including medical devices. Unlicensed software will be removed, and a report will be provided to Information Technology management.

2. Unacceptable Use of Software

a. The following activities are strictly prohibited on or using Banner Business Tools:

   i. Development of computer virus or malicious code fragment.

   ii. Intentional distribution of a virus, worm, Trojan, or malicious code or software, regardless of type (nuisance, destructive, etc.).

   iii. Downloading or installing unlicensed or malicious software programs or hacking utilities (such as network sniffers, scanners, and password cracking programs) onto a computer that may be attached to the Banner network, unless approved by Cybersecurity for a valid business need.

   iv. Use of unlicensed or pirated software.

   v. Intentional tampering with or altering of software programs from their original form in a manner that violates their integrity and trustworthiness.

   vi. Creation or use of back doors or other technical workarounds which have the intent or effect of bypassing Banner security controls.

   vii. Unapproved or unauthorized modification or reconfiguration of applications installed by Banner.

   viii. Using Business Tools, networks, or Media Devices to operate unlicensed software and/or peer-to-peer file transfer services.

b. The following activities are prohibited unless permitted by Cybersecurity and Information Technology for a legitimate business reason:

   i. Installation on Banner Business Tools of software not licensed to Banner, freeware, shareware, and/or software downloaded from the Internet on Business Tools.

   ii. The use of Banner-owned software on a personally-owned device.

   iii. The use of personal software on Business Tools.

c. Disabling or otherwise reconfiguring security software or control without prior authorization. This includes disabling or reconfiguring anti-virus software, account lockouts, web content filtering, firewalls, and hardware or software restrictions.

d. Most copyright licenses for software contain single Central Processing Unit (CPU) usage restrictions. These restrictions will be honored. In some instances, the software copyright owner may grant a variance from these restrictions to Banner. However, in the absence of an explicit written variance, single usage restrictions in the license will be respected.

e. User licenses by whom be reviewed periodically (every six months) to ensure that the number of user licenses is consistent with the number of Workforce Members using the software.

Reference: NIST 800-53 CM-10, SI-7

F. Use of Copyrighted Material

1. Workforce Members will comply with laws pertaining to copyright protection.

2. Workforce Members will not use the copyrighted material that is licensed to Banner beyond the scope of the license.

3. Unlicensed copyrighted material on Business Tools, networks, and Media Devices may be removed by Banner, without notice.

Reference: NIST 800-53 CM-10

G. Electronic Communication

1. User Adherence

    a. Electronic Communications (e.g., electronic mail, instant messages, text messages, and online meeting platforms) conducted on Banner-owned devices, data, or network will be deemed a business record.

    b. Forwarding or sending electronic email with non-public, Internal, Restricted and Confidential Information, including PHI, Sensitive PII, or CHD, to the sender's personal email accounts (including for the purpose of facilitating printing on personally-owned printers unless approved in advance by IT) is prohibited.

    c. Transmission of Non-Public, Internal, Restricted and Confidential Information to recipients outside of Banner's electronic mail system will be encrypted.

    d. Electronic mail will be archived in accordance with Records Retention and Destruction Policy and local, state, and federal laws; it may be monitored, reviewed, and restored by Banner Health.

    e. Banner-initiated web meetings will be conducted via a secure method with both internal and external users, in accordance with the following guidelines:

        i. Pass codes or authenticated users who received the meeting invite (e.g., via Microsoft Teams) will be required before joining the meeting.

        ii. Presentations, meetings, or similar communications that contain Confidential Information should not be downloaded or recorded unless approved for training purposes, official communications, town halls, or similar communications intended for a broad Banner audience. Requirements in the Records Retention and Destruction Policy will be followed for all saved and stored presentations, meeting recordings and similar.

        iii. Meeting host credentials will not be included in meeting invitations.

2. Unacceptable Use of Electronic Communication

    a. Forwarding Banner electronic mail containing Confidential and/or Restricted Information, including but not limited to CHD, PHI and PII, to external personal

electronic mail accounts (e.g., Google Gmail, Hotmail, Yahoo, AOL, etc.) is strictly prohibited.

b. Forwarding Banner email to external non-Banner email accounts is prohibited.

c. Unauthorized access to or interception of Electronic Communication is prohibited.

d. Workforce Members will not transmit, via unsecure email, credit card numbers, passwords, or other security data that can be used to gain access to services via Electronic Communications.

e. When using electronic mail to communicate, Workforce Members will adhere to the following requirements:

   i. The use of electronic mail will be consistent with Banner policies and relevant industry standards and applicable local, state, and federal laws.

   ii. Obscuring, disguising, or otherwise hiding ones' identity as a Workforce Member or role at Banner in an electronic mail is prohibited. External users who have been issued Banner electronic mail will not purport to be Banner employees.

f. Workforce Members will not use personal electronic mail accounts (e.g., email@gmail.com, email@yahoo.com, email@hotmail.com) to send or receive business-related electronic mail as part of their job duties; always use a Banner-issued electronic mail account to do so.

g. Workforce Members will not use their Banner email address to register for external services that are not related to their job duties. This includes shopping, entertainment, social media, or other personal activity and resources.

h. Workforce Members will be cautious when opening an unknown or unexpected electronic mail attachment or link due to the risk of a potential virus, worm, Trojan horse, or other malicious code or software; unknown or unexpected attachments will be reported to the Service Desk for further investigation.

i. Electronic mail from unknown senders or suspicious electronic mail that violate this policy will not be opened; the recipient will be reported to the Service Desk.

3. Subscribing Banner-issued electronic mail addresses (including another Workforce Member's) to mailing lists is prohibited unless directly related to Banner business or fulfillment of the user's Banner job responsibilities. This does not apply to electronic mail lists related to activities such as discussing terms and conditions of employment with other employees and/or third-parties, so long as it does not interfere with the system's efficient functioning.

4. Subscribing other Workforce Members to electronic mailing lists without their prior permission is prohibited.

5. Workforce Members are prohibited from sending Sensitive PII, PHI, CHD, or other Restricted or Confidential Information via unauthorized instant message, text message, and/or paging systems.

a. Instant messaging and text messaging are acceptable forms of communication for business purposes not involving transmission of Sensitive PII, PHI, CHD, or other Restricted or Confidential Information.

Reference: NIST 800-53 SI-12

H. Bring Your Own Device (BYOD)

1. Only approved personally-owned devices with Banner-managed Mobile Device Management controls are allowed to access Banner's Non-Public data.

2. Personally-owned device users will, at the user's expense:

   a. Comply with applicable regulations and related Banner policies, standards, and procedures, including the IT Bring Your Own Device (BYOD) Standard.

   b. Agree to safeguard the personally-owned devices from unauthorized users by protecting the device and Banner Information from unauthorized access and/or disclosure.

   c. Be cautious when connecting to an unsecured or public network.

   d. Keep devices updated with Cybersecurity authorized operating systems and security patches.

   e. Ensure anti-virus and malware protection software is enabled where technically feasible.

   f. Immediately notify the Service Desk of lost, stolen, or potentially compromised personally-owned devices that contain Banner Non-Public data.

   g. Not copy Non-Public Information from electronic mail, calendar, contact applications, or Banner-owned, managed, or installed application to applications on a personally-owned device.

   h. Not store Non-Public Information on the personally-owned device outside of Banner approved and/or managed applications.

   i. Not modify approved operating system configurations (i.e., jail break a device).

   Note that if a personally-owned device is used for Banner related business, such device is subject to inspection by Banner, and the Banner related information on such device is subject to retrieval, deletion and/or retention by Banner.

   Reference: NIST 800-53 MP-7

VI. Exceptions and Enforcement

A. Exceptions to this policy will be logged, maintained, periodically reviewed and approved by Banner IT.

B. Users will report violations of this policy immediately to their Direct Supervisor and/or Department Manager or Director, who is responsible for escalating and reporting to the Service Desk as necessary.

C. Sanction actions will be enforced in alignment with Banner's IT Personnel Security Standard.

VII. References

A. NIST 800-53 Mapping: Access Control (AC-3), Configuration Management (CM-10, CM-11), Media Protection (MP-7), Planning (PL-4), Personnel Security (PS-6), Physical and Environmental Security (PE-3), System and Communications Protection (SC-43), System and Information Integrity (SI-7, SI-12)

B. NIST CSF Mapping: PR.DS-1, PR.DS-2, PR.PT-2, DE.CM-3, DE.CM-5, DE.CM-7

C. HIPAA Mapping: 164.308(a)(5)(ii)(A), 164.310(b), 164.310(c)

D. PCI DSS v3.2 Mapping: 4.2, 8.1.8, 12.3.5, 12.3.10, 12.4, 12.5, 12.5.5

VIII. Other Related Policies/Standards

A. Cybersecurity Operations Policy

B. Cybersecurity Governance and Management Policy

C. Cybersecurity Technology and Infrastructure Policy

D. Cybersecurity Risk Management Standard

E. IT Data Classification Standard

F. Cybersecurity Identity and Access Management Standard

G. HIPAA Sanctions Policy

H. Social Media Policy

I. Solicitation and Distribution

J. IT Mobile Device Management (MDM) Standard

K. IT Information Handling Standard

L. IT Bring Your Own Device Management Standard

M. IT Exception Management Standard

N. Cybersecurity User Password Standard

O. IT Personnel Security Standard

P. Records Retention and Destruction Policy

Q. Code of Conduct

IX. Keywords and Keyword Phrases

A. IT Acceptable Use

B. Assets

C. Cybersecurity

D. BYOD

E. Cloud

F. Computer

G. Copyright

H. Electronic mail

I. Internet

J. Banner-Owned Devices

K. Personally-Owned Devices

L. Social Media

M. Software

N. Wireless

O. Working in Secure Areas

X. Appendix

XI. Revision History

Date	Revised By	Version #	Reason for Revision
06/30/2021	Cybersecurity	4	Align IT policies and standards to NIST 800-53 as part of the IT policy and standard refresh initiative.
07/10/2022	Cybersecurity	5	Minor wording updates. Updated user authentication requirements to allow for strong, potential “password-less” authenticators (smart cards, biometrics, etc.). Added wording to forbid using Banner email for personal use (shopping, etc.). Added wording about reporting lost or stolen Banner-issued devices. Added wording about

			not creating automated rules to forward Banner email to non-Banner email accounts.
4/23/2023	Cybersecurity	6	Updated timeout setting requirement for applications from 3 minutes to 15 minutes.