BAKER UNIVERSITY

1858

Administrative Policies and Procedures

| | |
|---|---|
| **Subject:** | **Information Technology Acceptable Use Policy** |
| **Responsible Office:** | **Information Technology Department** |
| **Effective Date:** | **July 16, 2020** |

## General Statement

Baker University's computing and network resources are intended for university-related purposes, including direct and indirect support of the university's instruction, research, and service missions; of university administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the university community and between the university community and the wider local, national, and world communities.

The use of university computing and network resources is subject to the normal requirements of legal and ethical behavior within the university community. Although some limitations are built into computer operating systems and networks, those technical limitations are not the sole restrictions or policies on what constitutes permissible use. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

## Applicability

This policy applies to all users of university computing and network resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. Examples of those resources: Computers, Servers, Firewalls, Switches, Routers, VoiceMail, VoIP Phone System, Web Servers, Flash Drives, all other devices used for storage or access to Baker Information whether connected to the network or not.

## Acceptable Use

1. ***Users may utilize only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.***
2. ***Ability to access computing resources does not, by itself, imply authorization to do so.*** Users are responsible for ascertaining what authorizations are necessary, receiving proper approvals, and for obtaining proper access before proceeding**.**
3. ***Accounts and passwords may not, under any circumstances, be shared with, or used by,*** persons other than those to whom they have been assigned by the university not even with family members or a partner.
4. ***Users are responsible for complying with the requirements of the contracts and licenses applicable*** to the software files and other data they install on University or personal systems. Proof of legal licensing should be available upon request.

5. ***Users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.*** Again, ability to access other persons' accounts does not, by itself, imply authorization to do so.
6. ***Users must respect the finite capacity of those resources and limit use so as not to consume an amount of those resources beyond their work requirements or to interfere with the activity of other users.*** The university may require users of bandwidth, disk space, CPU time, or other resources to limit or refrain from specific uses in accordance with this principle, or to archive data in alternative ways.
7. ***Users must not attempt to access restricted portions of the network,*** an operating system, security software, or other administrative applications without appropriate authorization by the Information Technology Department.
8. ***Baker computing and network resources and services may be used only by authorized persons for Baker University-related purposes, including those listed in the General Statement above.*** These resources may not be used for other purposes except as authorized by Baker University. Minimal use of computers and networks for personal purposes such as e-mail and web access is allowed, as long as it does not interfere with work responsibilities and does not place a burden on resources. Users may not run unauthorized servers off of the Baker network. Users are expected to respect the priority of university business and keep personal use to a minimum. **Baker provided email addresses are not be used for any personal businesses owned by the employee.**
9. ***Users should not use tools that are normally used to assess security or to attack computer systems or networks*** (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized in writing to do so by the Information Technology Department.

**Adherence with Federal, State and Local Laws and Policies**

1. ***Users are responsible for protecting all information related to Baker University obtained in the course of their work, including Personally Identifiable Information (PII), in these systems in accordance with State and Federal Laws and Baker University rules and policies.***
   a These include but are not limited to
      i FERPA
      ii Payment Card Industry (PCI)
      iii Gramm-Leach-Bliley Act
      iv Kansas Consumer Protection § 50-6,139b
      v All other applicable laws, regulations, rules and policies.
   b All devices that contain PII information must be maintained in accordance with all laws and be protected from unauthorized access.
      i Portable Drives
      ii Personal cloud-based storage
      iii Cell Phones
      iv Personal Computing Resources

2. ***Users must comply with all federal, Kansas and other applicable law, as well as all generally applicable university rules and policies.***
   a Examples of such potentially applicable laws, rules and policies include, but is not limited to:
      i Laws of libel, privacy, copyright, trademark, obscenity and child pornography
      ii The Computer Security Act of 1987
      iii The Computer Fraud and Abuse Act (CFAA)

iv Obtaining Information by Unauthorized Computer Access (18 U.S.C. 1030(a)(2))
v Accessing to Defraud and Obtain Value: 18 U.S.C. § 1030(a)(4)
vi Damaging a Computer or Information: 18 U.S.C. § 1030(a)(5)
vii Trafficking in Passwords: 18 U.S.C. § 1030(a)(6)
viii Threatening to Damage a Computer: 18 U.S.C. § 1030(a)(7)
ix Attempt and Conspiracy: 18 U.S.C. § 1030(b)
x Intercepting a Communication: 18 U.S.C. § 2511(1)(a)
xi Disclosing an Intercepted Communication: 18 U.S.C. § 2511(1)(c)
xii Using an Intercepted Communication: 18 U.S.C. § 2511(1)(d)
xiii Unlawful Access to Stored Communications: 18 U.S.C. § 2701
xiv Identity Theft: 18 U.S.C. § 1028(a)(7)
xv The Electronic Communications Privacy Act, and Kansas Computer Crime; Kansas Statutes Section 21-5839
xvi The University's Student Handbook
xvii The University's Faculty Handbook
xviii The University's Employment Policies Handbook for administrative and support staff.
xix All other applicable laws, regulations, rules and policies.

3. ***Users who engage in electronic communications with persons in other states or countries*** or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks.
4. ***Users are required to ensure any downloaded material (including print, audio, and video)*** stored on university or personal computers being used in the course of performing their work for Baker University is not in violation of copyright laws.

Authorization to use university trademarks and logos on university computing resources must be obtained prior to their use.

**Enforcement**

The university may temporarily suspend or block access to an account, prior to the initiation or completion of an investigation, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies as applicable.

Users who violate this policy may be subject to disciplinary action, and may be denied further access to university computing resources.

**Security and Privacy**

The university employs various measures to protect the security of its computing and network resources and of their users' accounts. Users should be aware, however, that the university cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their uses of university computing and network resources are not private. While the university does not routinely monitor individual usage of its computing and network resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. The university may also specifically monitor the activity and accounts of individual users of university computing and network resources, including individual login sessions and communications, without notice, when deemed necessary.

## Implementation and Revisions

Baker University Executive Director of Technology and Information Security is responsible for implementing this policy, in cooperation with the President's Cabinet and the Chief Human Resources Officer. The university may change this policy as necessary.