Baker College		IT Foundational Policy **400-Software/Data Policy**
Supersedes Policy No.:	Effective Date: 03-04-2019	Reviewed on: 07-20-20
Owner: PPAC		Team Members: PPAC

1.0 PURPOSE

The purpose of this policy is to establish procedures and guidelines for the procurement and administration of software and data used by Baker College.

2.0 SCOPE DETAIL

This policy is applicable to those responsible for the procurement, management, and use of software across the institution.

3.0 DEFINITIONS

ASME	The Academic or Admin individual responsible for testing, documenting, and reviewing the compatibility of a resource with the College's systems.
AUP	Acceptable Use Policy
CIO	Chief Information Officer
COO	Chief Operating Officer
Data	Information stored electronically or in printed form.
Data at rest	Data stored in persistent storage
Data in transit	Any information that is generally not considered harmful or an invasion of privacy if released and can be disclosed to outside organizations without prior written consent: student name, address, telephone, email, date / place of birth, photograph, honors / awards, dates of attendance, student identifier (UIN), library card number, enrollment status, and most

	recent educational agency or institution attended.
Desktop Software	Software that is installed on any Baker College desktop, laptop, or similar device.
Directory Information	Any information that is generally not considered harmful or an invasion of privacy if released and can be disclosed to outside organizations without prior written consent: student name, address, telephone, email, date / place of birth, photograph, honors / awards, dates of attendance, student identifier (UIN), library card number, enrollment status, and most recent educational agency or institution attended.
EAS	The Enterprise Application Services team
Education Records	Record means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video, audio tape, film, microfilm, and microfiche which directly relates to a student. Further description of educational records can be found in the attached document – Baker College FERPA – Official Records.
Enterprise Software	Any software, excluding desktop software, that is used across the organization.
EOS	The manufacturer End of Support or End of Service date.
FERPA	Family Educational Rights and Privacy Act
GLBA	Gramm Leach Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ISS	The Infrastructure Security and Support team
IT	Information Technology
Personally Identifiable Information (PII)	Any data that is protected regardless of protocol that is associated with an individual person. This includes SSN, financial information, credit card numbers, driver's license number, health records / insurance, family contact information, disability status, citizenship, biometric identifiers, background

Protected Information (organization)	Intellectual property, configuration of technology assets (network diagrams, access controls, user access)
SLA	Service Level Agreement defines the level of service expected by a customer from a supplier
SME	Subject Matter Experts are those individuals responsible for documenting instructions and reviewing the compatibility of a resource with the College's systems.
Software	Software means, in its broadest definition, electronically stored computer instructions, operating systems, utilities, application, application or hosting service provider services, software as a service, and related documentation
Technology Request	A formalized procedure that approves technology installation, acquisition, contracts, and renewals for IT Resources.
TSS	The Technology Services and Support team

4.0 POLICY

4.1 Software

4.1.1 Procurement Process

a.) New and donated software must be submitted and approved through a Technology Request prior to acquisition or installation.

b.) New software should be standardized across the enterprise whenever possible.

4.1.2 Software Asset Management

a.) Software Installation and Removal

i.) Desktop software will be managed by the SME and deployed using an endpoint management system when possible.

ii.) Enterprise software installation and removal will be managed by the EAS, ISS, and TSS departments.

iii.) Software life cycles are determined by academic needs, manufacturer EOS date, and system compatibility.

b.) License Management and Reporting

i.) Software usage and licensing must be audited and any violations reported to the Procurement Department.

ii.) Extra or unused licenses should be repurposed or removed when possible.

c.) Software usage should adhere to all guidelines as specified by the AUP.

4.1.3 Obsolete Operating Systems

a.) IT managed operating systems that have reached the end of support will not be allowed on any Baker managed networks unless directed by the COO/CIO.

4.1.4 Backup Policy

a.) Baker College IT will provide policy-based, system level, network-based backups of server systems under its stewardship.

b.) Working with the Baker College computing community and its business functions, Baker College IT will implement backup procedures on a per system basis that define:

i.) Selections

ii.) Priority

iii.) Type

iv.) Schedule

v.) Duration

vi.) Retention Period

c.) Storage, Access, and Security

i.) All backup media must be stored in a remote secure area that is accessible only to designated Baker College IT staff. Backup media will be stored in a physically secured, fireproof safe when not in use. Offsite storage vendors should be bonded and insured.

ii.) During transport or changes of media, media will not be left unattended.

d.) Hosted Solution Backups

i.) All hosted application backup procedures should be identified within the technical design documentation for each application.

4.2 Data Regulation

4.2.1 Baker College shall comply with Federal and State data regulations. The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of a student's education records. In compliance with FERPA, Baker College does not disclose personally identifiable information contained in student education records, except as authorized by law.

4.2.2 Baker College is required by the Health Insurance Portability and Accountability Act (HIPAA) to ensure the privacy and security of all "Protected Health Information" or "PHI" created, received, maintained, or transmitted by or for its health care providers and self-insured health plans that are subject to HIPAA. This policy is intended to guide components at Baker College that are covered by HIPAA ("HIPAA Covered Components") to rigorously implement all HIPAA-mandated requirements as they are subject to enforcement by the federal government. Regardless of where or in what form (paper, electronic or otherwise) Baker College data is stored, it remains the property of Baker College and the college's HIPAA Covered Components are responsible for ensuring proper protection.

4.2.3 Baker College is required by the Gramm Leach Bliley Act (GLBA) to safeguard personal financial information held by financial institutions and higher education organizations as related to student loan and financial aid applications. Examples of this type of data include student loan information, student financial aid and grant information, and payment history.

4.2.4 Personally Identifiable Information (PII) is information that, if made available to unauthorized parties, may adversely affect individuals or the business of Baker College. PII is information that can be used to uniquely identify, contact, or locate a single person. This classification also includes data that the college is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. PII should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored, transported, and/or destroyed.

4.2.5 Baker College is required to adhere to the Michigan Social Security Number Privacy Act. Social Security numbers are unique, nine-digit numbers issued to U.S. citizens, permanent residents, and temporary (working) residents for taxation, Social Security benefits, and other purposes. Baker College does not use Social Security numbers as identifiers for students, faculty, or staff.

4.2.6 Protected Information includes any information that Baker College has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require Baker College to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

4.2.7 Information Lifecycle

a.) The information lifecycle is the progression of stages or states in which a piece of information may exist between its original creation and final destruction. These phases are: Accessing, Data Handling, Storing, Auditing, and Destroying. It is important to understand that storing refers to a broad spectrum of activities including putting a file in a filing cabinet or on to a file server or entering information into a database or spreadsheet. The requirements for storing information apply equally to the source and to any copies made. For example, when a file is downloaded or copied from a file server to a laptop computer for use offline, it is stored in that new location and all of the storing requirements must be followed.

b.) The College will use best practices and methods to properly destroy and/or sanitize physical and digital media containing sensitive internal and confidential college information.

5.0 RESPONSIBILITIES

5.1 IT

5.1.1 The role of Baker College Information Technology is to ensure the IT environment and additional products and services are used to support the institution while striving to achieve the IT SLA’s.

5.1.2 The SME shall be responsible for:

a.) Maintaining a process to audit and manage access, accounts, and licensing for software.

b.) Notifications of product upgrades and enhancements.

c.) Software SMEs are responsible for scheduling and applying patches, updates, and upgrades on appropriate schedules to reduce risk, increase usability, and ensure availability.

d.) The SME will notify the Procurement Department of any licensing violations.

5.1.3 Each supervisor should conduct periodic reviews of where Protected Information data is located, who has access to it, and the access control mechanisms. Verify that procedures for removing access are documented and accurate.

5.2 Procurement

5.2.1 Where applicable, the Procurement Department is responsible for recording software usage, location, cost, and the start and end dates of contracts and agreements.

5.2.2 The Procurement Department will manage and provide reporting for contract and licensing expirations.

5.2.3 The Procurement Department will notify the software SME of any licensing violations.

5.3 Faculty/Staff

5.3.1 The ASME shall be responsible for:

a.) Testing new software and recommending changes based on curriculum needs.

b.) Notifying IT of product upgrades and changes in curriculum requirements.

c.) Providing training material and documentation to faculty.

5.3.2 Review potential donations or acquisitions of software with Campus IT.

5.4 Supervisors of the employee

5.4.1 Assist IT with software requests and audits.

5.5 End User

5.5.1 The end user is responsible for understanding all Federal and State regulations that apply to their role(s).

5.5.2 Usage should adhere to all guidelines as specified by the AUP, student handbook, and employee handbook.