Becker College Data Classification and Usage Policy

OVERVIEW:

Information technology and data constitute valuable Becker assets. In order to protect the security, confidentiality and integrity of Becker data from unauthorized access, modification, disclosure, transmission or destruction, as well as to comply with applicable state and federal laws and regulations, all Becker data are now classified within security levels, with regulations on the usage of data at different levels.

APPLICABILITY:

The policy applies to all employees.

PRINCIPLES:

The following definitions and rules for usage delineate types of data and provide instructions for usage of that data.

Level 1: Highly Confidential, Requires Notification: This includes data that is highly confidential and requires notification to subjects and various state and federal entities if breached. Level 1 data includes: A person's first and last name, or first initial and last name in combination with any one or more of the following data elements relating to that person:

a. Social Security Number;
b. Driver's License Number or state-issued identification card number, including passports;
c. Financial account number (bank, investment, 403B), or credit or debit card number;
d. Health care information, including patient billing or medical records, information about physical or psychological state of health, counseling records, disease, medical history, medical treatment, drugs, therapies, genetic test results, family health or morbidity history;
e. Biometric data including fingerprints, voice prints, retina image, iris image, or other unique physical representation, with the exception of the fingerprints associated with individual fingerprint readers used for securing laptop or desktop computers.

Rules for Usage of Level 1 Data
Highly confidential data shall be stored on institutionally supported applications residing in the Becker Data Center, but **not** in Word, Excel or Access (with the exception of information required for critical business purposes and stored in an approved, secure area). Level 1 data can also reside in approved third party hosted applications, but those applications must be approved by the CFO and CIO. Hard copy data shall be stored in locked receptacles and rooms. Access to this electronic data shall only be gained through authenticated access on the Becker network or approved VPN access. Hard copy data shall only be accessed when business requires such use and all storage receptacles and rooms shall be appropriately designed to allow for authorized access only.

To this end, employees **shall not** store or copy this data to laptop or desktop computers (whether institutionally-owned or personally owned), OneDrive, Dropbox, smart phones, USB devices or other portable or cloud based media. In addition, this data shall not be transmitted via e-mail, instant message, chat or other social media technologies, with the exception of approved third party vendors with appropriate encryption in place. If data is transmitted on a recurring basis to external vendors, it shall be sent via a secure transmission, such as secure FTP (SFTP).

Electronic and hard copy data shall be destroyed in accordance with Becker's Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form. All departments shall have policies in place and periodically review electronic storage areas and their hard copy storage areas to insure that data is being destroyed in a timely and effective manner.

Level 2: Confidential: This includes data protected by state or federal law, contractual agreements and proprietary information against unauthorized use, disclosure, modification and destruction. Confidential data includes, without limitation, the following:

a. Student records, including date of birth, place of birth, mother's maiden name, official grades recorded on a student's permanent record, academic information, race, judicial information and other information relative to a student's permanent record (i.e. official grades, judicial records, etc.).
b. Human Resources data including employment records, salary, benefits, personnel evaluations, date of birth, place of birth, mother's maiden name, race and other records pertaining to personnel files (i.e. payroll reports, yearly merit increase data, etc.).
c. Academic Affairs information relating to non-public research and promotion and tenure files (i.e. notes relating to tenure decisions).
d. Alumni or donor information, including date of birth, place of birth, mother's maiden name, donation amount and assets (i.e. Daily Giving Reports, Donor Profiles, etc.).
e. Corporate records including Board of Trustee minutes, Board of Trustee votes and other confidential information dispersed at Board meetings and/or shared with Board members.
f. Sensitive Personal Information including credit checks, criminal background checks, visa numbers, sexual behavior and criminal convictions (i.e. CORI/SORI reports).
g. Information security data, including passwords, and other data associated with security-related incidents occurring at the College.
h. Research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq).

Rules for Usage of Level 2 Data

Confidential data shall be stored in institutionally supported applications located in the Becker Data Center, institutionally supported shared drives, or approved third party hosted applications. Third Party hosted applications that store Level 2 data must meet Becker's Third Party Assurance standard. Confidential data can be stored on College-owned laptop or desktop computers, but **shall not**

be copied to non-College computers, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

To this end, employees are permitted to store data on institutionally-owned laptop or desktop computers and shared drives; however, the dissemination of this data shall be done securely. Data shall not be transferred via e-mail unless encrypted. If data is transmitted on a recurring basis to external vendors, it is preferable to send this data through secure transmissions such as secure FTP (SFTP).

Electronic data shall be destroyed in accordance with Becker's Data Retention Policy, and shall be rendered unreadable in paper or electronic form. All departments shall have policies in place and periodically review electronic storage areas and their hard copy storage areas to insure that data is being destroyed in a timely and effective manner.

Level 3: Internal Use Only: This includes information that requires protection from unauthorized use, disclosure, modification, or destruction, but is not subject to any of the items listed in the Level 1 or 2 definitions above. Internal Use Only data includes:

a. StudentID
b. Data related to Becker operations, finances, legal matters, audits, or other activities that are not public in nature, but not classified as Level 1 or 2.
c. Faculty grade worksheets (i.e. Excel files used to track student grading prior to submitting to the Registrar's Office).
d. Personal white page, business white page or professional employment information for students, alumni or donors. This includes name, business name, business address, home address, e-mail, cell phone numbers, business phone numbers, home phone numbers, occupations and titles, but not classified as Level 1 or 2.
e. Personal white page information for faculty and staff. This includes home address, cell phone, home phone, home fax and personal e-mail, but not classified as Level 1 or 2.
f. Personal characteristics such as gender, height, weight, marital status, nationality, personal interests, photographs and names of children and other demographic information that is not classified as Level 1 or 2.
g. Becker Network Diagrams which display IP Addresses.
h. Internal Becker data, the distribution of which is limited by intention of the author, owner, or administrator, but not classified as Level 1 or 2.

Rules for Usage of Level 3 Data

Internal Use data can be stored in institutionally supported applications located in the Becker Data Center, institutionally supported shared drives, third party hosted applications and laptop or desktop computers (both Becker issued and personally owned). This data can be copied to smartphones, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

To this end, employees are permitted to transmit this data via unencrypted e-mail. Electronic data can be destroyed using traditional application delete functionality. Hard copy information can be destroyed in accordance with an employee's personal or departmental policy.

Level 4: Unrestricted: This includes data that can be disclosed to any individual or entity inside or outside of Becker. Security measures may or may not be needed to control the dissemination of this type of data. Level 4 data includes:

a. Content and images on Becker's public web sites (i.e. www.Becker.edu)
b. Publically released press statements
c. Course catalogue
d. Business White Page information for faculty and staff, unless otherwise restricted. This includes name, title, department, office location, office phone and Becker e-mail.

Rules for Usage of Level 4 Data
All information, whether in paper or electronic form, can reside in the public domain and is available to all students, faculty and staff; but, it is subject to Becker's Acceptable Usage Policy and federal copyright laws.

ENFORCEMENT:

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in Becker's Confidentiality Agreement.

APPROVAL:

Approved by Becker's Information Security Advisory Committee on 11/14/11.

REVIEW CYCLE:

This program will be reviewed and updated as needed, at least annually.