Kirkwood
COMMUNITY COLLEGE

College Procedure:	**700.1 - Data Access**
Policy Reference:	**700 – IT Operations**
Responsible Department:	**Information Technologies**
Approval Authority:	**Cabinet**
Procedure Owner:	**Vice President, Information Technologies**
Effective Date:	**4/5/2011**

Version Number: 2
Legal Counsel Reviewed (yes/no): No
Legal Reference(s):
Scope: College-wide

Reason for Procedure

Institutional data must be protected from unauthorized modification, destruction, or disclosure. Functional Owners will assess institutional risks and threats to the data for which they are responsible, and accordingly classify its relative sensitivity as Level I *(low sensitivity)*, Level II *(moderate sensitivity)*, or Level III *(high sensitivity).* Unless otherwise classified, institutional data is Level II. Kirkwood personnel may not broaden access to institutional data without authorization from the Functional Owner. This limitation applies to all means of copying, replicating, or otherwise propagating institutional data.

Institutional data is information that supports the mission and operation of Kirkwood Community College. It is a vital asset and is owned by KCC. It is likely that some institutional data will be distributed among multiple units of the College, as well as occasionally shared with external entities. Institutional data is considered essential, and its quality must be ensured to comply with legal, regulatory, and administrative requirements.

The Procedure

- Permission to access institutional data will only be granted to eligible Kirkwood employees for legitimate College purposes.
- Authorization for access to Level II and Level III institutional data comes from the Functional Owner, and should be made through a formal request with signature approval from the requestor’s department head.
- Where access to Level II and Level III institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.
- Kirkwood employees must report instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction.
- Functional Owners must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with Kirkwood policy and procedure.
- Functional Owners must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.

- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Data Handling Requirements:

	LEVEL I **Low Sensitivity** **(Public Data)**	**LEVEL II** **Moderate Sensitivity** **(Non-Public/Internal Data)**	**LEVEL III** **High Sensitivity** **(Confidential/Restricted Data)**
Mailing & Labels on Printed Reports	None	May be sent via Campus Mail; No labels required	Must be sent via Confidential envelope; Reports must be marked "Confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use	As authorized by Functional Owner	As authorized by Functional Owner	Prohibited
Physical Data/Media Storage	No special controls	Access Controlled area	Access controlled and monitored area
External Data Sharing	No special controls other than for Student Lists. See Use of Student Lists	As allowed by: Iowa Open Records Law, FERPA restrictions, Non-KCC project/study participants, or specific Kirkwood policy: Use of Student Lists	As allowed by Federal regulations; Iowa Open Records Law; and FERPA restrictions;
Electronic Communication	No special controls	Encryption recommended for external transmission	Encryption required for external transmission
Data Tracking	None	None	Social Security Numbers and Credit Cards
Data Disposal	No controls	Recycle reports; Wipe/erase media	Shred reports; DOD-Level Wipe or destruction of electronic media

Auditing	No controls	Logins	Logins, accesses and changes
Mobile Devices	Password protection recommended; Locked when not in use	Password protected; Locked when not in use	Password protected; Locked when not in use; Encryption used for the Level III data

References

This video is required viewing as part of this policy. Please select the control button on your keyboard and click to open the link:

Keeping Data Secure: Iowa State Law
Duration: 4:56 min.

Definitions

Term	Definition
Functional Owner	The Cabinet member (or his/her designee) for each operational unit at Kirkwood.
Mailing & Labels on Printed Reports	A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.
Electronic Access	How authorizations to information in each classification are granted.
Secondary Use	Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.
Physical Data/Media Storage	The protections required for storage of physical media that contains the information. This includes, but is not limited to workstations, servers, CD/DVD, tape, USB Flash, laptops, and PDA's.
External Data Sharing	Restrictions on appropriate sharing of the information outside Kirkwood Community College
Electronic Communication	Requirements for the protection of data as transmitted over telecommunications networks. Methods allowed in order of preference:

	• Business partner pulls the data from Kirkwood secured ftp server in encrypted format using strong authentication. • Kirkwood can push the data to business partner via secured ftp in encrypted format using strong authentication. • Kirkwood can send encrypted data on CD, DVD, or Tape via certified mail. This option would need the approval from the Executive Director, Technology Services or the President.
Data Tracking	Requirements to centrally report the location (storage and use) of information with particular privacy considerations.
Data Disposal	Requirements for the proper destruction or erasure of information when decommissioned (transfer or surplus), as outlined in Kirkwood's Computer Data and Media Disposal Policy.
Auditing	Requirements for recording and preserving information accesses and/or changes, and who makes them.
Mobile Devices	Requirements for the protection of information stored locally on mobile devices. This includes, but is not limited to laptops, tablet computers, PDA's, cell phones, and USB flash drives.

Revision Log

Version Number	**Date Approved**	**Approved by**	**Brief Description of Change**
1	4/5/2011	Jon Neff, Vice President, Technology Services	
2		Cabinet	Procedure Template 8/27/2019