Data Access Policy

Keene State College Policies and Procedures

Keene State College Data Access Policy

Updated & Cabinet Approved: 5/24/2011

Overview

The Keene State College Data Access Policy identifies two data categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect the information against unauthorized access. The guiding principles for this policy are defined in the USNH Information Technology Security Policy.

The Data Access Policy applies to data owned by the College. College-owned data includes all paper and electronic data prepared, supplied, used or retained by college employees, within the scope of their employment, or by agencies or affiliates of the College, under a contractual agreement. This policy covers all data created through all college operations.

This policy classifies College data into two categories – restricted or unrestricted data. These categories are expected measures to protect College data and are outlined below.

Keene State College expects all employees, partners, consultants and vendors to abide by Keene State College Data Access Policy.

Restricted Data

- Data that is governed by state/federal law, USNH or institutional policy. This restricted data requires limited access and stringent security controls,
- Data that appointed Data Steward consider sensitive. This restricted data requires limited access and stringent security controls.

Data Classification Examples

Restricted Data Classification Examples, but not limited to:

- Social Security Numbers
- Bank Account number
- Financial Aid Award
- Payment History
- Student Bill
- Protected Health Information
- Driver's License number
- Human Subjects research
- Counseling treatment information
- Grades
- Test scores
- Advising records Employee evaluation
- Employee background check
- Credit report
- Search committee
- Affirmative action
- Donor or prospect donor

Data Access Requirements

Access to restricted data is limited and defined by roles. Approved authorization is required from the supervisory role and/or the Data Steward.

Data Storage & Transmission Requirements

Restricted data is to be stored only on P: or Q: drives. Restricted data is not to be stored on C: drive, nor on a portable device.

Restricted data in paper form is to be secured at the end of the work day. Restricted data in paper form is to be shredded at the end of use in KSC approved locked shred bins.

In the rare case when SSNs are used, SSNs must be encrypted when used outside of Datatel or Banner. SSNs must be encrypted during all types of electronic transmissions.

Unrestricted Data

- Data not defined as restricted data.
- Data available for public consumption.

Data Classification Examples

Unrestricted Data Classification Examples, but not limited to:

- Campus maps
- Directory information as listed on KSC web site
- Press releases
- Campus events
- Admissions requirements
- Academic program information

Data Access Requirements

No authorization access is required

Data Storage & Transmission Requirements

N/A

Summary of KSC Training Material for Data Access Policy and FTC Red Flags

- Data SecURity involves you
- Red Flags is about prevention, detection, mitigation of Identity Theft
    - Pay attention to red flags (altered ID)
    - Ask for additional ID (DL, passport, government issued)
    - Not sure – talk to your Data Steward
- KSC has two types of data classifications:
    1. Restricted (data that is governed by law, institutional policy, standards and/or data that has been defined as sensitive data by your data steward)
    2. Unrestricted (data that is considered acceptable for general public use)
- What can you do to protect KSC data:
    1. Use only minimal amount of data needed
    2. Ask questions, don't make assumptions about your use of data
    3. Review business practices – rethink "just because"
    4. At the end of your work day, secure paper with restricted data
    5. When you are done using paper with restricted data, put paper in KSC locked shred bin box
    6. Store restricted data only on P: or Q:
    7. In the rare business case of needing to use SSNs outside Datatel/Banner, you must use encryption
    8. You can instantly lock your Windows computer using Windows + L. For Macs, you can use the Ctrl-Shift-Eject key

combination.

9. Use complex passphrase. You can make a complex passphrase by taking the first letter of words from a phrase that has meaning to you + include number and special characters. For example: my favorite Treat is a plate of nachos = mfTi@p0n
10. You have a lot of passwords to try and remember. Store your passwords in a Excel > store your Excel password file on your P:\ drive > and Encrypt your Excel password file.
    - How to Encrypt:
        - In Excel > Click on the Windows Icon in the top left > Select Prepare > Select Encrypt
        - Create a password. Don't use your KSC NetID. You'll be prompted to enter a password twice. Your list of passwords is now encrypted. This also works the same in Word and PPT.
11. If you have questions, talk with your Data Steward.

Data Stewards

Data Stewards are charged with the role of ensuring the Data Access Policy is followed within their area of responsibility. Data Stewards are College officials with decision-making responsibilities and management oversight of functional units/departments.

Data Steward Responsibilities include:

A. Define restricted data for operational unit/department.
B. Ensure operational unit/department data users follow procedures for protecting restricted data.
C. Ensure that access to restricted data is limited to those with a need to know.
D. Perform periodic reviews of business processes to assess risk for unauthorized access to restricted data.
E. Support use of SIS/HR & Finance systems as the official "source of truth" for data and proactively support the retirement of shadow systems.
F. Support training and educational requirements for data users within operational unit/department.
G. Resolve stewardship issues and use of data elements that cross multiple operational units/departments.
H. Understand laws, regulations, retention requirements that are specific to data assigned to Data Steward.
I. Review and approve restricted data usage and use requests.
J. Coordinate with Director Enterprise Information Systems or IT Security Manager on vendor requests for restricted data.
K. May assign a designee to perform the above duties.

List of Data Stewards by Operational Areas/Departments

Student Affairs

- Associate Vice President of Student Affairs/Dean of Students
- Director of Admissions
- Director of Campus Safety
- Director of Residential Life

Academic Affairs

- Assistant VP of Academic Affairs
- Dean of Library
- Registrar
- Dean of Arts & Humanities
- Dean of Professional and Graduate Studies
- Dean of Sciences

Finance & Planning

- Associate Vice President of Finance
- Director of Financial Aid
- Director of Physical Plant
- Chief Information Officer

Advancement

- Vice President of Advancement
- Director of Development

Human Resources

- Director of Human Resource

Related Documents

Federal Regulations

1. Family Educational Rights & Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99)
2. Freedom of Information Act (FOIA)
3. Health Insurance Portability & Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA)
4. US Patriot Act

USNH Policies

1. USNH Information Technology Security Policy
2. USNH Personnel Policy USY V.C.8. Performance Issues
3. USNH Identity Theft Prevention Program

KSC Policies - http://www.keene.edu/it/policyprocedure.cfm

For questions or more information, please contact securitymanager@keene.edu or Director of EIS, (mwood6@keene.edu) .