Data Access Policy

Keene State College Policies and Procedures

Keene State College Data Access Policy

Updated: 9/1/2017

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.

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:

- Define restricted data for department/unit.
- Ensure employees within department/unit are trained on expectations for restricted data.
- Oversee that restricted data is limited to those with authorized roles in a 'need to know' responsibility.
- Perform annual internal review to confirm appropriate user access with respect to restricted data being used within unit/department. For Colleague internal review of user access, ITG will facilitate annual review with Data Stewards.
- Ensure operational unit/department procedures adhere to outlined access, transmission and storage protocols for restricted data.
- Support use of SIS/HR & Finance systems as the official "source of truth" for data and proactively support the retirement of shadow systems.
- Resolve stewardship issues and use of data elements that cross multiple operational units/departments.
- Understand laws, regulations, retention requirements that are specific to data assigned to Data Steward.
- Approve restricted data use requests with UNSH. Coordinate with Director Enterprise Information Systems or IT Security Manager regarding data sharing requests to share restricted data outside USNH.
- May assign a designee to perform the above duties.

All Employees - Expectations for Use of College Data

- Access data only in a manner consistent with assigned responsibilities and in a manner consistent with furthering the College mission.
- Abide by applicable laws, regulations, standards, and policies with respect to restricted data.
- When there is a question regarding use of College data, seek clarification from appropriate Data Steward.

	Data Classification Protocols	
	Restricted Data	Unrestricted Data
Data Classifications	Data is classified as "restricted" if data protection is required by federal or state law/institutional policy and/or data is defined as restricted by Data Steward. Examples: SSN, Credit Card data, Protected Health Information	Data is classified as "unrestricted" if it is not considered to be restricted. Examples: Admissions Requirements Course catalogue, directory information as defined on www.keene.edu, Institutional Report
Access Protocol	Data access is limited to those with authorized roles in a 'need to know'function.	At the discretion of the data steward, anyone may be given access to unrestricted information. However, care should always be taken to use Keene State College data appropriately and to respect all applicable laws. Data that is subject to copyright must only be distributed with the permission of the copyright holder.
Storage Protocol	Electronic restricted data is to be stored only on P: or Q: drives. Electronic restricted data is not to be stored on C: drive, nor on removable media. In the rare case when SSNs are used outside of Colleague or Banner, NIST-approved encryption must be used. Restricted data in paper form should be secured via secure print at multi-function print stations and restricted data in paper form is be disposed of via KSC approved locked shred bins.	No storage requirements.
Transmission Protocol	NIST-approved encryption is required when transmitting restricted data. Encryption must be employed for compliance with FERPA, HIPAA, PCI-DSS and/or federal/state requirements. SSNs must be encrypted during all types of electronic transmissions. A data sharing agreement and notification to appropriate Data Steward is required when restricted data is transmitted to an external source outside of USNH.	No transmission requirements.
Identifiable Human Subjects Research	Identifiable Human Subjects research data. Any human subjects research data set containing data elements that would allow the human	De-identified Human Subjects research data are not considered restricted data for the purposes of this policy. De-identified means that the information does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual. Information is considered de-identified under this policy if the eighteen identifiers outlined in

Protocol	subjects/participants to be identified is considered restricted data, and must conform to the outlined access, transmission and storage protocols outlined within this policy.	the HIPAA Privacy Rule are removed from the information and if no code exists enabling the linkage of the identifying information to private information or specimen. Coded Human Subjects research data are not considered restricted data for the purposes of this policy, so long as the code and the data are separately stored. Coded data means that: (1) identifying information (such as name or social security number) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a number, letter, symbol, or combination thereof (i.e., the code); and (2) a key to decipher the code exists, enabling the linkage of the identifying information to the private information.
	Keene State College Restricted Data examples, but not limited to:	
Functional Area	Restricted Data Examples	Data Steward
Academic data	Grades, registration data, curriculum management, degree audits, use of Student SSN	Registrar
Admissions data	High school transcripts, GPA, admissions status, Use of applicant SSN	Director of Admissions
Campus Safety data	Campus Safety/local Police investigations, door access data, closed circuit camera data, parking data	Director of Campus Safety
Dean of Students (Dean's file)	Student conduct data, leave of absence, withdrawals, probation, suspension, student record review	Associate Vice President of Student Affairs/Dean of Students
Financial Aid data	Financial aid award data, tax return data, contribution income, Use of applicant and student SSN for financial aid	Director of Financial Aid
Finance/Business Office	Credit card transactions, ACH numbers, banking account information	Associate Vice President of Finance and Administration
Residential Life data	Housing assignments, roommate preferences, student conduct data	Associate Dean of Student and Director of Residential Life
Human Resource (employee) data	Use of employee SSN, Affirmative action, background checks, employee file and history employee disciplinary action, employee gender identity, employee leave time, employee protected health information and search committee activity	Associate VP of Human Resources
Institutional Research data	Sexual assault survey results, alumni data survey, institutional reports	Director of Institutional Research
Library data	Patron data, borrowing history, library fines	Dean of Mason Library
Student Accounts data	Financial data, banking numbers, bill payment status, payment plans, deposits, use of SSN for 1098-t reporting to the IRS and in the case of a Parent Plus loan refunds	Director of Student Accounts
Sponsored Projects and Research data	Employee history, financial conflict of interest in research screening and disclosures	Director of Sponsored Projects and Research Data

Data Access Policy Training Reminders to Review:

- Data SecURity involves you.
- Identity Theft is about prevention, detection, and mitigation.
    - College students represent a known risk for identity theft.
    - Employees need to pay close attention to suspicious behavior or conflicting information and ask for additional information to confirm an identity.
    - If you have a question, talk with your Data Steward.
- KSC has two types of data classifications:
    - Restricted (data that is governed by law, institutional policy, standards and/or data that has been defined as sensitive data by your data steward).
    - Unrestricted (data that is considered acceptable for general public use).
- What can you do to protect KSC data:
    - Use only the minimal level of data needed to complete an assignment.
    - Review business practices – rethink "just because".
    - When printing restricted data, use secure print.
    - At the end of your work day, restricted data in paper forms needs to be secured. When you are done using restricted data in paper form, paper needs to be disposed of via approved KSC locked shred bin box.
    - Store restricted data only on P: or Q: - not on removable media.
    - In the rare case when SSNs are used outside of Colleague or Banner, SSNs must have NIST-approved encryption.
    - You can instantly lock your Windows computer using Windows + L. For Macs, you can use the Ctrl-Shift-Eject key combination.
    - Use of complex passwords represent a critical line of defense in protecting restricted data.
    - Do not share your account passwords. Your passwords are your responsibility, and any activity performed while you or someone else has logged in using your account is considered your responsibility.

- KSC NetID passwords must:
    - Be 8 to 16 characters in length.
    - Contain a lower case letter, an upper case letter, and a number.
    - Contain only alpha numeric characters and the following special characters
    - ! ~ % ^ + * - . _ [ ] ‘
    - Not contain spaces.
    - Not include your name.
    - Be different from previously used passwords.
    - Be sufficiently different from your current password.
- Tips for building a strong and memorable password:
    - Take a phrase that is easy for you to remember and convert it into characters. It could be the first line of a poem or a song lyric.
        - “Water, water everywhere and not a drop to drink” (Rhyme of the Ancient Mariner) converts to Wwe&nadtd.
        - “We Three Kings from Orient Are” converts to w3KfOr3691. (3691 is the year 1963 spelled backward to extend beyond eight characters.)
- A method for securely storing your passwords is to create an Excel file on your P:\ drive containing your passwords and then apply encryption to the Excel file.
- How to Encrypt a Excel file:
    - Click File > Info > Protect Workbook > Encrypt with Password .
    - Enter a password, and click OK.
    - In the Confirm Password dialog box, reenter the password you entered in the previous step.
- If you have questions, talk with your Data Steward.

Related Documents

Federal Regulations and Policies

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) and 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

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