Information Classification

Op12.07-14 Information Classification

Information classification

Information classification, in the context of information security, is the classification of information based on its level of sensitivity and the impact to the University should that information be disclosed, altered or destroyed without authorization. The classification of information helps determine what baseline security controls are appropriate for safeguarding that information. All University information is categorized into one of four classification levels. In cases where information may fall into more than one classification, the highest applicable classification will apply.

1. Highly restricted information

Highly Restricted information is University information required to be strictly protected through governing statutes, regulations, and standards with specific provisions for its limited use. This classification only includes categories of information specifically defined in this policy. Those categories are:

- Social Security Numbers
- Payment Card Cardholder Data and Sensitive Authentication Data
- Protected Health Information (PHI)
- National Security Interest Information and Information Subject to Export Controls

This information may only be disclosed to those who have explicit authorization to view or distribute it. Any unauthorized disclosure, alteration or destruction of this type of information could cause a significant level of risk and have very serious repercussions for the University, individuals or affiliates.

University employees' access to Highly Restricted information will be determined by job responsibilities. Any Highly Restricted information shared outside the University network requires a Sensitive University Data Export Request System (SUDERS) request approved by the Information Security Officer, Chief Information Officer, and the Custodian of Records to ensure adequate security controls are in place.

2. Restricted information

Restricted Information is that which the University has a legal, contractual, or proprietary obligation to protect, including but not limited to information protected by state or federal privacy regulations and information protected by confidentiality agreements. Any unauthorized disclosure, alteration or destruction of this information could cause a high level of risk to the University, individuals or affiliates.

Examples: Personnel records, student information that is not considered directory information as defined by the FERPA Policy, information protected by non-disclosure agreements, contracts, confidential research, etc.

University employees’ access to Restricted information will be determined by job responsibilities. Any Restricted information shared outside the University network requires a SUDERS request approved by the Information Security Officer, Chief Information Officer, and the Custodian of Records to ensure adequate security controls are in place.

3. Private information

Private information is University or personal information when the unauthorized disclosure, alteration or destruction of that information could result in a moderate level of risk to the University or its affiliates. By default, all Institutional information that is not explicitly classified as Highly Restricted, Restricted or Public information must be treated as Private information. A reasonable level of security controls must be applied to Private information.

Examples: Budget information, procurement documentation, research that has not been completed or published, vendor documentation, contracts, BearPass Number, etc.

University employees’ access to Private information will be determined by job responsibilities. Any Private information shared outside the University network requires a SUDERS request approved by the Information Security Officer, Chief Information Officer, and the Custodian of Records to ensure adequate security controls are in place.

4. Public information

Information is classified as Public when the unauthorized disclosure, alteration or destruction of that information would result in little or no risk to the University and its affiliates.

Examples: Student information that is considered directory information as defined by the FERPA Policy, press releases, course information, research publications, etc.

Definition

SUDERS: Sensitive University Data Export Request System (SUDERS), an online system that facilitates information security risk assessments and reviews by the Information Security Officer, Chief Information Officer and Custodian of Records prior to University information classified as Private, Restricted, or Highly Restricted being transmitted and/or stored outside Missouri State's network.

Note

Request for exceptions to this policy may be granted at the discretion of the Chief Information Officer.

Line of authority

Responsible administrator and office: Chief Information Officer, Information Services

Contact person in that office: Information Security Officer, Information Services