#### **Minnesota State Board Policy 5.23**

#### Security & Privacy of Information Resources

#### **Procedure 5.23.2 & Operating Instructions 5.23.2.1**

#### Data Security Classification

|  |  |  |
| --- | --- | --- |
| **Data Security Classification** | **Definition** | **Highly Restricted Data Elements** **(This is an Exhaustive List)** |
| **Highly Restricted** | Institutional data must be classified as "highly restricted" if the data requires limiting access to only persons with a legitimate need to know, and:* the data elements for which loss of confidentiality is sufficient to assume a person’s identity in financial transactions; or
* by law, regulation, or contract, the data requires high-level security controls, or
* the loss of confidentiality could cause significant personal or institutional harm.
 | * Social security numbers
* Credit/payment card numbers and related information
* Financial account numbers such as banking or investment account numbers
* Security or access codes or passwords used to access highly restricted data
* Personal health/medical information including insurance policy ID numbers and any information covered under HIPAA
* Non-public investigation data (determined by legal counsel)
* Credentials for IT systems that manage data elements in this classification level
* Biometric information
* Trade secret or intellectual property protected by a non-disclosure agreement
 |
| **Data Security Classification** | **Definition** | **Restricted Data Elements****(Not an Exhaustive List)** |
| **Restricted** | Institutional data must be classified as “restricted” if it does not classify as “highly restricted” but the data:* by law is not public data, or
* requires limiting access to only persons with a legitimate need to know, or
* whose unauthorized disclosure will require statutory notification to affected parties (i.e., breach notification).
 | * Student records – admission applications, transcripts, exam papers, test scores, evaluations, grades, student discipline, student class schedule, student worker information, financial aid, and loan collection records
* Student directory information that has been suppressed by the student
* Student class lists
* College, university, system office, or faculty trade secret or intellectual property
* Library use information
* Individual demographics including age, race, ethnicity, gender, citizenship, visa status, veteran or disability status, employee home address/phone, dependent information
* Faculty/staff employment applications, personnel files, benefits information, birth date, and personal contact information
* Donor contact information and non-public gift amounts
* Privileged attorney-client communications
* College, university or system office internal memos, email, reports, and financial data identified as non-public
* Driver’s license numbers
* \*Student ID numbers (if not directory data) and passwords
* Employee performance information and other private personnel data
* Parking lease information
* Request for proposal vendor responses and scoring information prior to contract award
* Credentials for systems that manage data elements in this classification level and systems classified as Low
* Partial social security number
* Business continuity and disaster recovery plans
* Security information as defined by Minn. Stat. § 13.37
 |
| **Data Security Classification** | **Definition** | **Public Data Elements****(Not an Exhaustive List)** |
| **Low** | Institutional data must be classified as "Low" if by law it is available to the public upon request. | * Certain employee information name, job title, job description, work location and phone number, employee identifier, salary, gross pension, value and nature of fringe benefits, payroll time sheets, education/training and previous work experience, first and last employment dates, existence and status of complaints, terms of employment settlement disputes, final disposition of discipline, honors and awards received or as identified as public in Minn. Stat. § 13.43, subd. 2.
* Student information (unless suppressed by the student) name, other information identified as directory information by the college/university in its published FERPA policy
* Financial data on public sponsored projects
* Course offerings
* Invoices and purchase orders
* Budgets
* “Summary” or statistical data that does not identify an individual
* Information authorized to be made available on or through a website that does not require a Minnesota State recognized authentication system (e.g., StarID)
* Published research data
* Campus maps
* Job postings
* Information in the [public domain](http://www.copyright.gov/help/faq/faq-definitions.html#public_domain)
 |

\*Limited Directory Data (LDD) at SMSU.