Data Classification Standard

Confidential

Data classified in this category is considered to be highly sensitive in nature. Such data should not be copied or removed from the institution's operational control without department head permission. Confidential data is subject to the most restricted distribution and must be protected at all times. Compromise of data classified as Confidential could seriously damage the reputation, mission, safety, or integrity of the institution, its staff, or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

Examples: Personal Identifiable information such as Social Security Numbers, Driver's License Numbers; Institution Finances; Employee Personnel data; Vendor Bids information; Ongoing audits and Investigations; HIPPA protected information; Student transcripts: FERPA; Student addresses;

Institutional

Data classified in this category is for internal institutional use only, the release of which must be approved prior to dissemination outside the institution. Its compromise may inconvenience the institution, but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity. Protection of this information is required and would be determined by the institution.

Examples: Daily institutional finances; Research data; Test questions and answers; Minutes of meetings; Agenda for discussion

Public

Data classified in this category is for general use and is approved by the institution as available for routine public disclosure and use. Security at this level is the minimum required by the institution to protect the integrity and availability of this data. This data should be sent out or made available only through Institutional Communications and/or other approved departments.

Examples: Press material; Marketing content; Public posts; Annual Reports

Data Classification	Confidential	Institutional	Public
Reputational risk	High	Med	Low
Financial Risk	High	Med	Low
Other institutional risks	Information in this category may provide access to physical or virtual resources	Protected data from a department's point of view	General information
Legal requirements	Protection of data is required by law (State and federal laws and regulations, FERPA, HIPPA, GLB, DMCA, etc.)	BSU has a contractual agreement or operational need to protect data in this category	Protection of this data is at the discretion of the data owner.
Access	Only designated BSU employees who have a need to know and need to use may be provided access.	BSU employees and non-employees (vendors) who have a need to know.	BSU community, and general public
Examples	Social Security Numbers, Employee personnel Information, Payroll information, bank account numbers, routing numbers, HIPPA information, Prospective student records with SSN, phone numbers and addresses, Financial bid information prior to bid submission, Credit Card numbers, Investigations and audit information, Tax Payer ID, Purchasing card information, and Student data guided by FERPA.	Resources with access to restricted information, Research details Information for Institution internal use only and Financial transactions that do not include restricted data. Some parts of confidential information that may be reduced in sensitivity after a certain time;	Campus maps, Community announcements, Business contact information, newsletters