BOWIE STATE UNIVERSITY 1865

https://www.bowiestate.edu/it/security-and-compliance/

Data Classification Rule

Rule #	3.0	Effective Date	2015	Email	infosec@bowiestate.edu
Version	1.2	Contact	DIT Info Security	Phone	301-860-4357
BSU Policies	N/A				
Standards/Regulations Addressed	USM Security Standards v4 - 2.4 NIST SP 800-53: MP-3 Media Labeling; Data destruction MP-6. SP 800-122 PII. SP 800-60				

Table of Contents

PURPOSE

This rule defines the requirements assigning and maintaining classification settings for all BSU computer and communications system information assets.

SCOPE

This rule applies to all BSU computer systems and facilities, with a target audience of BSU Information Technology employees and partners.

RULE

Asset Ownership

Information Ownership - All information possessed by or used by a particular organizational unit must have a designated Information Owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

Information Systems Data Custodian – All information systems must have a data custodian. These individuals are technology experts who guarantee data availability throughout the information system network. BSU DIT provides help desk engineers, network engineers, and system administrators as data custodians.

Information Data Steward - Each significant type of information must have a designated Steward who will properly protect BSU information in keeping with the designated Information Owner's access control, data sensitivity, and data criticality instructions.

Information Systems Department Ownership Responsibility - With the exception of operational computer and network information, the Information Systems Department must not be the Owner of any production business information.

Asset Classification

Four-Category Data Classification - All BSU data must be broken into the following four sensitivity classifications: RESTRICTED, CONFIDENTIAL, INTERNAL, and PUBLIC. There are distinct handling, labeling, and review procedures must be established for each classification.

Data Classification Descriptions - The following descriptions are used for identifying and labeling each sensitivity classification for all BSU information.

RESTRICTED - This classification label applies to the most sensitive business information that is intended for use strictly within BSU. Its unauthorized disclosure could seriously and adversely impact the University, its customers (students), its business partners, and its suppliers. Examples include merger and land acquisition documents, USM or University level strategic plans, litigation strategy memos, and trade restrictions such as certain computer applications development.

CONFIDENTIAL - This classification label applies to less-sensitive business information that is intended for use within BSU. Its unauthorized disclosure could adversely impact BSU or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Examples include social security numbers, employee performance evaluations, student transcript data, student requests for data privacy, strategic alliance agreements, unpublished internally-generated market research, computer passwords, and internal audit reports.

INTERNAL USE ONLY - This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact BSU or its employees, suppliers, business partners, or its customers. Examples include the BSU employee telephone directory, computer access numbers, new employee training materials, and internal rule manuals.

PUBLIC - This classification applies to information that has been approved by BSU management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Default Classification - Information without a label is by default classified as Internal Use Only or Confidential.

When data is shared with other institutions, the State, or federal agencies, that shared data should be managed with the security requirements determined to be the highest among the sharing institutions involved, and approved by the institutional CIO or data steward.

Asset Labeling

Assigning Data Classification Labels - For all existing information types, the Information Owner is responsible for choosing an appropriate data classification label to be used by all employees who create, compile, alter, or procure production information.

Multiple Classification Labeling - When information of various sensitivity classifications is combined, the resulting collection of information must be classified at the most restricted level found anywhere in the sources.

Data Classification Labeling - All restricted or confidential information must be labeled according to the Data Classification Reference, while information not falling into one or more of the sensitive categories need not be labeled.

Equipment Identification Codes - All BSU computer and communications equipment must have an identification number placed on the equipment that can be used to assist police in their attempts to return stolen property.

Hardcopy Sensitivity Labels - All printed, handwritten, or other human-readable manifestations of restricted, confidential, or private information must have an appropriate sensitivity label on each page.

Information Life Cycle Labeling - From the time when information is created until it is destroyed or declassified, it must be labeled with a sensitivity designation if it is either restricted or confidential.

Declassification And Destruction

Dates For Reclassification - If known, the date that Restricted or Confidential information will no longer be sensitive must be indicated on all BSU sensitive information. This will assist those in possession of the information with its proper handling, even if these people have not been in recent communication with the information's Owner. Personally Identifiable Information (PII) that is no longer needed must be destroyed.

Expired Classification Labels - Those employees in possession of sensitive information that was slated to be declassified on a date that has come and gone, but is not known definitively to have been declassified, must check with the information Owner before they destroy the information.

Notifications - The designated information Owner may, at any time, declassify or downgrade the classification of information entrusted to his or her care. To achieve this, the Owner must change the classification label appearing on the original document, notify all known recipients and Custodians.

Schedule For Review - To determine whether sensitive information may be declassified or downgraded, at least once annually, information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical. Personally Identifiable Information (PII) that is no longer needed must be destroyed.

VIOLATIONS

Any violation of this rule may result in disciplinary action, up to and including termination of employment. BSU reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. BSU does not consider conduct in violation of this rule to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, BSU reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

Confidential Information (Sensitive Information) – Any BSU information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, social security numbers, pre-public financial results, product costs, and pricing, and employee information and lists. Confidential Information also includes any confidential information received by BSU from a third party under a non-disclosure agreement.

Information Asset - Any BSU data in any form, and the equipment used to manage, process, or store BSU data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Partner - Any non-employee of BSU who is contractually bound to provide some form of service to BSU.

References

NIST Cybersecurity Framework
ISO/IEC 27002 - 8.2 Information Classification

Related Documents

Approval and Ownership

Edited by	Title	Date	Signature
John Husfield	Info Assurance Analyst		
Ifueko Fify Omoruyi	IT Security Manager	03/2019	I.O
Approved By	**Title**	**Date**	**Signature**
IT Security Committee	N/A	6/2015	By committee

Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	MM/DD/YYYY	MM/DD/YYYY	
1.2	Update	03/2019		