Data Governance Policy

Policy Name: Data Governance Policy
Approval Authority: President and Executive Leadership Team
Interpreting and Implementing Authority: Director of Computer and Information Resources
Effective: 03/21/2014
Last Revised: 07/01/2024
Next Review Date: July, 2029

Policy Statement

Data Governance Scope and Objective

This Data Governance Policy (this "Policy") sets forth the rules that govern the handling of any sensitive or controlled information by Wesleyan College, including its employees, contractors, consultants, vendors, temporary employees, and other workers. The data governed by this policy may include but is not limited to, social security numbers (SSN), driver's license numbers (DL), credit card data, bank account numbers, financial information, medical information, educational records, credit information, tax information, other types of sensitive information, and other types of personally identifiable information (PII). The goal of this policy is to ensure the accessibility, confidentiality, and integrity of the data Wesleyan College receives, processes, and stores, either internally or externally and transmits in accordance with all relevant laws and regulations.

Policy Responsibilities

Data Governance Roles

- **Data Governance Authority**—The President of the College and Executive Leadership Team is responsible for defining, implementing, and managing policies related to data governance.
- **Data Owner** – the institution's executive office or President responsible for all data read, created, collected, reported, updated, or deleted by the organization.
- **Chief Information Officer** – A designated individual with managerial oversight ensuring that technical infrastructure is in place to support the data needs and assets, including availability, confidentiality, and integrity.
- **Data Steward** – The individual responsible for the data being read, used, created, collected, reported, updated, or deleted and the technology used in their data area(s).
- **Data System Administrator** - A technical expert managing an information system.
- **Data User**—Any faculty or staff member authorized by the appropriate institutional authority to access institutional data.

Policy Details

Data Management

1. **Data Classification**
    1.1. Data types must be classified as **Public**, information requiring availability and integrity but not confidentiality; sensitive, information not disclosed to the public but lacking a controlling authority; and **Confidential,** information controlled through agreements, laws, or regulation.
    1.2. Data must be classified according to the most restrictive classification of any individual system record.
    1.3. Generally, **Sensitive** and **Confidential** information must be handled in such a manner as to prevent the unauthorized disclosure of or access to such information.

1.4. All physical and electronic information transmitted or released that contains **Sensitive** or **Confidential** must be marked as such.

2. **Data System Documentation**

2.1. Information systems must be assessed to determine the suitability for housing the institution's data.

2.2. The Data Steward, CIO, and System Administrator must document the system purpose, responsible parties, associated data types, data classification, data processing flow, system impact, system security, system backup and recovery, system data retention, and system lifecycle.

3. **Data System Evaluation**

3.1. Data Systems with information classified as **Sensitive or Confidential** must be assessed and evaluated according to risk.

3.2. Data Systems with information classified as **Confidential** must be secured according to the laws, standards, or regulations pertaining to the associated data types. Appropriate controls or approved mitigation methods must be implemented.

3.3. Data Systems with a high degree of impact on college operations must be evaluated for availability.

3.4. Data Systems must be evaluated to determine threats and vulnerability to unauthorized access to data.

3.5. Data Systems must be evaluated to determine the effectiveness of backup and recovery processes.

3.6. Data Systems must be evaluated to determine retention and lifecycle.

3.7. Data Systems must be approved by the CIO after the evaluation process before purchase to ensure they meet all necessary requirements.

4. **Data Security.** All employees are responsible for maintaining the privacy and security of sensitive or confidential data. The following are additional specific policies that must be followed to maintain sensitive and confidential information data security.

4.1. According to Google's Terms of Services information for educational institutions, the College uses Google Apps, which complies with the Family Educational Rights and Privacy Act (FERPA) security policy. If email messages and data stay within the Google Apps system or the college's email accounts, there should be no concern about violations of the FERPA policy. All departments that handle sensitive or confidential information must use two-factor authentication for their College email account.

4.2. All sensitive or confidential data stored on a portable medium, such as a laptop or flash drive, must be encrypted. The Computer and Information Resources department will configure the encryption for you. Sensitive or confidential data must not be put on employee-owned computers, smartphones, tablet computers, storage devices, or other portable devices. Suppose sensitive or confidential data is downloaded from Google or another Internet-based system. In that case, it must be saved directly to the departmental shared drive, so it does not reside in unencrypted storage. The connection must be encrypted during data transmission to any other system or service. Sensitive or confidential data should not be stored in unencrypted portable media.

4.3. When an employee leaves the College for any reason, the Computer and Information Resources department must be notified to clean the employee's computer and other devices of sensitive or confidential information. The department is responsible for removing any files that need to be kept and saving them to the departmental shared drive.

4.4. Departmental supervisors are responsible for requesting appropriate access or restrictions to the College's systems and data.

4.5. All users with sensitive or confidential access must use their designated account.

4.6. Any departmental, vendor, service, or other account must be assigned to a specific individual during access. Designated supervisors log account assignments and revoke access by changing the account password.

4.7. All users who handle sensitive or confidential data are responsible for changing their email and system passwords every three months. Other users are required to change their passwords on an annual basis. If a user's account is suspected of being compromised, the password should be immediately changed.

4.8. Training will be provided for all departments related to handling sensitive or confidential data on an annual basis.

4.8.1. Data governance training shall also be provided during the new hire orientation.

4.9. Any remote access to the Wesleyan internal network must be encrypted according to current industry standards, use multi-factor authentication, and be approved by the Director of Information Computer and Information Resources.

5. **Transmission—Digital transmission methods of sensitive or confidential information must have prior approval from the Director of Computer and Information Resources. Any digital transmission of sensitive or confidential information must use encryption technology.** When faxing sensitive or confidential data, you should ensure the recipient can receive the fax and validate the number of pages received.

6. **Storage –** Physical or digital sensitive or confidential information must be secured when unattended. Do not leave materials containing such information in areas where they may be seen by anyone who is not authorized to view such information. Information stored electronically should be protected using available authentication procedures and file privileges. You must not leave sensitive or confidential on your screen when you leave your work area. You must lock your workstation when you are not present. Computers should not be logged in when you leave the office for an extended period. Sensitive or confidential data on unsecured media is prohibited.

7. **Disposal—When information is no longer needed, hard copies should be shredded. Discarded computer equipment must be decommissioned,** and the storage medium must be removed and destroyed.

8. **Termination—Once a user's relationship with the college has been terminated, their accounts will be immediately disabled,** and all access to the College systems and software will be revoked.

9. **Physical Security –** Access must be limited to those individuals authorized by the College. Supervisors are responsible for ensuring that proper security practices are maintained and that their employees follow this policy. Doors must be locked to prevent unauthorized access. You must advise your supervisor if you become aware of a door that does not close or lock properly. Keys or critical cards should not be left unattended or carried in such a way that makes them easy to lose or steal. You must immediately notify your supervisor if keys or cards are lost or misplaced. For departments that handle sensitive or confidential information, for anyone leaving their desk where your computer is not visible (by you or a fellow departmental staff member), the display should be locked, or the user account logged out.

10. **Incident Response Plan—If you suspect a security incident, data breach, system compromise, or other malicious activity (each, a "Breach"), you should immediately contact the Computer and Information Resources department.** They will follow the appropriate steps detailed in the Security Breach Response Policy.

11. **Administration of this Policy—The College's Computer and Information Resources department is responsible for administering this policy.**