Data Governance Policy

Policy Name: Data Governance Policy
Approval Authority: President and Cabinet
Interpreting and Implementing Authority: Director of Computer and Information Resources
Effective: 03/21/2014
Last Revised: 04/01/2019
Next Review Date: April, 2024

Policy Statement

Application and Purpose

This Data Governance Policy (this "policy") applies to each employee, contractor, consultant, temporary employee, and other worker ("you" or a "User") at Wesleyan College ("us," we" or "College") and to all physical areas where the College keeps information. You agree to this policy by using or accessing the College's systems. This policy sets forth the rules that govern your handling of Personally Identifiable Information ("PII"). This data may include, but is not limited to social security number, credit card data, bank account number, financial and medical information, educational records, credit information, address and tax information. This policy does not supersede any state or federal laws.

Entities Affected by the Policy

The entities affected include all faculty, staff, and students, whether full-time, part-time, or under contract.

Policy Details

1. **Training**
   General data security training shall be provided as part of the new hire orientation. This training should include acceptable use training, physical security training, recognition and reporting of potential security incidents and appropriate use of security features (e.g., locked screen saver, password management, etc.). The new hire must sign the bottom of this policy as an acknowledgement of this training upon completion. Application-specific training may be given on specific applications and should focus on the types of PII that is at risk. Our Computer and Information Resources department shall provide regular updates regarding security threats and annual security awareness briefings.

2. **Personally Identifiable Information**

   2.1. **Generally.** PII must be handled in such a manner as to prevent the unauthorized disclosure of or access to such information.

   2.2. **Access.** User access to the College's information resources will not be provided until a background check and appropriate paperwork has been completed and approved by Human Resources and Payroll departments.

   2.3. **Identification.** All physical and electronic information transmitted or released that contains PII must be marked "Confidential".

   2.4. **New Systems.** All proposed systems must be approved by the Director of Computer and Information Resources before purchase so that the appropriate data security capabilities are available and integration requirements are evaluated.

   2.5. **Software.** The Computer and Information Resources department must approve all software that collects or stores PII before its installation on a College owned computer or mobile devices.

   2.6. **Data Security.** All employees are responsible for maintaining the privacy and security of PII. The following are additional policies that must be followed to maintain PII data security.

      2.6.1. The College uses Google Apps, which according to Google's Terms of Services information for educational institutions, complies with the Family Educational Rights and Privacy Act (FERPA)

security policy. If email messages and data stay within the Google Apps system or within the Colleges email accounts there should be no concern about violations of the FERPA policy. All departments that handle PII information must use two factor authentication for their College email account.

2.6.2. All PII 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. PII data must not be put on any employee owned computers, smartphones, tablet computers, storage devices or other portable devices. If PII data is downloaded from Google or another Internet based system it must be saved directly to the departmental shared drive so it does not reside on unencrypted storage. During transmission of data to any other system or service the connection must be encrypted. PII data should not be stored on CDs or DVDs.

2.6.3. When an employee leaves the College for any reason the Computer and Information Resources department must be notified so the employee's computer and other devices can be cleaned of any PII information. It is the department's responsibility to remove any files that need to be kept and then save them to the departmental shared drive.

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

2.6.5. All users having access to PII must use their own designated account.

2.6.6. Any departmental, vendor, service or other account must be assigned to a specific individual at the time of access. Designated supervisors are responsible for logging account assignment and revoking access by changing the account password.

2.6.7. All users that handle PII data are responsible for changing their email and systems passwords every three months. Other users are required to change their passwords on an annual basis. At any point a user's account is suspected of being compromised the password should be immediately changed.

2.6.8. Training will be provided for all departments related to handling PII data on an annual basis.

2.6.9. 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.

2.7. **Transmission.** Digital transmission methods of PII must have prior approval from the Director of Computer and Information Resources. Any digital transmission of PII must use encryption technology. When faxing Personally Identifiable Information, you should ensure that the recipient is available to receive the fax and validate the number of pages received.

2.8. **Storage.** Physical or digital PII must be kept secure in cabinets, drawers, or otherwise 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 PII on your screen when you leave your work area. You must lock your workstation when you are not present. Computers should not be left logged in when you leave the office for an extended period of time. PII on unsecured media is prohibited.

2.9. **Disposal.** Hard copies of information should be shredded when they are no longer needed. Discarded computer equipment must be decommissioned and the storage medium removed and destroyed.

2.10. **Termination.** User accounts will be immediately disabled once the user's relationship with the College has been terminated and all access of the College systems and software will be revoked.

3. 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 key cards should not be left unattended or carried in such a way that makes them easy to be lost or stolen. You must immediately notify your supervisor if keys or cards are lost or misplaced. For departments that handle PII, anyone leaving their desk where your computer is not visible (by you or a fellow departmental staff member) the display should be locked or user account logged out.

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

5. **Administration of this Policy**
   The College's Computer and Information Resources department is responsible for the administration of this policy.

6. **Discipline**
   Employees who violate any provision of this policy are subject to discipline, up to and including termination of employment.

Responsibilities

The President of the College and Cabinet will provide approval for this policy and any changes. The Director of Computer and Information Resources will oversee the daily compliance of this policy.

Violations of the Policy

Any violation of this policy for the inappropriate handling of data must be reported to the Director of Computer and Information Resources. The user's account will be temporarily suspended, when necessary, to assure proper security of the College systems until a proper review is performed. Upon indication of a violation, the Director of Computer and Information Resources will report the incident to the appropriate Vice President to determine further action.

All student workers or contractors handling data must abide by this policy.

Interpreting and Implementing Authority

Computer and Information Resources Department.

Acknowledgment of Receipt and Review

I acknowledge the receipt of a copy of the College's Data Governance Policy. I have read and familiarized myself with the policy's contents and I understand my responsibility for adhering to this policy. I agree to abide by the College's rules and procedures as outlined in the policy. I understand that the College, at its discretion, may monitor my activities when using College equipment and information systems. I understand that violations of this policy will be investigated and, if found to be substantive, may result in disciplinary action, including but not limited to termination of employment. I further understand that certain violations of this policy may be subject to criminal prosecution.

Signature: _____

Printed Name: _____