Data Security Policy

Purpose

Wartburg College acknowledges its obligation to ensure appropriate security for data, business systems, and technology resources in its domain of ownership and control. Furthermore, the College recognizes its responsibility to promote security awareness among the members of the campus community.

Wartburg College develops, publishes, and enforces policies, procedures, and standards in order to achieve and maintain appropriate protection of institutional data and business systems. This document along with related security policies, procedures, and standards identifies key security issues for which individuals, departments, and units are responsible.

Scope

This policy applies to all faculty, staff, and students as well as any other individuals or entities who use data and business systems at Wartburg College. This policy applies to all institutional data, even if stored without the use of a technology resource. Further, this policy applies to all technology resources owned or leased by Wartburg; to any privately-owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, mobile devices, phones, multimedia devices, storage media; and the campus network itself.

Policy Statements

Every member of the Wartburg community is responsible for protecting the security of institutional data and business systems by adhering to the objectives and requirements stated within published policies. In addition, individuals are required to comply with the additional security policies, procedures, and practices established by departments or other units. If multiple policy statements or security standards are relevant for a specific situation, the most restrictive security standards will apply.

Access to Level II and Level III data, as defined by the Data Classification Policy shall only be granted to authorized or approved users on a need-to-know basis.   Every user must maintain the confidentiality of level II and III institutional data even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.
All technology resources of the college are protected through IT policies, procedures, standards, and actions that meet applicable federal, state, regulatory, contractual, or administrative requirements and support the Wartburg College mission, vision, and values. The Chief Information Officer (CIO) or their designee shall publish appropriate procedures and standards to protect the confidentiality, integrity, and availability of technology resources and institutional data.

All units must provide opportunities for individuals to learn about their roles in protecting institutional data and business systems.

Procedures

Data Protection Requirements

The CIO or their designee shall publish security procedures and standards applicable to all technology resources. The procedures and standards shall be updated regularly as advances in technology occur and will have the full force and effect of this policy.

Some College systems must be protected with a higher level of attention and caution. The classifications found in the Data Classification Policy will be used to define which business systems require additional attention. Such business systems will have additional security requirements placed upon them by the CIO, the data steward, or their designee(s). Such requirements will be published by the CIO. Certain systems, such as those necessary for credit card and protected health information, have additional legal requirements which can be provided by the corresponding data steward.

Unnecessary or High-Risk Storage of Institutional Data

A fundamental principle to reduce the risk of a loss of confidentiality of data is to simply not store the data. As such, transitory/convenience records must not be retained indefinitely. The Wartburg College Records Retention Policy dictates the retention periods for various types of institutional data. Transitory/convenience records should be destroyed when they cease to be useful. Digital backup copies of institutional data must be managed through a central ITS service and not at the department or division level. Departments must not attempt to store **level III data** on technology resources without requesting assistance from ITS personnel.

Cloud Storage of Institutional Data

Institutional data of level I or II may be stored in an ITS supported cloud location. ITS staff must have administrative privilege to the cloud storage provider and the specific storage location to ensure proper safeguards are implemented. All data stored in a cloud location is subject to the same procedural requirements as data stored within the source Business System.

Sensitive Personally Identifiable Information

The CIO or their designee shall maintain security procedures and standards applicable to sensitive personally identifiable information (PII) such as social security numbers, passport numbers, driver's license numbers, credit card numbers, etc. All systems shall be regularly evaluated for the presence of PII. ITS will deploy automated solutions where possible to identify PII stored on technology resources. As required under this policy, all sensitive PII must be approved for storage.

Risk Assessment

Risk assessment is a systematic process used in determining the potential impact of a negative event by evaluating the nature of the information and information systems. All business systems with level III data will be designated for conducting a risk assessment at an interval prescribed by the auditors, CIO or the data steward. The results of risk assessments will be placed on file for audit and accountability purposes.

Specific Roles and Responsibilities

Chief Information Officer (CIO)

The Chief Information Officer has responsibility for security oversight of Wartburg's technology resources. Implementation of security policies is assigned to Information Technology Services and may be delegated throughout the College at the CIO's discretion. The CIO has the ability to make exceptions to data security procedures in support of Wartburg's mission.

Data Steward

The data stewards, as members of the Data Governance Group, are responsible for recommending and establishing policies, procedures, standards, and guidelines for data administration activities. Data stewards may delegate their role to other employees. They are also responsible for advising departments, units, and individuals in security practices relating to institutional data. The data steward has authority to authorize or deny access to data.

Data User

The data user, synonymous with user, is the individual, automated application, or process that is authorized by the data steward to create, enter, edit, and access data, in accordance with the data steward's policies and procedures.

Users have a responsibility to:

- Maintain the security of passwords; personal identification numbers (PINs); authentication tokens, devices, and certificates; as users will be held accountable for any activities linked to their accounts.
- Use the data only for the purpose specified by the data steward.

- Comply with controls established by the data steward.
- Comply with controls implemented by Information Technology departments.
- Follow terms of the Technology Resource Use Policy
- Prevent disclosure of confidential or sensitive data.
- Report security incidents that may have breached the confidentiality of data to ITS

Departments and Other Units

Departments and other units are responsible for securing any information they create, manage, or store, and for any information they acquire or access from other College systems (e.g., student educational records, personnel records, and business information). This responsibility includes participating in periodic risk assessments, developing and implementing appropriate security practices, and complying with all aspects of this policy.

Individuals Using Personally-Owned Computers and Other Network Devices

Students, faculty, and staff who use personally owned systems to access Wartburg technology resources and institutional data are responsible for the security of their devices. Further, they are responsible for following and implementing necessary security protocols on their personal devices and required to follow all applicable laws, regulations, policies, and procedures directed at the individual user. Data stewards may prohibit the use of personal devices to access data under their purview.

Level III data may not be stored on personally owned systems.

Third Party Vendors

Third party vendors providing hosted services and vendors providing support, whether on campus or from a remote location, are subject to Wartburg College security policies and will be required to acknowledge their security obligations in contractual agreements. The vendors are subject to the same auditing and risk assessment requirements as departments and other units.

Other Registered Entities

Any entity that is a registered user and connected to the College network is responsible for the security of its computers and network devices. Further, they are responsible for following and implementing necessary security protocols on their personal devices and required to follow all applicable laws, regulations, policies, and procedures directed at the organization or individual user.

Non-Compliance

Violations of this policy may be referred for disciplinary action as indicated in the Technology Resource Use Policy

Usage of Terms

AVAILABILITY – Availability is the ability to assure that systems work promptly and service is not denied to authorized users. A loss of availability is the disruption of access to or use of information or an information system.
BUSINESS SYSTEM – A business system is any system handling institutional data, including technology resources and paper-based records.
CONFIDENTIALITY – Confidentiality ensures that confidential information is only disclosed to authorized individuals. A loss of confidentiality, for the purposes of this policy, is the unauthorized disclosure of information.
DATA STEWARD– Data stewards are senior staff who have planning, management, and policy-level responsibility for data within their functional areas. A data steward has the authority to authorize or deny access to data. For example, the Registrar, Director of Human Resources, Controller, Executive Director of Admissions, Department Heads, Deans, Vice Presidents, and the President would all be data stewards. Institutional administrators may act as data stewards for departments under their authority. The Data Governance Group and its members individually will support data stewards in the execution of their roles, particularly with regard to advising on matters of data access and use.

INTEGRITY – Integrity is the appropriate maintenance of information and systems. A loss of integrity is the unauthorized modification or destruction of information.
TECHNOLOGY RESOURCES - Wartburg College Technology Resources include college-owned computer systems and peripherals, local-area networks and network-attached devices, telecommunications equipment and the high-speed network connecting the campus to the Internet. Technology resources may include computers, software, servers, network utilization, storage utilization, virtual machine capacity, tablets, phones, multimedia devices, storage devices, wireless spectrum, and any other in-demand resource managed by ITS staff.
POTENTIAL IMPACT – Potential impact is the level of adverse effect a loss of confidentiality, integrity, or availability could be expected to have on college operations, college assets, or individuals.
INSTITUTIONAL DATA – Institutional data are information that supports the mission and operation of Wartburg College. Institutional data is a vital asset and is owned by the College. Some institutional data are shared across multiple units of the College as well as outside entities.
USER – User includes any faculty, staff, student, developer, contractor, vendor, or visitor as well as any other individual or entity using information, institutional data, and/or technology resources of Wartburg College.

Revision History

ITS Review completed June 14, 2022

DGG Review completed June 24, 2022

Final Revision Edited June 24,2022

Cabinet Approved July 25,2022