Calvin College
Information Security Policy

Purpose
The Calvin College Board of Trustees, Administration, and Faculty Governors believe that the valuable information the College produces and has been given stewardship over should be protected from serious threats. Risks to this information’s confidentiality, integrity and availability should be addressed and appropriate effort taken to reduce harm and negative impacts of these risks to the College and its constituents.

This policy addresses information security risk by establishing an information security data framework and related responsibilities.

Philosophy
Information security is the discipline of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. This goal is commonly expressed as protecting the confidentiality, integrity, and availability of information.

Information security enables safe sharing of information. This is accomplished by making necessary and appropriate information available to authorized people.

Information security is a responsibility shared by all and, therefore, must be cultivated and infused into the life and culture of the College.

The information security concepts articulated by this policy are meant to be consistent with information security best practices and College obligations, both contractual and regulatory.

Scope
The policy covers all information infrastructure and information assets that are owned by the College or used by the College under license or contract, whether electronic, print, or other.

This policy applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and vendors with access to College information resources.
Definitions

**Information Asset:** Data in any media format created, processed and/or used by the business. Media formats may vary from paper copies (memos, letters, check stock, etc.), to electronic files stored on hard drives, USB flash memory devices, CD’s, DVD’s, back-up tapes, etc.

**Information infrastructure:** Computing and telecommunications equipment, software, processes, facilities.

**Physical Security:** Physical barriers and control procedures applied as preventive measures or countermeasures against threats to resources and sensitive information. Door locks, guards, fire sprinklers and exit doors are examples of physical security measures.

**Regulations with Information Security impact:**

- **FERPA** – Family Education Rights and Privacy Act
- **HIPAA** – Health Insurance Portability and Accountability Act
- **GLBA** – Gramm Leach Bliley Act
- **FACTA** – Fair and Accurate Credit Transactions Act
- **PCI-DSS** – Payment Card Industry Data Security Standard
- **Michigan Identity Theft Protection Act 445.61 2004**
- **Michigan Library Privacy Act 455**

Data Framework Classification and Roles

**Data Classification Model**

There are two general categories of information the College gathers during the normal course of institutional operation, Sensitive information and Public Information:

1. **Sensitive information:** Information in this category may not be distributed without Consideration of its sensitive nature.

   - **Private information** is personal information, including personal intellectual property, which is accessible only by its owner and those to whom the owner directly entrusts it, except under exceptional circumstances.
     Examples: Intellectual property, email

   - **Confidential information** is institutional information normally handled in the same manner as private information, but may be accessed by other authorized
members of the College community under limited additional circumstances.
Examples: social security number, credit card information, date of birth, medical records,
education record, financial record, library record

- **Community information** is institutional information that is intended for
distribution within the College community.
Examples: listserv, internal mailings

2. Public Information: Information in this category is distributed without restriction.
Examples: marketing materials, public facing website

Roles

**Information Users** – An Information User is anyone who has access to a college information asset or
infrastructure, and the ability to consume, use, or manipulate it.

Users are responsible for protecting information resources by adhering to College policies and exercising
good judgment in the protection of information resources. Users may only access and use information
for which they have been given authorization or that their job duties require. Users must also follow
information usage procedures, standards and guidelines established by Information Owners, Stewards,
or the Information Security Officer.

Users must alert College authorities of misuse, mishandling, or abuse of information (See Incident
Response section of this policy). Non-compliance with this policy could lead to disciplinary action (See
Enforcement section of this policy).

**Information Owners** - An Information Owner is someone who has chief responsibility over particular
information. The responsibility includes how information is classified, used, maintained, protected,
accessed, and disposed of.

Private Information is the responsibility of the information creator. Confidential information and
community information is the responsibility of an upper level management representative, such as a
Vice President. In order to execute these responsibilities, the Information Owner may delegate
particular responsibilities to Information Stewards.

**Information Stewards** – An Information Steward is an individual or group that has delegated
responsibility from the Information Owner over particular information classified as College confidential
information or community information.

Stewards assist the Information Owner in carrying out the day to day care of their information,
especially authorizing, revoking, and auditing access to and use of the information they have
stewardship over.
**Information Security Officer (ISO)** – The Information Security Officer is tasked with oversight and execution of the College Information Security Program. The ISO is an advisor to the College and provides guidance and expertise in the discipline of Information Security.

The ISO has the authority to develop, monitor, and enforce policies, procedures, standards, and guidelines pertaining to information security and data privacy.

**Information Custodians** – Information Custodians are typically information technology professionals, engineers, and technical support staff. Vendors and other 3rd parties may also be contracted with to provide information custodianship.

Custodians are responsible for the protection and maintenance of information assets. Custodians work with systems, processes, and infrastructure to make information available for use.

### Responsibilities

**Information Handling**

1. Unauthorized disclosure of sensitive information is prohibited.

2. Unauthorized tampering or alteration of sensitive information is prohibited.

3. Unauthorized destruction or disposal of sensitive information is prohibited. Laws and policies governing information retention must be complied with.

4. When confidential information is being transported or stored, it must be protected from unauthorized disclosure, modification, or destruction.

5. When possible, confidential information must be protected with sufficient publicly vetted encryption algorithms while in transit and at rest. If encryption is not possible appropriate compensating controls must be considered and implemented.

6. Before access is granted to confidential information, a signed non-disclosure agreement must be on file for that individual or organization. When appropriate, criminal and reputational background checks must be conducted.

7. Confidential information being transported to or stored with a third party outside of the Colleges network or physical premise must be approved by the Information Security Officer and Information Owner / Information Steward. Particular attention should be given to risk assessment, audit of the third party’s security controls, and contractual agreements.

8. Confidential information, both digital and physical, must be disposed of properly to prevent unauthorized disclosure.
9. Use of sensitive information outside of the parameters established by Information Owners / Information Stewards is prohibited.

Identity and Access
10. Anonymous identities (usernames, UIDs) should be avoided, and are prohibited when accessing confidential information unless an exception is granted by the Information Security Officer and Information Owner / Information Steward. Exceptions must be documented, logged, and regularly reviewed.

11. Information Users will be given the minimum level of access to systems and information that their duties require.

12. No single employee with access to confidential data may be given total control of College identified critical or sensitive transactions. When appropriate, separation of duties or checks and balances must be implemented.

13. Managers and Supervisors must report change of an employee’s employment status or role to Human Resources or the Student Employment Office.

14. Remote access to the College network or systems is only allowed by authorized individuals via methods which employ appropriate access control, encryption, and logging methods.

15. Passwords, pass-phrases, and private keys (physical and private digital) must be protected, must comply with established College standards, and may not be shared.

16. Usage of physical keys providing access to confidential data storage locations must be detected and logged. The identity of key holders must be documented and regularly reviewed.

Information Compromise
17. If it is suspected that "sensitive" data has been accessed by an unauthorized party or has been used improperly by an authorized party, the discovering individual must report the incident immediately (See the Incident Response section of this policy).

18. If a password, pass-phrase, or key is believed to have been compromised, it must be changed immediately. If that password authorizes access to sensitive information, the incident must be reported (See the Incident Response section of this policy).

Information Infrastructure
19. Unauthorized eavesdropping, redirection, sniffing, and tapping of network traffic or systems is prohibited. Law enforcement, the Information Security Officer or authorized custodians may use these methods for judicial, criminal, incident investigation, or system administration purposes.

20. Information infrastructure must be protected from theft, intrusion, malicious code, and abuse.
21. Information infrastructure must be implemented, and maintained according to a documented standard.

22. Information infrastructure must be regularly patched for security and stability.

23. Locations that house digital and paper copies of confidential data must employ appropriate physical preventative, detective, and deterrent controls.

24. Availability of critical information and infrastructure must be reinforced with appropriate redundancy, backup, and disaster recovery plans and technologies.

25. A “defense in depth” or layered security strategy must be applied to College information, network, and system architecture and design whenever possible, especially pertaining to sensitive information.

Assessment and Compliance

26. Risk assessments must be regularly conducted to reveal security posture, and to identify vulnerabilities and weaknesses in software, infrastructure, policy, procedure, practices and personnel.

27. All employees must participate in information security awareness training that is provided by the College.

28. In addition to this policy, all security requirements found in state law, federal law, and other College contractual obligations, such as FERPA, HIPAA, GLBA, FACTA, PCI-DSS (not an exhaustive list) must also be considered and complied with.

Incident Response

In the case of a sensitive data breach, or misuse/abuse of sensitive information, contact the Information Security Officer (ISO) or the Chief Information Officer (CIO), immediately.

The ISO or CIO will execute an incident response plan to address the Incident appropriately.

Enforcement

29. Violations of this policy will be handled consistent with College disciplinary procedures applicable to the relevant persons or departments. The College may temporarily suspend, block or restrict access to information and network resources in order to protect the integrity, security, or functionality of College resources or to protect the College from liability. The College may routinely monitor network traffic to assure the continued integrity and security of College resources in accordance with applicable College policies and laws. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.
Approvals and Policy Status
31. Draft review – Summer of 2012
32. Policy Approved by The Planning and Priorities Committee – August 2013

Policy Review
33. This Policy will be reviewed and updated annually, and as otherwise needed, by the Information Security Officer.