Gettysburg College Cybersecurity Program

Introduction and Philosophy

Gettysburg College Information Technology division has designed its Cybersecurity Program around four general philosophies: Keep It Simple, Use Common Sense, Use Standards and Best Practices whenever possible, and Build A Maintainable Program. The Cybersecurity Program is recorded in three components: this overview narrative based document; supporting documents stored in IT's private network file folder which include policies, detailed procedures, and reports; and the two assessment and planning tools:

- National Institute of Standards and Technology (NIST) based assessment and planning worksheet, NIST 800-171
- Educause's security worksheet based upon the International Organization for Standardization (ISO) 27002:2013 "Information Technology Security Techniques. Code of Practice for Information Security Management."

In addition, the Board of Trustees IT Committee provides guidance, oversight and periodic review of IT policies and procedures regarding strategic direction and security.

Gettysburg College's IT division uses a layered approach as a foundation to cybersecurity following generally the International Standards Organization (ISO) network stack model. IT collapses the ISO layers into User and Policy; Application; and Computer, Server, Network, and Physical layers. Throughout these layers, audit processes are applied for the appropriate act or regulation guidelines. The content and format of the Gettysburg College Cybersecurity Program was developed by leveraging the theoretical, practical, compliance related, and standards related knowledge of the Information Technology Leadership team. This security program is reviewed and iteratively improved with feedback and context from campus members, government regulations, legal input, and current technology trends and best practices. IT uses two templates derived from the NIST 800-171 document and the Educause security worksheet as tools to plan and measure progress and compliance.

User and Policy Layer

Cybersecurity Governance

The institutional view on cybersecurity is the responsibility of the Ethics and Integrity Committee. The key responsibilities are policy creation and review, ensuring compliance awareness and planning, and ensuring the appropriate user education.

Policy Inventory

Policies related to cybersecurity are below and the most up to date version can be found at: Ethics and Integrity Committee Policies

- Identity Theft Prevention (Red Flags) Policy
- Information Management Policy
- Advance C/S Application Access Policy
- Infrastructure and Computing Support Policy
- Campus Web Policy
- E-Communications Policy
- IT Computer/Printer Replacement and Upgrade Policy
- Network Use Policy
- PeopleSoft Application Access Policy
- Social Media Policy
- Supported Software on Gettysburg College Computers
- Web Policy

Cyber Liability Insurance

Each year, the Vice President for Information Technology and the Institutional Risk Manager complete the required forms for the College's Cyber Liability Insurance. The forms are thorough questionnaires and inventories of applicable vendor contracts. For any questions, please contact the Vice President for Information Technology. The complete yearly forms and applicable contracts reside on IT's shared private network storage.

Security Education and Outreach Program

Every Gettysburg College new employee receives training on data protection and email best practices. Faculty members working with data requiring approval by the Gettysburg College's Institutional Review Board receive additional training. IT also works with Faculty who require additional training due to a grant or other third party requirements. Employees working with Personally Identifiable Information receive periodic data security training to refresh best practices. Periodically, IT provides data security and social networking training at divisional meetings and sessions open to the campus. Students receive security training through the various student dashboards.

Travel Tips

The World Travelers web site has sound travel tips for taking digital equipment on a trip. To learn more, click on their link here.

Contract View Process

IT reviews technology related contracts with designated college attorneys to understand risk and security related issues and to determine what next steps are required if any.

Application Layer

Data Classification and Data Location

Gettysburg College classifies data stored in an institutional supported system as public or confidential. A system is secured based upon the most sensitive data that is stored in the system as defined by FERPA, HIPPA, and a common definition of Personally Identifiable Information. IT signifies data as located in an on-campus *System*, in an off-campus vendor supported *Cloud* service, or stored in files located on *Mobile* computing or storage devices. A current list is maintained in IT's private network file storage.

Vendor Security Questions

IT has a two-page list of security questions that cloud based vendors are required to complete. The answers are used as evidence for a security risk assessment of the cloud provider. The current security questions are stored in IT's private network file storage. Gettysburg College also recognizes SOC 2 and ISO 27001 application layer certificates in place of the security questionnaire.

Data Systems Security Prevention and Assessment

Data Systems (DS) employs current security techniques to evaluate existing enterprise software and to develop secure custom software. DS grounds its work in best practices as described at The Open Web Application Security Project (OWASP). Enterprise web based applications and custom software are evaluated using criteria similar to those in the OWASP Top Ten Project. In addition, DS employs automated vulnerability scanning tools to assess web-based applications.

Academic Software Assessment

The Educational Technology department meets with faculty requiring specialized hardware or software. During this meeting, the security profile of the requirements is established and security forward solutions are designed and implemented.

Computer, Server, Network, and Physical Layer

Computer and Mobile Devices

For College owned computers, antivirus and malware protection software is installed and cannot be removed by a user. Along with real time monitoring by the antivirus software, weekly scans are performed on all College owned computers. These scans cannot be disabled. All College owned computers automatically update the operating system software and other critical software

components. All computers are deployed with passwords enabled and screen locking enabled. IT does not assist anyone with disabling these security features. Network access passwords are complex and must be changed every six months. College owned mobile devices/smartphones are deployed with passwords enabled and remote wipe capability.

Personally owned mobile devices are permitted on a designated wireless network. All devices must pass a security scan checking for such items as an up to date virus software package. Personally owned mobile devices by non-college personnel have a limited usage time and are removed after a period of inactivity.

Server and Telecom Security

All College virtual and physical servers have antivirus software installed. The operating system software and other critical software components are automatically updated. Access to servers is on a need only basis. All servers are located in a secured server room with access controls and monitoring equipment. Only approved IT members are permitted access to server rooms. Others including vendors who need to work in these rooms can enter when accompanied by an IT member.

Network Security

The College employs current network security devices, appliances, and best practices. The Unified Threat Management appliances (UTM), Intrusion Detection System, and Intrusion Prevention System use a preemptive approach to network security to identify potential threats and respond to them swiftly. These systems are regularly updated in real time. The College segments its campus network based upon security and usage requirements. Network technicians receive status updates from autonomous network monitoring devices which alerts via email and text messaging on over 1100 network connected devices every couple of minutes. Data is logged to a centralized and protected server.

Physical Controls

All campus virtual and physical servers are located in one of the College's server rooms. The access to these rooms are limited to a select number of IT members. Data center access is by physical keys which are carefully controlled. The rooms are monitored for temperature, humidity, light, sound, and moisture levels. Alarms are emailed and texted to personnel if room conditions are not nominal. All environmental data is recorded. The rooms are also monitored with motion triggered video cameras which record access and activity to a secure location. A log book of entries and exits is maintained in each room. Non-college personnel that require access to these rooms are escorted at all times by an IT member.

All physical devices that have contained data are physically destroyed by shredding with certificate of destruction.

Audits and Assessment

Audits

Each year, IT has a planned and targeted audit of its operation. These audits range from the specific such as reviewing database security and operating procedures to generalized security audits of the entire division and the College cybersecurity profile. IT's security and software development, change management procedures and policies are reviewed every year during the annual financial audit. In addition to this annual comprehensive audit, IT participates in the institutional audit where each division experiences an in-depth review on a periodic basis. All annual audit recommendations and next steps are reviewed with the Trustee Information Technology Committee at the Spring committee meeting. To maintain Purchase Card Industry (PCI) compliance, an external periodic vulnerability scan is performed on select portions of the College's network and systems.

Past Audits

The overall results of each audit or review from below are documented and stored in the IT private network folder.

Audit Year (Academic)	Audit
2007/2008	Information Management Risk Assessment
2008/2009	Security and Information Management Policy review
2009/2010	Review data storage location of sensitive information
2010/2011	Review IT Recovery Processes
2011/2012	IT Security Program Review
2012/2013	External Reviews
2013/2014	IT Risk Assessment by RCMD
2014/2015	Review Cloud Vendor Assessment Procedure
2015/2016	Enterprise Data Applications – Email Audit
	Oracle Database Review: Reviewed configurations and security surrounding core PeopleSoft database
2016/2017	Physical Space Audit for Innovation & Creativity Laboratory
2017/2018	Internal GDPR/GLBA reviews
2018/2019	IT Risk Assessment by RCMD
2019/2020	Cybersecurity Audit
2020/2021	External Penetration Test

Assessment

To assess Gettysburg College's cybersecurity program and security profile, IT maintains two security and planning templates derived from the following:

- National Institute of Standards and Technology (NIST) based assessment and planning worksheet, NIST 800-171
- Educause's security worksheet based upon the International Organization for Standardization (ISO) 27002:2013 "Information Technology Security Techniques. Code of Practice for Information Security Management."

Compliance

Gramm-Leach-Bliley Act (GLBA) Plan and Documented Audit

IT maintains documents reporting the minutes from audits and next steps of the key departments covered under the GLBA. Below are the key points from GLBA to which IT assesses and plans.

- Develop, implement, and maintain a documented data security program;
- Designate an employee or employees to coordinate the program;
- Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of
    - employee training and management;
    - information systems, including network and software design, as well as information processing, storage, transmission, and disposal;
    - the ability to detect, prevent, and respond to attacks, intrusions, or other systems failures;
- Control the risks identified, by designing and implement information safeguards and regularly test/monitor their effectiveness;
- Oversee service providers by
    - taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, and school (customer) information at issue;
    - requiring your service providers by contract to implement and maintain such safeguards;
- Evaluate and adjust your school's data security program in light of
    - the results of the required testing/monitoring,
    - any material changes to your operations or business arrangements,
    - any other circumstances that you know may have a material impact on your information security program.

European Union General Data Protection Regulation (EU GDPR) Plan and Documented Audit

IT maintains documents from assessments and next steps of the key components covered under GDPR. Below are the key points from GDPR to which IT assesses and plans.

- Lawful Basis for Processing
- Individual Rights
    - The right to be informed
    - The right of access
    - The right to rectification
    - The right to erasure
    - The right to restrict processing
    - The right to data portability
    - The right to object
    - Rights in relation to automated decision making and profiling
- Accountability and Governance
- Security
- International Transfers
- Data Breaches

Purchase Card Industry (PCI) Compliance

Gettysburg College has performed a thorough PCI self-assessment over several years. IT has been a campus partner with Financial Services to track and work to keep Gettysburg College PCI compliant. Questions regarding Gettysburg College's PCI compliance can be directed to the Vice President for Information Technology or Vice President for Finance and Administration.

Data Breach Reporting and Procedures

If a data breach is suspected or detected, the processes and procedures outlined in the *Gettysburg College Emergency Operations Plan Appendix A and IT's Internal Incident Handling document* would be triggered and followed within the specified time period of the shortest regulation or insurance agreement. Currently, regulations may require same day data breach reporting to the Department of Education. In addition, data breach table top exercises are performed for awareness and training.

Cybersecurity Program Assessment and Updates

In the spring of each year, the IT security team of the Vice President, Associate Vice President, and Director of Infrastructure & Computing, meet to review IT's Cybersecurity Program and other related compliance items. This team reviews the status of current security related goals and recommends goals for the upcoming year to be included in IT's Annual Goals.

Cybersecurity Knowledge Update

IT members receive critical security information updates from Homeland Security and other such organizations as Carnegie Mellon University's CERT organization. IT members regularly attend conferences, seminars, and webinars to receive security updates. In addition, the IT Leadership members belong to key professional organizations such as Educause and receive current technical knowledge articles and publications.

Resource Links

US CERT Security Tips

Last Update: January 2021