Information Security Policy
Gonzaga University

Revision Date: 04/06/2021

Contents

Information Security Framing Principles

The information security function at Gonzaga University adds value by successfully supporting the institution, mission, and goals of the University and by promoting good information security practices through the principles associated with the following three tasks:

1. Support the university:
    - **Focus on the institution** to ensure that information security is integrated into essential university activities.
    - **Deliver quality and value to stakeholders** to ensure that information security delivers value and meets university requirements.
    - **Comply with relevant legal and regulatory requirements** to ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided.
    - **Provide timely and accurate information on information security** to support university requirements and manage information risk.
    - **Evaluate current and future information threats** to analyze and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.
    - **Promote continuous improvement in information security** to reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.

2. Defend the university:
    - **Adopt a risk-based approach** to ensure that risk is treated in a consistent and effective manner.
    - **Protect sensitive information** to prevent disclosure to unauthorized individuals.
    - **Concentrate on critical university applications** to prioritize scarce information security resources by protecting the university applications in which a security incident would have the greatest business impact.
    - **Develop systems securely** to build quality, cost-effective systems on which the institution can rely.

3. Promote responsible information security behavior:
    - **Act in a professional and ethical manner** to ensure that information security-related activities are performed in a reliable, responsible, and effective manner.
    - **Provide relevant Cybersecurity Awareness Training** to all users, annually, and specific security training (such as Payment Card Industry (PCI) compliance training) as needed.
    - **Foster an information security-positive culture** to provide a positive security influence on the behavior of end-users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

The above tasks and their associated principles are supported by the establishment of an Information Security Framework. The Information Security Framework establishes security practices for Gonzaga University. Practices provide general, overarching guidance on matters affecting security that workforce members are expected to follow. Practices document methods and minimum compliance activities as appropriate to ensure that objectives are met.

Security practices apply to all hardware, software, data, information, network, personal computing devices, support personnel, and users within departments. Going forward, these components of information technology are covered by the umbrella term of “Information Resources.”

“Just enough” security

The ideal for any environment is to have “just enough” security. It is at this point that information is secure without overspending on needless or redundant security measures. The practices contained in this document allow business innovation and efficiency while ensuring that security is not overlooked or shortchanged.

As risks to Information Resources are identified, mitigating actions should always address root issues and not symptoms. While “just enough” security intends to put the proper emphasis on balancing security requirements with university opportunities, it should not be construed as minimizing the need for secure systems. To the contrary, any application or service exposing University Information Resources to unacceptable levels of risk should not be implemented if risks cannot be adequately addressed within budget constraints.

Information Technology Use Policy

In the event of an inconsistency between this Information Security Policy and the Information Technology Use Policy as applied to an employee’s use of IT Resources, the Information Technology Use Policy shall control.

Training

The practices contained in the Framework are easy to understand. Departments should not hesitate to point their workforce to those of special significance to their university mission. Expecting the workforce to understand and abide by all information security practices is a reasonable requirement of employment.

Enforcement

Fortunately, most University workforce members are hardworking and well-intended. However, when a workforce member commits a security violation, it needs to be addressed as a matter of discipline in accordance with the procedures in the Policies & Procedures Manual (PPM) or Faculty Handbook. Measures will obviously vary depending on the nature of the infringement. But it is a management responsibility to point out the error and entice proper behavior in the future to minimize continued and/or more serious mistakes. To reinforce the importance of security and assess the workforce’s adherence to practices, compliance with information security practices and procedures should be considered in all workforce member performance evaluations.
Though the possibility of disciplinary action for a violation is documented directly in some practices it is applicable to all practices and any violation.

Practice Overlap

The practices contained in this document have some overlap as a result of the comprehensive construct of the ISO/IEC 27001:2013* standard on which they are based. Where there is overlap, practice themes are consistent in their intent and objectives. To have a complete understanding of the University’s security practices, some issues may demand referencing more than one policy.

* ISO/IEC 27001:2013 is an international standard that gives guidelines for organizational information security standards and information security management practices.

Overview of Sections

Section 1– Security Practice: Discusses the scope of information security practices, as well as roles and responsibilities.

Section 2– Organizational Security: Addresses security responsibilities of the workforce, third parties, and outsourcers.

Section 3– Risk Assessment and Treatment: Documents the process the University will use to identify and assess risk as well as treat the risk through controls and practices.

Section 4– Asset Classification: Assures appropriate protection of University physical assets.

Section 5– Human Resources Security: Addresses the considerations with University workforce members prior to employment, during employment, and after employment.

Section 6– Physical and Environmental Security: Deals with the protection of physical areas and equipment from physical threats and unauthorized access.

Section 7– Communications and Operations Management: Addresses the many facets of information technology operations.

Section 8– System Access Controls: Tackles access restrictions for users at network, operating system, application and mobile computing levels.

Section 9– System Development and Maintenance: Deals with the many aspects of application development and maintenance security concerns.

Section 10– Information Security Incidents: Discusses the reporting and management requirement for security incidents.

Section 11– Business Continuity: Plans for interruptions of business activities.

Section 12– Compliance: Addresses the University's compliance with laws, regulations, security policies, controls and practices as well as audit considerations.

Section 1– Security Policy

1.1 Information security practice ownership and authority

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
   This Policy identifies responsible parties for the development and maintenance of information security policies. Departments are responsible for working with the Information Security Officer (or appropriate designee) to make policies complete and effective.

2. Revision history

3. Persons, groups, systems affected:
   All University employees, volunteers, contractors.

4. Practice
   The Information Security Officer (ISO) shall develop information security policies. Policies shall be regularly reviewed and updated to properly reflect changing risk conditions and mitigation opportunities. The primary goal for policies shall be to protect Information Resources commensurate with requirements for confidentiality, integrity, and availability. Additionally, policies shall protect the University's investment in information resources.

   The ISO shall educate through appropriate means, and with cooperation from University organizations, on policies that ensure information security.

   Each University organization shall formally delegate responsibility for all information security matters and interact with the ISO as needed. Organizations shall notify the ISO of issues requiring attention through policies as well as needed modification to policies. Organizations will work with the ISO or appropriate designee to monitor for practice compliance.

1.2 Information security practice establishment, approval, and exceptions

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice defines the process of security practice establishment, approval, and exceptions.

2. Revision history

3. Persons, groups, systems affected:

All University employees, volunteers, and contractors.

4. Practice

Information Security Practice Establishment

The authority to establish information security policies and practices is given to the Chief Information Officer. The Chief Information Officer has established the ISO position and delegated authority for the development and enforcement of approved information security policies and practices.

Information Security Practice Approval

Practices shall be consistent with other existing directives, laws, organizational culture, guidelines, procedures, and the University's overall mission. With these objectives in mind, IT shall develop practices through the inclusion of University department personnel and specialized expertise as appropriate and effective. University department IT staff and other appropriate audiences (dependent on content) may be asked to review and comment on draft practices. Practices shall be periodically compared with best practices appropriately incorporating changes in technologies, personnel, and business practices. The ISO or appropriate designee shall update practices as necessary and route them back through the review process.

Information Security Practice Exceptions

The ISO shall consider the need for waivers or variances based upon business requirements to established information security practice. Requests for practice exception shall be submitted to and approved by the ISO (or appropriate designee) before the waiver or exception may be implemented.

1.3 Information security practice violations and enforcement

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice instructs workforce members on the disciplinary ramifications for practice violations. Departments will consider the severity of the violation(s) and the negative consequences, and other pertinent factors in determining disciplinary actions.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Workforce members shall adhere to University information security practices. They shall follow the requirements and exercise appropriate judgment to ensure the protection of University information resources.

Workforce members will access only those Information Resources for which they are authorized. Accessing or attempting to access Information Resources without authorization is prohibited.

ITS retains the right to monitor workforce member's use of University Information Resources. This includes active monitoring (e.g., e-mail, keylogging) and historical analysis (email history, browser history and cache) among other measures (specifics regarding limits on monitoring of law school data can be found in the *Information Technology Use Policy*, Security and Privacy, page 6). The University recognizes the unique nature of digital information stored or created by the law school in the representations of clients; specifically, records covered by the attorney-client privilege, or otherwise relating to the authorized representation of a client, and the attorneys' professional and legal obligations regarding those records. (see *Information Technology Use Policy*)

Individuals found to be in violation of practices shall face disciplinary actions up to and including dismissal from employment in accordance with the procedures in the PPM and Faculty Handbook. Departments shall consider the severity of the violation(s), negative outcomes resulting from the violation, and other pertinent factors in determining the extent of discipline. Criminal prosecution is possible where the act constitutes a violation of law. A breach of contract, where applicable, may also apply. The University retains all rights to take whatever legal action it deems appropriate when investigating, monitoring, and/or remediating information security incidents.

Section 2– Organizational Security

2.1 Information security roles and responsibilities

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice establishes that the CIO and ISO are responsible for information security leadership. The ISO is responsible for developing and maintaining security practices, evaluating security risks, and working with Information Resource owners on protective measures. Department system owners, support providers, and workforce members also play key roles, and bear certain responsibilities, in securing Information Resources.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

IT Information Security, led by the ISO, shall coordinate resources to address the information security function required by Gonzaga University. The Information Security organization of ITS is responsible for providing guidelines and practices for securing information and its supporting resources. It is the responsibility of workforce members and agents of the University to communicate their security requirements for the protection of information to the Information Security organization.

All workforce members shall assume responsibility for complying with the University's information security policies and shall be aware that violations may result in discipline up to and including termination in accordance with the procedures in the PPM and Faculty Handbook. Criminal prosecution is possible where the act constitutes a violation of state and/or federal criminal codes. A breach of contract, where applicable, may also apply.

System users shall ensure the security of their systems by coordinating and overseeing the successful execution of sound operating practices and practice compliance by those providing support.

Independent audits of the information security program and of individual systems shall evaluate effectiveness on a regular, recurring basis.

2.2 Security of Third-Party access (Third Party Risk Management, TPRM)

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice addresses third parties using University Information Systems or executing business on behalf of the University or in addition to University employees. The expectations for trusted third parties are to protect University data to the same degree that is expected from University employees.

2. Revision history

3. Persons, groups, systems affected:

All University employees, volunteers, contractors, and third parties with access to University Information Resources, including emeriti faculty, and alumni.

4. Practice

Third parties shall gain access to University information assets only where there is a business need, only with approval of data and system owners, and only with the minimum access needed to accomplish the business objective.

Third parties with Gonzaga network* accounts shall be subject to the same policies and practices as are other members of the University workforce (e.g., accepting the Information Technology Use Policy) unless an exception is granted.

Standard contract language shall detail the security requirements of all parties involved in an agreement with audits conducted as needed to assure compliance. University information shall be protected whether used, housed, or supported by the University workforce or third parties.

(*See 8.3 *Network access control* for more information on “networks”)

2.3 Outsourced services contracts

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice directs departments to include enforceable security and audit provisions in contracts and agreements.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Data and system users shall ensure adequate protective controls are in place by outsourcers or contractors in the provision of services involving University Information Resources. Contractual requirements shall clearly define information protection requirements on the part of the outsourcer. These terms shall address expected protections through all aspects of operations and the lifecycles of Information Resources. Regular audits shall evaluate compliance with contractual terms and security requirements. Violations or failures to comply shall result in consequential actions determined necessary by the system owner up to and including contract termination.

Outsourcers shall comply completely with applicable University security practices. Data or system owners shall provide a copy of the University's practices to the outsourcer. Requests for practice exceptions shall be submitted by the data or system owner, on behalf of the outsourcer, to the ISO or appropriate designee.

Section 3– Risk Assessment and Treatment

3.1 Assessing security risk

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
This practice recognizes the importance of conducting risk assessments on Information Resources. A formal, disciplined approach to risk identification and classification is an organizational necessity to implement appropriate security measures.

2. Revision history

3. Persons, groups, systems affected:
All University employees and contractors

4. Practice
ITS shall perform risk assessments on University divisions' information systems and key technology assets. Assessing and mitigating risk is a mutual responsibility of ITS and the division owning the information asset.

ITS shall use a standard risk assessment methodology that is consistently repeatable and adequately considers threats to the asset. Risk assessments shall occur at regular intervals determined by threats, with the identification of new risks, or with impacting environmental changes.

Risk assessments shall have a defined scope (enterprise, department specific, system specific, component specific) and assign and agree to ownership of mitigation activities and compliance requirements.

3.2 Treating security risks

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice discusses the need for action plans once risks are identified. The clear expectation is that ITS will develop divisional mitigation strategies and adapt their security measures appropriately throughout the lifecycle of Information Resources.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall assure the development and execution of remediation plans and the ongoing monitoring of risks to their Information Resources. Risk treatment plans must include the scope of mitigation actions and controls.

Departments shall develop treatment plans for risks categorized as Severity 1 and 2, and asset owners* shall provide annual assessments of the risk treatment's effectiveness, evaluate the treatment's efficiency, and implement improvements.
The asset owner shall identify the controls necessary to ensure security of the asset as well as the means for measuring their effectiveness.

(**asset owner*: budget department responsible for the purchase of the asset)

Treatment plans shall be developed in design stages making certain requirements are accurately defined and enabling the incorporation of effective system controls.

Severity Rating	**Impact**
1	A. Network or system outage with significant impact to the user population or operation of the University. B. High probability of propagation. C. Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.) D. Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities. E. Notification of entities outside of the University is required.
2	A. Some adverse impact to the operation of the University. B. Adverse effects are localized or contained, or minimal risk of propagation. C. No apparent release or compromise of sensitive data. D. Remedial but not immediate action is required. E. Notification of entities within the University is required.
3	A. Minimal impact to small segment of user population or operation of University. B. Completely localized, with few individuals affected, and presenting little or no risk to other entities. C. No loss or compromise of sensitive data. D. Remedial action is required.

	E. Individual notification is required.

Section 4- Asset Classification and Control

4.1 Information Resources Stewardship

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice makes clear that ownership of Information Resources is the key to a secure environment. Each asset must have a specific individual responsible for all aspects of its proper maintenance and protection.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

All Information Resources must have a designated owner. For the purposes of this Policy, the designated owner is not the legal owner, but instead is the individual University employee who is responsible for the effective use and protection of the asset. Responsibilities include determining appropriate sensitivity classifications, criticality ratings, and access controls. Further, the designated owner is responsible for assuring compliance with the requirements of classifications and controls.

When there are several possible owners, ownership assignment shall go to the individual who makes the greatest use of the information. Information owners must establish specific policies identifying the roles, functions, processes, systems and applications that may have access to the information assets including the specific actions that the access privileges allow.

Owners shall ensure workforce members and agents of the University using their resource(s) are aware of their responsibility and held accountable for its protection and preservation. Owners shall spread this awareness appropriately.

There shall be sufficient degree of separation of duties among workforce members and agents of the University to ensure no individual has sole or complete authority for the modification or destruction of the subject information. With the exception of computer and network operations components, ITS personnel shall not be the designated owners of any department information.

4.2 Information asset categorization

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice directs divisions to classify their information. Data categorization then drives system designs and operations support methodologies to assure availability and protective requirements are attained.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Information Resources shall be categorized regarding sensitivity and availability requirements. Risk assessments considering severity and likelihood of risks along with cost factors determine categorization. Once determined, information assets and their requirements must be kept current in an information systems inventory.

Categorizing information shall be the responsibility of ITS and the Division that, by assignment of functional responsibilities, creates, collects or originates the information. All workforce members and agents of the University who develop information are responsible for assisting department leadership with the assignment to the appropriate category. All workforce members and users of the information are responsible for handling it according to its assigned category.

Categorization shall define operating requirements including but not limited to access to information, labeling and disposal rules, network and server designs, and disaster recovery planning.

4.3 Public disclosure of information

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets forth requirements for department authorization and limitations on the publication of information it owns.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Information shall only be released to the general public, regardless of its categorization, through established procedures approved and authorized by the department owning the information. IT or contracted hosting services shall understand their role as custodian of the information. Access, use, or release of department data shall only be given with the relevant Department's approval or as required by law enforcement with appropriate legal authorization in the form of a warrant, a court order, or the relevant Department's consent.

Workforce members, consultants, or contractors placing information in the public areas on the University's electronic infrastructure grant to the University the right to edit, copy, republish, and distribute such information in the event the University did not previously possess said rights.

4.4 Non-standard requests for information or access

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets guidelines for addressing requests for non-standard access to information and elevated privileges. Specific emphasis is placed on ITS operations staff due to their roles and the preponderance of requests they receive to give access to information.

2. Revision history

3. Persons, groups, systems affected:

All workforce members with specific guidance to Information Technology staff

4. Practice

Access to department data

University-owned information shall be used only for the purposes specified by designated owners. Use of these information assets for any other reason shall not be permitted without written authorization from the designated owner of the information. Unauthorized access to data by IT Service Operations or outsourced equivalents will result in prompt disciplinary action, up to and including immediate dismissal from employment in accordance with the procedures in the PPM and Faculty Handbook, criminal prosecution where the act constitutes a violation of state and/or federal criminal codes, and an action for breach of contract where applicable.

Internal department information requests

a. ITS staff shall not access, use, or release department data without the relevant Department's consent or as required by law enforcement with appropriate legal authorization in the form of a warrant or court order.

b. Employees receiving requests to monitor an employee's computer use or requests for access to a Department's data shall only do so with direct authorization from the Chief Information Officer, ISO, or where delegated via a formalized practice. By default, all requests will be routed through the ISO or appropriate designee. Other authorization channels should only be used as necessary to meet customer service expectations. Coverage includes access to emails, databases, files, and other information hosted or maintained by ITS.

c. Typically requests come from human resources, law enforcement, or as part of a public records inquiry. Service Operations staff shall not be burdened with trying to determine appropriate authorization for the request. The ISO or appropriate designee will confirm authorization and then engage the appropriate Service Operations staff to properly respond to the request.

d. Service Operations staff shall keep the matter strictly confidential so that the identities of individuals are protected. Workload requirements associated with the request may be discussed with managers, but they are not entitled to know the identity of any individual subject to the request.

Public information requests

a. Because it is not an agency under the state Public Records Act, the University is generally not subject to the Public Records Act. If, however, the University receives a public records request, ITS's ISO (or appropriate designee) shall coordinate with the University's General Counsel before responding to any public records request. ITS, in the role of custodian, will never provide University data or records in response to a public records request without appropriate approval.

ITS requests

a. ITS managers/supervisors wishing to review the files/email/computer use of an ITS employee must discuss the request with the Chief Information Officer.

b. Upon approval, the Chief Information Officer (or appropriate designee), not the manager/supervisor will engage the Information Security department for assistance. Such requests shall be based on reasonable suspicion of prohibited activity and will not be a substitute for management of an employee.

c. Persons conducting investigations of the Information Security department shall confer with the Chief Information Officer.

4.5 Personal and confidential information protection

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets guidelines for the protection of personal and confidential information. Every University workforce member is obligated to protect the personal information of constituents.

2. Revision history

3. Persons, groups, systems affected:

All workforce members and volunteers

4. Practice

Collection and Protection

Personal and confidential information shall be collected only where required by law and only used for purposes of the original intent. If not mandated by law or regulation, University departments should develop identifiers other than social security numbers for use in information systems.

The processing of personal and confidential information shall be kept to a minimum. Information systems containing personal and confidential information shall be closely restricted in their access. Departments with systems containing personal and confidential information shall establish rules for managing and protecting it.

Information systems shall incorporate protective measures that appropriately manage access, restrict its transport, discourage leakage, and ensure suitable and confidential destruction. Departments are responsible for, and must oversee the protection of, the personal and confidential information they collect and store.

In the event personal and confidential information is compromised all applicable laws shall be followed. Law enforcement shall be engaged as appropriate with chain of custody of information and evidence preserved. Timely notification of those adversely impacted shall be provided after the extent and cause of the compromise have been determined.

5. Definitions

Personal Information current definition:

(A) As used in this section, "personal information" means:
(1) An individual's:
(a) First name and last name; or
(b) First initial and last name; and

(2) At least one (1) of the following data elements:
(a) Social Security number.
(b) Driver's license number or identification card number.

(c) Account number, credit card number, debit card number, security code, access code, or password of an individual’s financial account.

(d) Gonzaga ID number

(B) The term does not include the following:

(1) The last four (4) digits of an individual's Social Security number.

(2) Publicly available information that is lawfully made available to the public from records of a federal, state, or local government agency.

Section 5 - Human Resources Security

5.1 Workforce security prior to employment

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
   This practice requires departments to exercise due diligence in securing their information assets through appropriate background checks of individuals. The degree of scrutiny shall vary depending on the involvement of the role with confidential or sensitive information.

2. Revision history

3. Persons, groups, systems affected:
   All University employees and contractors and volunteers

4. Practice
   All new hires shall undergo background checks commensurate with their job duties, or of those of the departments they support. The University Human Resources department sets standards for background investigations dependent on the role of the new hire.

   Departments shall communicate security responsibilities of the position during recruitment.

5.2 Workforce security during employment

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice confirms to departments that workforce members will receive training on acceptable use of University-provided information assets. Training will also be provided by the departments to address additional security requirements of their role.

2. Revision history

3. Persons, groups, systems affected:

All University employees, volunteers, and contractors

4. Practice

All workforce members shall receive annual Cybersecurity Awareness Training (CAT) and agree to abide by the Information Technology Use Policy (ITUP), within four weeks of beginning employment. Failure to accept the agreement will result in a loss of access to Information Resources unless the CIO grants an exception to the agreement and training.

Departments shall define and explain security responsibilities for the role played by the workforce member and make clear the ramifications of failing to comply. Workforce members shall be provided sufficient training and supporting reference materials to properly protect University owned information assets and resources.

Workforce members shall responsibly apply this training and support to protect the University's information assets. Workforce members shall address concerns regarding an activity prior to performing that activity if appropriateness is questioned.

Workforce members changing roles shall be appropriately subjected to additional security scrutiny and training before beginning a new role with more stringent security requirements.

5.3 Workforce security for terminated or changed employment

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice requires the timely elimination of access rights and appropriate return of assigned assets for employees leaving or changing roles in the workforce.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall assure that timely notification of terminated workforce members, as well as those changing roles, is provided to ITS and other technical support entities. ITS and other support providers shall promptly eliminate access capabilities of the terminated ID or an ID changing roles.

Departments shall confirm the return of all information assets in the possession of a terminated workforce member. An evaluation of all services used by the terminated workforce member shall determine the need for continuation (e.g. – phone, cell phone, flash drives, etc.).

The immediate manager of a workforce member or agent of the University no longer working on behalf of the University shall review both computer-based and paper files in their possession to determine the disposition of such files.

Section 6- Physical and Environmental Security

6.1 Secure areas

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
This practice instructs departments to consider the security requirements of their university information in determining appropriate physical access limitations and protections.

2. Revision history

3. Persons, groups, systems affected:
All University employees and contractors

4. Practice
University departments shall protect their physical areas consistently with the categorization of university information stored in the area regardless of format (printed, digital). Physical access to Information Resources shall be restricted to only those individuals needing access to them. Workforce members shall be granted the least level of access required to complete their job responsibilities.

Departments shall have procedures in place minimizing third party access. Visitors shall be monitored appropriately. Keys and access codes to secured areas shall be controlled to assure only authorized personnel gain access. Workers in secure areas shall tactfully confront unrecognized visitors for authorization and thoroughly understand access rights and restrictions.

Physical access rights shall be immediately removed for terminated staff and/or modified appropriately for staff changing roles. Departments may grant temporary access to workforce members and/or vendors requiring additional access to Information Resources for special projects, overtime, etc., provided the timely return to normal access is returned upon the conclusion of the project.

Delivery loading areas for data centers shall be isolated and enable inspection of deliveries.

6.2 Equipment security

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice conveys the requirement for departments to have adequate physical protections, regardless of their location, for their equipment assets from purchase through disposal.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall protect their equipment, including cabling, from physical threats and unauthorized access. Equipment requiring special protection shall be isolated or employ special physical protections according to need. Equipment shall be appropriately protected from power failures and surges as well as from heat, cold and moisture.

Equipment and software taken off-site shall be authorized by management. If physical protection for equipment is lacking, compensating control measures shall be implemented to protect information assets stored on the device.

Departments shall maintain IT equipment per manufacturer recommendations with service completed only by authorized providers.

Destruction of obsolete and damaged equipment, including storage devices, following The National Institute for Standards and Technology (NIST) 800-88, widely recognized as the current industry standard

Section 7- Communications and Operations Management

7.1 Operational procedures and responsibilities

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice requires departments to be involved and invested in the reliable, disciplined and secure management of their systems. Service providers impart technical experience and expertise but departments must be satisfied that necessary discipline in operational support results in the meeting of expected service and security levels.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments are responsible for ensuring that all people, processes, and technology they manage are compliant with Gonzaga Information Security policies and practices.

Departments shall ensure the correct and secure operation of information processing facilities employed by their service providers. Documented procedures shall define operating instructions and identify the roles and responsibilities of all parties.

Change Management best-practices should be implemented and enforced. An emergency change process shall be established to enable appropriate actions to prevent or respond immediately in the case of a crisis. Proper communication shall be provided to all parties potentially affected by changes as well as details regarding predicted impact. Security updates to software shall be applied within pre-defined timeframes except as emergency conditions dictate.

Service providers shall segregate duties to reduce the risk of unauthorized access, unauthorized modification, and misuse of information assets. Audit capabilities will enable the monitoring of typical users as well as those with elevated privileges.

Storage of data shall be limited to networked storage devices. Exceptions to this practice shall be permitted only with the authorization of the system owner and department leadership. In instances where personal information is authorized for local storage the drives shall be encrypted.

All computer-resident information that is classified as sensitive should be located on computers and networks that have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

7.2 Outsourced service delivery management

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets the clear expectation for departments regarding their ownership of system information regardless of the business relationship to the application developer or host services provider. The protection of information and service level agreements (SLAs) of outsourced providers are to be managed aggressively and effectively by departments.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

The University shall always maintain control of security aspects of services provided to or on behalf of the University by third parties. Third party service providers shall be subject to documented SLAs that are measured and enforced by University departments.

Third party providers shall abide by terms of contracts and agreements stipulating the processes, controls and audits to be employed to ensure the security of University information assets. Among the disciplines expected of third-party providers are configuration management, capacity management, change management and disaster recovery planning.

7.3 System planning and acceptance

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice recognizes the importance of a structured and consistent systems development and acceptance methodology.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

With assistance from ITS, departments shall structure agreements for system development in a manner assuring their completion within acceptable timeframes, consistent with cost projections, and with fulfillment of department development architectures or industry best practices that ensure secure application code and operations.

Systems shall be protected from failure allowing for redundancy where required to reach service level agreements.

System owners shall obligate their service provider to adhere to applicable programming, database, and hardware standards.

Departments shall not accept a system until it meets testing criteria.

All systems shall have completed operational documentation prior to the system's use in a production environment. The documentation must be written so that the system may be run by persons unacquainted with it.

Operations staff shall be trained to monitor and maintain the system.

7.4 Protection from malicious software

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice addresses the continual threat posed by malicious software. Malicious software has many entry points into the University's operating environment. Workforce members must be diligent in protecting against malicious software and may be subject to discipline through the procedures in the PPM and Faculty Handbook for malware damage resulting from their negligence.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall protect against malicious code by ensuring that anti-virus software is installed as part of ITS support practices on University-owned, University-operated or University-authorized information systems. ITS will set an appropriate interval for automatic updates as well as scan settings for various file types and computer accessories (e.g. – flash drives).

Departments shall ensure all software, including internally developed application software, is free from malicious code before installation onto a computer or other system asset.

Workforce members shall not distribute malicious code or disable anti-virus software. Encounters with malicious code on University-owned computing devices shall be reported to department contacts who will then notify the ISO (or appropriate designee). Incident management procedures shall be pursued as dictated by the event.

Storage of "confidential" and/or "internal use only" information on non-University equipment is strictly forbidden.

Departments shall create and/or distribute to all users the appropriate instructional materials for malicious code security on University-owned devices as described throughout this practice.

Departments shall ensure that procurement processes contain assurances (e.g. - contract terms) that software obtained is free from malicious code.

7.5 Data backup

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

The purpose of the Data Backup practice is to provide for the continuity, restoration and recovery of critical data and systems. Departments need to ensure critical data is backed up periodically and copies maintained at an offsite location. Data backups are not conducted to meet or be capable of satisfying Gonzaga University retention requirements.

2. Revision history

3. Persons, groups, systems affected:

All University departments

4. Practice

With assistance from ITS, all University departments shall ensure that backups conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up (includes all patches, fixes and updates)
- Records must be kept of information backed up and how and where it is maintained
- Records of software licensing should be backed up
- Sufficient generations of back-up data must be retained to assure recovery and restoration is compliant with prescribed service levels
- The backup media must be precisely labeled, and accurate back-up records must be maintained
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site
- Regular tests of restoring data/software from the backup copies should be undertaken to ensure that they can be relied upon for use in an emergency
- Data backed up shall be encrypted

Individual workstations connected to a University network shall not be backed up through a service provider without written approval of the CIO. Users shall store data on servers rather than locally, especially files containing personal information. In exceptional cases, responsibility for data backup on a local drive rests with the user. Where exceptions require systematic backup of workstations, the extent shall be defined, coordinated with the service provider, and tested for effectiveness.

Departments shall assure proper destruction of backup media when retired.
Standard backups shall not be the means of complying with records retention requirements.

7.6 Network management

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice intends to ensure reliable and secure network services. The practice directs departments regarding the establishment of network services and sets expectations for the providers of network services.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Local area networks and wide area networks used by University departments shall be supported through a means determined by the Department of Information Technology Services. Under no circumstances shall new local area networks (LAN's) be established, nor the technology of existing University networks varied without ITS approval. Workforce members shall not connect networking gear without ITS authorization.

Wireless networks connected to the University network shall be installed and supported by ITS. ITS shall maintain a documented database for the network. This information shall be kept electronically and must be backed up regularly.

Security patches shall be applied within established timeframes on University networking equipment.

Network infrastructure shall be periodically scanned (e.g. quarterly or after significant changes) for known vulnerabilities. All software configurations for network equipment shall be backed up on a regular cycle (e.g. daily or weekly) and a copy stored securely off-site.

Physical access to network devices shall be restricted to prevent unauthorized access. All physical locations housing network equipment shall be accessible only to authorized personnel both during and after normal business hours. Third party access to these facilities shall be allowed only with approval of ITS. Third parties must adhere to documented network and data security practices and standards while working.

Access to management functions within network equipment shall be limited through implementation of strong authentication measures. Passwords shall change from those as shipped from the manufacturer. Periodic password control (employees leaving, etc.) or other methods such as Radius, TACACS, or Active Directory integration shall be implemented.
Services not needed from devices shall be removed (e.g. web server, SNMP, FTP, etc.). Remaining services shall be set up with strong passwords (SNMP community strings are the equivalent of passwords and shall be changed from the vendor-provided defaults). Access control lists shall be used to limit access to services needed.

Access shall be restricted from Internet and University network locations not needed. Filters, access lists, or firewalls shall be used to limit access to the management interface and/or services available on the device. Firewall default behavior shall deny all communications/connections that have not been explicitly permitted.

7.7 Media handling

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice directs departments on handling media of all types through its lifecycle.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

With assistance from ITS, departments shall ensure the safety of their information through appropriate media protection measures whether in use, storage, or transit. Protection schemes must consider losses from theft, unauthorized access, and environmental hazards.

Departments shall review media handling procedures, document storage, distribution, and disposal requirements ensuring they appropriately consider data classification. Erasure and destruction parameters shall assure disposal without data compromise.

Department system documentation shall specify the number of backup copies to be maintained considering importance, restoration requirements, and availability requirements.

7.8 Exchanging information and software

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
This practice sets the integrity and security requirements for communications in department operations.

2. Revision history

3. Persons, groups, systems affected:
All University employees and contractors

4. Practice
With assistance from ITS, departments shall ensure that exchanges of information between the University, its workforce, and third parties consider relevant laws, regulations, contractual terms, and other agreements.

Personal information and other confidential materials shall not be included in unencrypted emails unless as part of an agreed upon process between University departments. Sending personal information to non-University systems, including email and other transmissions, unless appropriately protected in transit from unauthorized disclosure and physical damage is prohibited.

Departments shall not use non-University e-mail systems to conduct University business. ITS shall deploy technology and expertise to reduce Spam and malware from entry to the University's email system.

Departments shall communicate requirements of workforce members regarding use of voice, facsimile, email, and video communications.

7.9 Electronic commerce services

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets requirements for departments choosing to conduct electronic commerce services.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments implementing electronic commerce for receipt of payments or delivery of benefits shall be in compliance, at minimum, with current PCI Data Security Standards before beginning operations. Systems shall be managed to stay PCI-DSS compliant throughout the life of the service.

Electronic commerce transmission controls shall maintain integrity and verify authenticity while mitigating risks of introducing malicious code.

Gonzaga University has contracted with a company specializing in Internet commerce and transactions. All entities intending to provide electronic commerce services over the Internet shall consult with the University's Controller's Office to ensure consistency with the University's Internet commerce direction and with expected application safeguards.

Third parties conducting e-commerce on campus shall comply with the payment processing policy.

7.10 Event log monitoring

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
- This practice sets requirements for monitoring event logs of key Information Resources.

2. Revision history

3. Persons, groups, systems affected:
- All University employees and contractors

4. Practice

Departments shall monitor their applications for unauthorized information processing activities, record events, and document circumstances around anomalies.

ITS workforce members shall monitor data communications infrastructure and all centrally supported systems, services, and applications to meet operational objectives and to maintain a secure environment. Monitoring shall include key measurements for each device supported. Authorized technicians may actively scan Information Resources to identify vulnerabilities and/or compromised hosts. Technicians shall exercise due diligence when performing any scanning activity to preserve production capabilities. Thresholds for alarms and alerts shall be configured to identify possible security breaches including intrusion events or violations of practice.

ITS and authorized technicians must execute their duties respecting the privacy of others. Information discovered in the monitoring process shall not be used or disclosed for purposes other than those for which the process was approved. Exceptions include potential illegal or grossly inappropriate activities uncovered unintentionally. Such findings shall be discreetly disclosed to appropriate management for their evaluation and action.

The ISO, or appropriate designee, will routinely scan all on-campus network-connected devices for vulnerabilities, and to ensure consistent and appropriate security settings.

The University shall use video surveillance equipment in areas requiring monitoring to ensure the provision of security to both the workforce and to Information Resources.

Any information residing on any server or workstation owned by the University, connected to the University's networks or located on University premises may be examined with appropriate justification by authorized University department personnel or technicians acting on their behalf. This Practice includes University owned machines used at home and personal systems that are connected to the University's network (including VPN).

Web history shall be logged for a brief period and individual activities may be researched in cases of suspected unauthorized or inappropriate use.

Any workforce member engaging in monitoring activities without proper authorization shall be subject to disciplinary measures up to and including termination in accordance with the procedures in the PPM and Faculty Handbook. Criminal prosecution is possible where the act constitutes a violation of state and/or federal criminal codes. A breach of contract, where applicable, may also apply.

Section 8- System Access Controls

8.1 Business requirements and access control

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
   This practice sets expectations for access to University information systems.

2. Revision history

3. Persons, groups, systems affected:
   All University employees and contractors

4. Practice
   Access to Information Resources is granted based on defined and documented roles. Access to Information Resources shall be consistent between workforce members in the same role. Access rights to information will be at the minimum required to successfully accomplish work responsibilities.

   Special or administrative privileges require a different ID than one used for normal business and shall only be used when performing tasks demanding the exceptional rights.

   Elevated privileges shall be granted only to workforce members needing them to complete their duties. This number shall be limited to the minimum number possible without compromising service levels.

8.2 Workforce access management

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for workforce access to systems.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall require each workforce member to have a unique ID with GU Information Resources access limited only to authorized users subject to defined limitations. User access rights shall be regularly reviewed by system owners to assure optimal access to information is granted by the system.

Workforce members shall change passwords at initial login, never share passwords, and change passwords securely.

Departments shall limit the number of staff with elevated privileges to the minimum number required to assure appropriate service levels. Workforce members shall only modify production data through an approved, controlled process.

Auditors, information security administrators, programmers, computer operators, or system administrators shall not update production university information. Computer operations staff shall have access to, or be permitted to modify production university information, production programs, or the operating systems only when essential and only with supervisors’ approval.

Special or administrative privileges require a different ID than one used for normal business and shall only be used when performing tasks demanding the exceptional rights.

8.3 Network access control

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for network access.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

ITS is responsible for maintaining the networks used by University departments. Information Resources connected to Gonzaga University-owned or operated networks shall comply with the minimum standards for security set by ITS. University departments may develop stricter standards as dictated by their university missions. ITS may disconnect devices that do not meet minimum standards for networked host security configurations.

Access to network resources owned, operated, or paid for by the University shall be limited to authorized users and to those services required. Users shall only use external connections operated or approved by ITS. Workforce members and vendors must not make arrangements for, or actually complete the installation of, data lines with any carrier or through any means without express approval from ITS management. All external connections to internal computer networks shall pass through an access control point for authentication prior to allowing entrance.

Access to non-guest network resources requires user authentication. Users and devices must use encrypted authentication mechanisms unless otherwise granted an exception by the ISO (or appropriate designee).

System security requirements shall dictate segregation of networks. Network routing ensures only allowed paths to services are used. If a service is not necessary for the intended purpose or operation of a network device, that service shall not be running. Network gateways shall be equipped with needed filters.

ITS shall inventory network equipment. Devices shall be physically located in an access-controlled environment wherever possible. Firmware versions shall be upgraded as soon as practical. Access to network devices shall be physically and logically limited to authorized personnel with diagnostic port access limited and audited. Changes to network device configurations shall be documented and implemented via an established change control process.

ITS shall regularly audit network services to assure protection from security risks.

8.4 Operating system access control

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for operating system access.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Responsibility for maintaining all servers used by University departments shall be clearly established and kept up to date. Access to servers owned, operated, or paid for by the University shall be limited to authorized users. Server access shall require user authentication with password files encrypted. Shared IDs shall be permitted only as exceptions, approved by management, and documented. Users shall be disconnected from servers at defined inactivity time-out intervals.

ITS shall inventory servers and ensure they are physically located in an access-controlled and environmentally protected area. Server ownership shall be documented and include:

- the server contact(s) and location, and a backup contact
- hardware and operating system/version
- main functions and applications

Operating systems shall have security patches applied as soon as practical utilizing required change control procedures. User activity and security event log information shall be monitored and maintained. Operating system services unnecessary for the intended purpose service shall not be running. Administrative functions shall be performed with unique privileged IDs traceable to an individual and only when non-privileged accounts are insufficient for the necessary task.

“Root” or “administrator” account use shall be limited to only those with a business need for such access. Access to system utilities shall be limited to authorized resources.

ITS shall regularly audit all servers to assure protection from security risks.

8.5 Application and information access control

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for application access.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Applications shall permit only authorized user access and limit access to stored information through approved methods. Sensitive systems shall be physically and logically isolated to the degree necessary for protection.

Applications shall have security patches applied as soon as practical utilizing required change control procedures. User activity and security event log information shall be monitored and maintained.

Access to applications shall require user authentication. Users must use encrypted authentication mechanisms unless otherwise granted an exception by the ISO (or appropriate designee).

Only licensed applications shall be installed on University-owned devices.

Departments shall regularly audit applications to assure protection from security risks.

8.6 Mobile computing and teleworking

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets requirements for workforce members working at home or at off-site locations.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Workforce members authorized to work from home or off-site locations shall be subject to all University security policies and practices. Provision of equipment and connectivity shall be determined between the workforce member and University department. Use of University provided equipment and connectivity to University networks shall be limited to authorized University workforce members. Connectivity to University networks shall be made only through ITS approved services.

Information stored or created by workforce members on behalf of the University shall be on University provided media. Whether created in a University facility or while telecommuting the work product remains the property of the University, subject to any intellectual property rights held by an employee pursuant to University policy or separate agreement between the University and an employee. The University may examine University equipment used by its workforce when circumstances merit an investigation. With the exception of information which the workforce member is professionally or legally obligated to protect as confidential client information, workforce members shall have no expectation of privacy associated with the information they create, store, or send through these University systems.

Non-University owned devices connecting to the University network must be approved by the department authorizing the connection and shall have appropriate operating security patches and virus protection software. Additionally, non-University owned devices will be required to “register” with the University’s mobile device management solution and run all applications deemed necessary to protect University data as determined by ITS.

Section 9- System Development and Maintenance

9.1 Security requirements of information systems

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for security requirement consideration in the design and development of department applications and that they are continually maintained through the lifecycle.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

With the assistance of ITS, University departments shall identify and design security requirements in the business process of developing applications. This includes user-developed applications. Defined security requirements shall be met through purchasing and development decisions.

With the assistance of ITS, University departments shall develop applications with secure code. Secure code results from trained staff, established standards, conducive development environments, and proven methodologies. Secure code shall be certifiable by objective, independent parties. Contract provisions for third-party application development should provide enforceable and effective protection regarding application security.

With the assistance of ITS, University departments shall evaluate security history and standards of commercial software providers before purchasing their products. Departments shall follow all University and ITS security and procurement practices prior to selecting vendors. University departments are ultimately responsible for the security of the products implemented and shall select and manage their vendors accordingly.

Effective patch management, auditing, logging, and lifecycle management (or enhancement) programs shall be incorporated into the support and maintenance strategies for all applications.

Non-commercial or internally developed applications shall not be installed on University systems without the prior approval of ITS.

9.2 Correct processing in applications

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations that new applications and changes to existing applications work correctly.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

University departments shall implement controls and audits of their applications to prevent errors, loss, unauthorized modification, and misuse of information. System controls shall ensure data integrity and protect against corruption. Data output shall validate correct processing.

9.3 Cryptographic controls

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets forth requirements for using encryption technologies.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Under guidance from ITS, University departments shall apply encryption technology to assure the prevention of disclosure of electronic information to unauthorized parties. Departments shall consider encryption technology when physical security measures are lacking, when traditional layers of security are not in place (e.g. – firewall), or when necessary to protect the information sufficiently. The ramifications of encryption on system performance shall be considered before implementation.

University departments deploying encryption technology shall have an encryption key management plan. This plan must ensure that data can be decrypted when access to data is necessary. This requires backup or other strategies to enable decryption to ensure data can be recovered in the event of loss or unavailability of cryptographic keys. The plan must also consider handling compromise or suspected compromise of encryption keys.

Departments encrypting data at rest shall ensure information availability. University information shall be stored in a known location in unencrypted form, or if encrypted, the means to decrypt the information must be available to more than one person.

Encrypting data in transit shall be applied where confidential information faces unacceptable risk of exposure if intercepted or misrouted. A secure method shall be used to convey the decryption measure to the recipient.

Users shall be aware of their responsibilities if given the role for maintaining control of cryptographic keys. Management of encryption keys and key management software and hardware must be supervised and authorized by department leadership.

All laptops shall utilize whole-disk encryption solutions to secure the data stored on them.

9.4 Security of system files

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets requirements for securing key aspects of applications operations and testing.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Department IT project and support activities shall use appropriate controls to assure integrity and confidentiality in the eventual production system. Change control procedures shall protect program libraries and test data. System reviews assess the effectiveness of controls and identify improvements. Audit trails exist for all changes.

Use of live data is prohibited for testing and all test data shall be de-personalized.
Departments shall restrict access to operational source program libraries. Access shall be auditable. Old versions shall be archived.

9.5 Development and support processes security

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice describes security requirements for systems development and support.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall strictly control project and support environments enabling the timely development of quality applications. Change control procedures to development and support environments shall require authorized, documented, and audited changes.

Application support teams shall evaluate changes for impacts to applications and shall obtain approval by system owners prior to applying patches and/or operating system updates.

Departments shall purchase applications only from reputable sources where confidence in source code quality is high. Changes to off-the-shelf software applications shall be made only in compliance with licensing terms.

Departments shall manage outsourced software development to assure favorable licensing terms and certification of code quality. Continued audits to application security shall be a part of the ongoing maintenance process.

Systems shall appropriately separate development, test, and production facilities. Development and test systems shall not use production data.

9.6 Technical vulnerability management

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for departments to monitor their systems for vulnerabilities.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Working with ITS, departments shall ensure that application support providers proactively monitor and remediate published software vulnerabilities. Identified vulnerabilities shall be assessed for the degree of risk posed to information resources. Patches and updates addressing vulnerabilities shall be applied in a manner consistent with the level of risk. Fixes shall be evaluated and tested prior to moving into production.

Section 10- Information Security Incident Management

10.1 Information security incident reporting requirements

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets expectations for reporting security incidents.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall communicate information security incidents through documenting events, identifying the scope of the incident, and notification of owners of impacted information or assets. Communications shall adhere to applicable laws and pre-defined communication procedures. Security incidents shall be reported in a timely manner. Departments shall train staff on incident reporting requirements.

Workforce members must report all suspected information security incidents as quickly as possible to the Chief Information Officer or ISO (or appropriate designee).

10.2 Information security incident management

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice establishes department requirements for handling security incidents.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Departments shall report security incidents to the Chief Information Officer or ISO (or appropriate designee). They will then engage the information security Incident Response Triage Team (IRTT) for their analysis and guidance in handling the incident.

With the assistance of ITS, departments shall develop incident handling procedures that enable the effective handling of incidents by appropriate levels of technical and managerial staff. Procedures shall assure incident investigations are complete and minimize further damage.

Departments shall respond quickly and with organization to assure an effective response. Incidents shall be studied, and preventative measures identified and implemented to inhibit recurrences.

Departments shall assure incident handling procedures consider the collection and handling of evidence for law enforcement and other evidentiary purposes.

Section 11- Business Continuity

11.1 Business continuity management

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
   Describe the expectations for managers of Distributed IT units (IT services provided outside of the standard ITS division; Distributed IT is primarily found in the School of Engineering and Applied Science) to ensure effective business continuity for services they manage.

2. Revision history

3. Persons, groups, systems affected:
   All University employees and contractors

4. Practice
   ITS shall work with University organizations to document plans for interruptions to business activities and protect critical business processes from the effects of major failures or disasters. ITS and University organizations shall identify their critical processes, identify their recovery requirements, and assure recovery plans are in place.

   ITS shall work with University organizations to develop response strategies for known impacts of interruptions, with measures in place to successfully restore services in defined timeframes. Plans shall identify parties and their roles and emergency procedures.

   Resumption procedures shall consider emergency and fallback plans and testing schedules. Departments shall assure that business continuity plans are tested, and that documentation is updated regularly.

Section 12- Compliance

12.1 Information system compliance with legal requirements

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose
   Describe the expectations for use of University provided Information Resources considering pertinent legislation.

2. Revision history

3. Persons, groups, systems affected:
   All University employees, and contractors

4. Practice
   Department information systems shall comply with all applicable laws, regulations, and contractual obligations. Procedures shall be implemented to assure compliance with statutes, regulations, licensing agreements, and intellectual property rights. Procedures shall also assure the protection and retention of essential records with retention schedules following Gonzaga University guidelines.

   Protection of personal information contained in department systems shall at a minimum meet levels required by legislation. Current definitions of “personal information” and/or “personal data” should be in accord with the European Union’s General Data Protection Regulation (GDPR).

   Departments shall assure Information Resources are used for authorized business purposes only.

12.2 Auditing information systems

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice notifies departments that regular security audits will be performed on their information systems.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Department information systems shall be subjected to security reviews ensuring compliance with controls and practices. System reviews shall address identified shortcomings through action plans.

12.3 Requirements of security audits

Effective Date: April 9, 2021
Last Updated: April 9, 2021
Responsible University Office: Information Technology Services (ITS)
Policy Contact: Information Security Officer (ISO)

1. Purpose

This practice sets forth requirements for conducting required information system audits.

2. Revision history

3. Persons, groups, systems affected:

All University employees and contractors

4. Practice

Department information system audits shall safeguard information and productivity while being conducted. Use of audit tools will be approved by impacted support organizations and used only for authorized audits. System audit tools shall be stored appropriately to prevent misuse or compromise. Access to the tools shall be controlled and permitted only to authorized users.

Information systems owners and application owners shall agree on system audit scope, timing, and the resolution of discovered vulnerabilities.

Security reviews are conducted only with authorization and qualified personnel performing security tests.