Information Security Policy

Objective

Whitworth University is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets entrusted to Whitworth University to ensure that regulatory, operational, and contractual requirements are fulfilled.

Whitworth University will take a risk-based approach to information security to ensure that students, investors, and employees have the appropriate balance of services and opportunities at a level of risk that suits the needs of the organization.

Whitworth University recognizes that perfect security will never exist, and no organization will ever be 100% risk free; this program is designed to manage risk and regulatory compliance in an appropriate manner, to ensure the appropriate balance of risk and value to our students, faculty, and staff.

Goals

The policy's goal is to protect the organization's informational assets against all internal, external, deliberate or accidental threats.

- Executive Leadership has approved the information security policy.
- The security policy ensures that:
    - Information will be protected against any **unauthorized access;**
        - **Confidentiality** of information SHALL be assured;
        - **Integrity** of information SHALL be maintained;
        - **Availability** of information for business processes SHALL be maintained;
        - **Legislative, Contractual, and Regulatory** requirements SHALL be met;
        - Where applicable and appropriate, **Privacy** SHALL be met.

- **Information security training** will be available for all employees;
- **All actual or suspected information security breaches** will be reported to the Information Assurance Team and will be thoroughly investigated.
- Procedures exist to support the policy, including virus control measures, passwords and continuity plans.
- Business requirements for availability of information and systems will be met.
- The Information Assurance Team is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.
- Any time that an Information Security policy, standard, procedure, guideline, or other governance document conflicts with the health or safety of a student or employee, that governance document must be followed, only to the extent that the health or safety of a student or employee is not compromised.

- Situations where the health safety is adversely affected by such a governance document MUST be communicated to the Information Assurance Team and/or to Cabinet/executive leadership team members.

All information collected, processed, stored on or transmitted over Whitworth University's computer systems and networks will be treated as a Whitworth University's corporate asset and SHALL belong to Whitworth University; exclusively, unless specifically authorized or where laws exclude such an exemption.

Policy Statements

It is the policy of Whitworth University to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of our sensitive information assets. Whitworth University will maintain an information security program that is designed to control risks associated with access, use, storage, sharing, and destruction of sensitive employee, student, and financial information.

This Whitworth University's IT Security program manual is the master governing document for all IT security related matters and supersedes any guidance that is less secure, and all previously issued IT security governance documents.

Whitworth University recognizes the immense value and importance of its employees, facilities, assets, information, and tasks employees, contractors, students, staff and faculty to be committed to ensuring their continued protection.

Whitworth University shall protect its employees, facilities, assets, information, and information technology assets at a level appropriate to the prevailing security threat, with standards and best practice defining the minimum level of achievement.

Information Management shall be a consideration at the design and development stages of every business activity and not merely during implementation.

Whitworth University shall seek to make continuous improvement in methods of threat analysis and information management so that it can protect itself appropriately.

This policy document shall be approved by the Whitworth University Cabinet/executive leadership team, published and communicated, as appropriate, to all employees and identified stakeholders.

This policy shall be reviewed annually, and in case of influencing changes, to ensure it remains appropriate.

Whitworth University IT Security Program Manual shall comply with the Whitworth University Information Management Framework and be guided by ISO 27002:2013.

Enforcement

Failure to comply with Whitworth University's Information Security policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws. Violations by students will include disciplinary actions up to and including expulsion.

In the event that any person violates any provision of this policy, management will ensure a formally documented discussion occurs, based on the severity.

Summary of Responsibilities

All employees, contractors, students, staff and faculty:

1. You may only access information needed to perform your legitimate duties as a Whitworth University employee and only when authorized by the appropriate Business data owner or designee or the Information Assurance Team.
2. You are expected to ascertain and understand the sensitivity level of information to which you have access through training, other resources, or by consultation with your manager or the business data owner.
3. You MUST NOT in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the Business Data Owner within the scope of your professional activities.
4. You must understand and comply with Whitworth University's requirements related to personally identifiable information (PII), sensitive student information, cardholder data, and all other data protection requirements.
5. You MUST adhere to Whitworth University's requirements for protecting any computer used to conduct Whitworth University business for any computers used to transact Whitworth University business regardless of the sensitivity level of the information held on that system. This includes reporting known or suspected security issues, concerns, or breaches to the Information Assurance Team.
6. You MUST protect the confidentiality, integrity and availability of Whitworth University's information, as appropriate for the information's sensitivity level, wherever the information is located (e.g., held in physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.).
7. Information deemed Confidential under this policy MUST be handled in accordance with Whitworth University's requirements for protecting non-public information.
8. You MUST safeguard any physical key, ID card or computer/network account that allows you to access Whitworth University's information. This includes creating difficult-to-guess computer passwords and passphrases.
9. You MUST destroy or render unusable any confidential information contained in any physical document (e.g., memos, reports, microfilm, and microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded or take it to the IT Department for appropriate disposal.

10. You MUST report any activities that you suspect may compromise sensitive information to your supervisor or to Whitworth University's Director, Network Services & Information Security.
11. Your obligation to protect sensitive information continues after you leave Whitworth University.
12. Any data that is not publicly released remains the property of Whitworth University and MUST NOT be released without written approval; this too extends to after you leave Whitworth University. NOTE: there are laws that govern educational institutions and that require additional protection; from a cybersecurity standpoint.
13. While many federal and state laws create exceptions allowing for the disclosure of non-public information to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests should contact Whitworth University's Information Assurance Team or legal team before taking any action; unless a written policy allows such a disclosure.
14. All standards, written by management, are an extension of this policy and MUST be followed. In situations where they cannot be followed or should not be followed, a risk acceptance waiver must be attained.

Assignment of Duties

Whitworth, under the direction of the COO has assigned its Director, Network Services & Information Security to be the point person overseeing its Information Security policy and environment including policy and procedure development and compliance, system security, log management, intrusion and attack detection and ISO-27001 development and compliance.

In addition, Whitworth has engaged Arctic Wolf Networks to act in the role of our SIEM. In that role they are assisting Whitworth in the continuous monitoring of the network and providing guidance and expertise on policy development, audit compliance and breach protection and management.

Throughout the Information Security Program, the Director, Network Services & Information Security when duties are shared with the Arctic Wolf Networks Team SHALL be referred to as the Information Assurance Team.

The COO is a member of both the President's Cabinet and assigned to the Whitworth Board of Trustees Audit committee and is responsible with informing, receiving guidance and developing policies, procedures and plans in concert with Cabinet and Audit committee priorities and all applicable federal and state regulations.