USAO Written Information Security Program

Purpose and Scope:

The University of Science and Arts of Oklahoma (USAO) has successfully implemented a comprehensive Written Information Security Program (WISP) in accordance with the Gramm-Leach-Bliley Act (GLBA) requirements. USAO has a designated the IT director as the "Qualified Individual" responsible for overseeing, implementing, and maintaining the information security program.

Our WISP includes the design and implementation of administrative, technical, and physical safeguards to manage identified risks effectively. We conduct regular testing and monitoring of these safeguards to ensure their effectiveness. Additionally, we have established policies and procedures for security awareness training, ensure that all personnel with access to GLBA data receive appropriate training annually.

Furthermore, the USAO oversees our service providers by requiring them to maintain a written comprehensive information security program. Our incident response plan is in place to address any potential security breaches promptly.

The WISP is regularly reviewed and updated to address new security risks and to ensure ongoing compliance with applicable regulations.

1. Definitions

For the purposes of this WISP, the following definitions apply:

Nonpublic Financial Information (NFI): Any information that a student or other third party provides in order to obtain a financial product or service from the University, any information about a student or other third party resulting from any transaction with the USAO involving a financial product or service, or any information otherwise obtained about a student or other third party in connection with providing a financial product or service to that person.

Covered Data: All NFI that is accessed, collected, distributed, processed, protected, stored, used, transmitted, or disposed of by the University.

2. Information Security Program Coordinator

The IT Director is designated as the Information Security Program Coordinator (ISPC). The ISPC is responsible for coordinating and overseeing the WISP. The IT Director reports directly to the President of the Institution who is responsible for direction and oversite of the ISPC.

Duties of the ISPC include but are not limited to:

- Initial implementation of the WISP
- Regular testing of the WISP safeguards
- Evaluating the ability of third-party service providers to comply with the GLBA
- Reviewing the WISP periodically, at least annually
- Reviewing staff training and procedures to ensure compliance

3. Risk Assessment

The USAO will identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of NFI that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information of such information, and assesses the sufficiency of any safeguards in place to control these risks. This shall be done periodically and may be done on an annual basis and documented by the ISPC.

The risk assessment shall include:

- Employee training and management
- Criteria for the assessment of the confidentiality, integrity, and availability of the information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats faced.
- Implement policies, procedures, and controls that are designed to monitor and log the activity of authorized users to detect any unauthorized access or tampering of NFI.
- The ISPC will implement multi-factor authentication for any individual who uses or has access to NFI.
- The ISPC will develop and implement procedures for secure disposal of customer information in any format. This will be done within two years after the last date the information is used in connection with a provision of a product or service, unless otherwise noted.
- Describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risk.
- Detecting, preventing, and responding to attacks, intrusions, or other system failures.
- Develop practices for in-house applications utilized by USAO, for transmitting, accessing, or storing customer information. Procedures to evaluate, assess, or test the security of externally developed applications that USAO uses to transmit, access, or store data will be developed.
- Adopt procedures for a change management.

4. Employee Management and Training

USAO will:

- Check references and conduct background checks before hiring employees who will have access to covered data.
- Periodically review access controls, including technical and as appropriate, physical controls to:
    - Limit access to covered data to employees who have a business need to see it.
    - Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis.
    - Use password-activated screensavers to lock employee computers after a period of inactivity.
    - Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices.
- Train employees to take basic steps to maintain the security, confidentiality, and integrity of covered data, including:
    - Locking rooms and file cabinets where paper records are kept
    - Encrypting sensitive student information when it is transmitted electronically
    - Regularly remind all faculty and staff of USAO guidelines to keep critical information secure and confidential.
- Utilize the qualified information security personnel to oversee the security program.
- Provide training sufficient to address relevant security risks.
- Verifying that key personnel take steps to maintain current knowledge of threats and countermeasures.

5. Information Systems

USAO will:

- Know what student information and personal information is stored on our computer systems.
- Identify all connections to the computer systems where covered data is stored.
- Assess the vulnerability of our computer systems to commonly known or reasonably foreseeable attacks.
- Maintain up-to-date firewalls and anti-virus software to protect covered data.
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of covered data.
- Implement regular system monitoring to detect actual and attempted attacks on or intrusions into our systems.
- Take steps to preserve the security, confidentiality, and integrity of covered data in the event of a computer or other technological failure.
- Store protected data on a secure server that is accessible only with a username/password and MFA (where applicable) – or has other security protections – and is kept in a physically secure area.
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area.

- Maintain a careful inventory of our university's computers and any other equipment on which covered data could be stored.

6. Detecting and Managing System Failures

USAO will:

- Implement and maintain procedures to detect actual and attempted attacks on or intrusions into our systems.

7. Service Providers and Contracts

USAO will:

- Before engaging a service provider, conduct due diligence and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue.
- Require our service providers by contract to implement and maintain such safeguards.
- Periodically access our service providers based on the risk they present and the adequacy of their safeguards.

8. Monitoring and Testing

The ISPC will:

- Regularly test and monitor the effectiveness of the safeguards key controls, systems, and procedures, including those to detect actual and attempted attacks on or into information systems.
- Conduct a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of covered data.
- Review logs of access to covered data.
- Evaluate and adjust the WISP in light of the results of the testing and monitoring.
- Establish a written incident response plan that will address the following areas:
    - Goals of the Incident response plan
    - Internal processes for responding to a security event
    - Definition of clear roles, responsibilities, and levels of decision-making authority
    - External and internal communications and information sharing
    - Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls
    - Documentation and reporting regarding security events and related incident response activities
    - Evaluation and revision as necessary of the incident response plan following a security event.
- The ISPC will report in writing, regularly and at least annually, to the USAO Board of Regents. The report shall include:
    - The overall status of the information security program and our compliance

    - Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management responses thereto, and recommendations for changes in the information security program.
- Notify the Federal Trade Commission about notification events in accordance with 16 CFR 314.4(j)(1)

9. Program Review

The ISPC will review this WISP at least annually and update it as necessary to reflect changes in our business arrangements, technology, and security risks.

10. Enforcement

Violations of this WISP will result in disciplinary action, in accordance with USAO policies. Employees who violate this WISP may be subject to disciplinary action up to and including termination of employment.

Revision History:
Last updated – May, 2025