PROCEDURE TITLE:	INFORMATION SECURITY PROGRAM
PROCEDURE NO.:	5.30:2
RELATED POLICY:	5.30REV
PAGE NO.:	1 OF 20
RESPONSIBLE ADMINISTRATOR:	CHIEF INFORMATION SECURITY OFFICER
EFFECTIVE DATE:	06/21/2024
NEXT REVIEW DATE:	06/2027
APPROVED BY:	PRESIDENT

These Information Security Program (ISP) procedures clarify the rationale, objectives, and the encompassing framework devised to protect the confidentiality, integrity, and availability of all information assets at SSU. It serves as the bedrock upon which our security initiatives and protocols are built, ensuring that every stakeholder, from faculty and students to administrative staff and partners, is aligned with our vision of a secure digital ecosystem.

Moreover, in an era where cyber threats evolve rapidly, and the landscape of digital information expands exponentially, this program underscores SSU's proactive stance. By embedding security into the fabric of our institution, we not only respond to current challenges but also anticipate and prepare for future threats.

In essence, this introduction is an invitation for every member of the SSU community to understand, embrace, and champion our collective responsibility towards information security. Through the subsequent sections of this ISP, we will delineate the specifics of our approach, ensuring that our commitment is not just stated, but acted upon, measured, and continually enhanced.

1.0 OBJECTIVES

At Shawnee State University (SSU), our vision for information security transcends the basic need for protection—it encompasses the broader ambition of fostering trust, facilitating uninterrupted academic and administrative operations, and safeguarding our reputation as a beacon of excellence. To realize this vision, the Information Security Program (ISP) revolves around clearly defined objectives. These objectives are the guiding pillars that shape our strategies, drive our initiatives, and define the metrics for our success.

1.1 Preservation of Confidentiality- We are committed to ensuring that sensitive and proprietary information remains accessible only to those authorized to view it. Whether it's the personal details of a student or employee, protected data, or sensitive administrative communication, the sanctity of confidentiality remains paramount.

1.2 Integrity Assurance – Beyond just preserving confidentiality, SSU stresses the importance of data integrity. Every piece of information, once entered or created, should remain unaltered unless subjected to an authorized modification. This ensures that decisions across the university, whether academic or administrative, are based on accurate and untampered data.

1.3 Continuous Availability - Our digital resources, systems, and data repositories are fundamental for the seamless operation of SSU. The ISP aims to ensure that these resources are available when needed, thereby minimizing downtime and ensuring that the academic and operational rhythm of the university remains uninterrupted.

1.4 Regulatory and Legal Compliance - In a world woven together by numerous legal and regulatory threads, SSU remains committed to full compliance with mandates such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and the Safeguards Rule. Beyond just adherence, the university continuously seeks to be a model of best practices in regulatory compliance in the academic realm.

1.5 Cultivation of a Security-Conscious Culture - The most sophisticated security system can be rendered ineffective without the active participation and awareness of its users. Thus, our ISP stresses the importance of cultivating a security-conscious ethos across SSU, ensuring that each individual understands their role in the larger security framework.

1.6 Proactive Threat Identification and Management - Given the evolving nature of cyber threats, SSU's ISP aims for a proactive approach. By staying abreast of the latest vulnerabilities and potential risks, we position ourselves to preemptively counter threats before they can manifest as tangible challenges.

1.7 Comprehensive Incident Response Strategy - While prevention is our primary goal, preparedness for potential security incidents is equally critical. The ISP defines a clear framework for incident detection, response, recovery, and subsequent analysis to ensure that lessons are learned, and similar challenges are mitigated in the future.

1.8 Continuous Policy Improvement - The digital landscape and the threats within it are in constant flux. Recognizing this, one of our core objectives is the commitment to the iterative improvement of this ISP, ensuring it remains relevant, effective, and aligned with both current and anticipated challenges.

2.0 SCOPE

The scope of the Information Security Program (ISP) at Shawnee State University (SSU) defines the breadth and depth of its application, setting clear boundaries and ensuring comprehensive coverage. This section delineates the parameters within which the ISP operates, encompassing the myriad facets of the university’s operations, resources, stakeholders, and information assets.

2.1 Information Assets Covered

2.1.1 Digital Data -All electronic data stored, processed, or transmitted, including databases, files, emails, application data, and backups.

2.1.2 Physical Documents - Paper-based records, files, reports, and any other form of written or printed information.

2.1.3 Media and Devices – Storage devices such as hard drives, USB drives, CDs/DVDs, servers, laptops, desktops, mobile devices and any other media that might store SSU's data.

2.2 Systems and Infrastructure

2.2.1 Information Technology (IT) Systems – All software applications, operating systems and network configurations.

2.2.2 Communication Systems - Email platforms, instant messaging tools, telecommunication systems, and other communication infrastructures.

2.2.3 Physical Infrastructure - All SSU premises, including classrooms, administrative offices, labs, Intermediate Distribution Framework (IDF), Main Distribution Framework (MDF), data centers, and storage areas.

2.3 Stakeholders and Entities

2.3.1 Internal Stakeholders - Faculty, staff, students, research scholars, and any temporary or contractual personnel affiliated with SSU.

2.3.2 External Entities - Vendors, third-party service providers, collaborators, partners, consultants, and any entity or individual interacting with SSU in a capacity that might involve accessing, processing, or storing SSU's data.

2.4 Geographical and Jurisdictional Parameters

2.4.1 On-Campus Activities - All activities taking place within SSU's campuses and satellite locations.

2.4.2 Remote and Online Operations - Online courses, remote administrative activities, virtual meetings, cloud-based operations, and any other off-campus endeavors that involve SSU's data.

2.4.3 Global Interactions - Research collaborations, partnerships, or any interaction that SSU has with entities outside the United States, ensuring adherence to international data protection regulations and standards.

2.5 Timeframe

2.5.1 Historical Data - Information stored or archived from SSU's inception to the present.

2.5.2 Current Operations - Ongoing data collection, processing, and storage activities.

2.5.3 Future Endeavors - Anticipated projects, research, collaborations, and any future activity that would involve SSU's data, ensuring a forward-looking approach to information security.

2.6 Situational Considerations

2.6.1 Normal Operations - Routine academic, administrative, and extracurricular activities.

2.6.2 Emergency Scenarios - Crisis situations such as natural disasters, cyber-attacks, pandemic-related disruptions, and any other extraordinary circumstances that might impact SSU's information assets.

2.6.3 Transitional Activities - Mergers, acquisitions, partnerships, or any significant structural change in the university that could influence the way data is managed and protected.

2.7 Regulatory and Compliance Domains

2.7.1 Federal and State Laws - Compliance with regulations like Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLBA), including the Safeguards Rule, among others.

2.7.2 Industry Standards - Adherence to best practices and norms of the education sector and the broader IT industry.

2.7.3 International Regulations - Where applicable, compliance with international data protection and privacy regulations such as the General Data Protection Regulation (GDPR), which governs how personal data of individuals in the European Union may be processed.

3.0 ROLES AND RESPONSIBILITIES

Ensuring the security of SSU's information assets is a shared responsibility. A successful Information Security Program requires the active participation of all stakeholders. This section elaborates on the specific roles and responsibilities of various entities within SSU to foster a culture of shared accountability and vigilant protection of our data.

3.1 University Leadership

3.1.1 Oversight and Guidance - Provide strategic direction, ensuring that the Information Security Program aligns with SSU's overall vision and mission.

3.1.2 Resource Allocation - Commit necessary financial, human, and technical resources to support the program's initiatives and endeavors.

3.1.3 Policy Endorsement - Approve and advocate for the security policies and guidelines, emphasizing their importance at the highest levels of the institution.

3.2 Information Security Office (ISO) and Team

3.2.1 Program Implementation - Oversee the practical application of the Information Security Program, ensuring all measures are executed correctly.

3.2.2 Risk Management - Identify, evaluate, and manage potential risks, ensuring SSU's preparedness against evolving threats.

3.2.3 Incident Response - Lead and coordinate responses to any security breaches or vulnerabilities, minimizing impact and ensuring rapid recovery.

3.2.4 Training and Awareness - Organize regular workshops, training sessions, and awareness campaigns to instill a security-conscious culture.

3.3 Academic Departments

3.3.1 Curriculum Integration - Embed cybersecurity principles in relevant courses, fostering a generation of students who understand and value data privacy.

3.3.2 Secure Research - Ensure that research activities, especially those involving sensitive data, adhere to SSU's security protocols.

3.3.3 Reporting - Promptly inform the ISO or concerned authorities about any suspected breaches or vulnerabilities.

3.3.4 Responsible Behavior - Avoid sharing passwords, downloading unauthorized software, or engaging in actions that might compromise SSU's systems.

3.4 All Employees

3.4.1 Daily Adherence - Follow security guidelines in daily operations, especially while handling sensitive student or staff data.

3.4.2 Vendor Management - Ensure that third-party vendors or partners understand and comply with SSU's security expectations.

3.4.3 Continuous Learning - Participate in training sessions and remain updated about the latest security procedures and protocols.

3.4.4 Reporting - Promptly inform the ISO or concerned authorities about any suspected breaches or vulnerabilities.

3.4.5 Responsible Behavior - Avoid sharing passwords, downloading unauthorized software, or engaging in actions that might compromise SSU's systems.

3.5 Students

3.5.1 Compliance - Adhere to all the university’s cybersecurity measures, especially while accessing SSU’s digital resources.

3.5.2 Responsible Behavior - Avoid sharing passwords, downloading unauthorized software, or engaging in actions that might compromise SSU’s systems.

3.5.3 Reporting - Immediately inform the concerned department or the ISO about any suspicious activities or potential threats they encounter.

3.6 ITS Department

3.6.1 Systems Maintenance - Regularly update and patch software, ensuring the robustness of SSU's technical infrastructure.

3.6.2 Access Management - Implement and manage user access controls, ensuring only authorized individuals have access to specific data.

3.6.3 Backup and Recovery - Maintain regular data backups and establish a robust disaster recovery plan.

3.7 External Partners and Vendors

3.7.1 Contractual Compliance - Adhere to all security clauses and requirements stipulated in contracts or agreements with SSU.

3.7.2 Data Management - Handle any SSU data they access with the utmost care, respecting all confidentiality and security protocols.

3.7.3 Reporting and Collaboration - Collaborate transparently with SSU's ISO and related departments, especially in scenarios involving shared data or interconnected systems.

3.8 Periodic Review Committee

3.8.1 Annual Evaluations - Conduct a thorough review of the Information Security Program to assess its effectiveness and relevance.

3.8.2 Recommendations - Provide actionable feedback for improvements, upgrades, or modifications to the program.

3.8.3 Stakeholder Engagement - Engage with various university stakeholders to gather their insights, concerns, and feedback about the program's effectiveness.

4.0 RISK ASSESSMENT

Risk assessment is a foundational pillar of SSU's Information Security Program (ISP). It provides the blueprint for understanding, evaluating, and addressing potential threats to the university's information assets. This section delves deep into the risk assessment processes, methodologies, and protocols that will be followed to ensure the protection of SSU's digital and physical data ecosystem. All departments that work with regulated data will work with the IT department to do regular risk assessments.

4.1 Purpose of Risk Assessment

4.1.1 Identify Vulnerabilities - Detect weaknesses within our systems, processes, and operations that could be exploited.

4.1.2 Understand Threats - Recognize potential dangers, whether they be from cyber-attacks, human error, natural disasters, or any other source.

4.1.3 Prioritize Resources - Allocate resources more efficiently by addressing the most critical risks first.

4.1.4 Inform Strategy - Shape the overall security strategy based on actual, measurable risks, rather than perceived ones.

4.2 Risk Assessment Methodology

4.2.1 Data Collection - Gather comprehensive information on SSU's assets, including software, hardware, data repositories, and more.

4.2.2 Threat Analysis - Identify potential threats, categorizing them based on their likelihood and potential impact.

4.2.3 Vulnerability Assessment - Utilize tools, software, and expertise to scan for weaknesses in SSU's systems.

4.2.4 Risk Evaluation - Combine threat and vulnerability analyses to determine the overall risk levels.

4.2.5 Documentation - Maintain thorough records of all risk assessment findings for review, future reference, and compliance purposes.

4.3 Risk Categories

4.3.1 Technological Risks - Vulnerabilities within the IT infrastructure, outdated software, and potential for cyber-attacks.

4.3.2 Human Risks - Potential errors, negligence, or malicious activities by staff, students, or other stakeholders.

4.3.3 Environmental Risks - Natural disasters, power outages, or other environmental factors that could impact data integrity.

4.3.4 Legal and Regulatory Risks - Potential violations of regulations such as FERPA, HIPAA, GLBA, and others.

4.4 Risk Mitigation Strategies

4.4.1 Prevention - Implement protective measures to avoid the risk altogether.

4.4.2 Reduction - Limit the impact or likelihood of the risk through various controls.

4.4.3 Transference - Shift the responsibility or repercussions of the risk, possibly through insurance or contractual agreements.

4.4.4 Acceptance - Acknowledge the risk and prepare contingency plans without actively mitigating it.

4.4.5 Avoidance - Change processes, operations, or activities to eliminate the risk.

4.5 Continuous Monitoring and Reassessment

4.5.1 Periodic Reviews - Conduct risk assessments at regular intervals, at least annually or after significant changes to the IT environment.

4.5.2 Real-time Monitoring - Deploy monitoring tools to identify and report potential threats in real-time.

4.5.3 Stakeholder Feedback - Engage with SSU community members to gather insights and feedback, ensuring a holistic understanding of potential risks.

4.6 Collaboration with External Experts

4.6.1 Third-party Assessments - Engage external agencies or consultants to conduct unbiased risk assessments.

4.6.2 Industry Benchmarking - Compare SSU’s risk posture with industry standards and best practices to ensure optimal protection.

4.6.3 Threat Intelligence Sharing - Collaborate with other educational institutions and organizations to share information about evolving threats and best practices.

5.0 INFORMATION SECURITY CONTROLS

To safeguard the university's valuable digital assets, implementing comprehensive security controls is paramount. Information security controls are the mechanisms, procedures, and

measures designed to prevent, detect, and mitigate risks to data integrity, availability, and confidentiality. This section makes clear the various layers of security controls put in place under SSU's Information Security Program (ISP).

5.1 Administrative Controls

5.1.1 Policy Development and Management - Formulate, regularly update, and communicate clear and concise security policies and procedures for the entire SSU community.

5.1.2 Personnel Security - Conduct background checks, provide security training, and establish procedures for granting and revoking access to information systems.

5.1.3 Vendor Management - Establish protocols for the selection and management of third-party vendors, ensuring they adhere to SSU's security standards.

5.1.4 Incident Response Plan - Develop and regularly update a detailed plan outlining the steps to be taken in the event of a security incident.

5.1.5 Disaster Recovery and Business Continuity - Establish and periodically test plans for restoring services and data in the event of a significant disruption.

5.2 Technical Controls

5.2.1 Access Controls - Implement mechanisms such as user authentication, role-based access controls, Multi-Factor Authentication (MFA), and session management to ensure only authorized individuals can access relevant data.

5.2.2 Network Security - Utilize firewalls, switches, routers, Virtual Private Network (VPN)s, Network Access Control (NAC) servers, cloud services, AI and machine learning, intrusion detection and prevention systems, and secure network protocols to safeguard against unauthorized infiltrations.

5.2.3 Endpoint Protection - Deploy antivirus, anti-malware, and endpoint detection and response (EDR) solutions on all devices connected to SSU's network.

5.2.4 Encryption - Ensure data, both at rest and in transit, is encrypted using industry-standard algorithms.

5.2.5 Application Security - Regularly patch and update software applications, and implement security measures during the development phase of SSU-owned software.

5.3 Physical Controls

5.3.1 Facility Access - Restrict physical access to server rooms, data centers, and other sensitive areas using card access systems, biometrics, or other secure methods.

5.3.2 Surveillance - Employ CCTV cameras, security personnel, and intrusion detection systems at critical locations.

5.3.3 Equipment Security - Secure computing devices with locks, ensure proper disposal of obsolete equipment, and have measures against theft or loss.

5.3.4 Environmental Controls - Install fire suppression systems, uninterrupted power supplies, and climate control mechanisms to protect technological assets.

5.4 Environmental Controls

5.4.1 Regular Audits - Conduct routine security audits to identify potential vulnerabilities and rectify them before they can be exploited.

5.4.2 Security Awareness Training - Provide regular training sessions to faculty, staff, and students, ensuring they're aware of security best practices and potential threats.

5.4.3 Patch Management - Routinely update and patch software and hardware components to address known vulnerabilities.

5.5 Detective Controls

5.5.1 Monitoring and Logging - Continuously monitor system activities and maintain detailed logs for forensic purposes and to detect any anomalies.

5.5.2 Intrusion Detection Systems - Utilize advanced systems that scan for, report, and respond to unauthorized system activities.

5.5.3 Regular Security Assessments - Perform vulnerability assessments and penetration testing to identify potential security gaps.

5.6 Corrective Controls

5.6.1 Incident Response - Have a defined set of actions to isolate, mitigate, and recover from security breaches.

5.6.2 Backup and Restore Procedures - Maintain regular backups of critical data and ensure efficient procedures for data restoration.

5.6.3 System Rollbacks - Implement mechanisms to restore systems to their state prior to any unauthorized changes or breaches.

6.0 THIRD-PARTY AND VENDOR MANAGEMENT

Recognizing the potential risks posed by third-party vendors and service providers, SSU places a premium on stringent vendor management. A rigorous system ensures that third parties adhere to the same exacting standards of information security that SSU upholds. This section details the guidelines, protocols, and procedures associated with the management of third-party interactions and vendor relationships.

6.1 Vendor Selection and Onboarding

6.1.1 Due Diligence - Before establishing any relationship, a comprehensive review of the potential vendor's security policies, practices, and reputation in the industry is conducted. This includes assessing past incidents, financial health, and references.

6.1.2 Security Audits - Require potential vendors to undergo third-party security audits to ensure their systems and practices are up to par with SSU's standards.

6.1.3 Contractual Agreements - Every contract with a vendor must include clear clauses on data protection, breach notification, regular security audits, and the right of SSU to evaluate security practices.

6.2 Continuous Monitoring and Assessment

6.2.1 Periodic Reviews- Conduct regular reviews of vendor performance, security practices, and adherence to the terms of the contract.

6.2.2 Vulnerability Assessments - Vendors with access to SSU systems or data must undergo periodic vulnerability assessments to ensure the integrity of their connection to SSU's systems.

6.2.3 Incident Reporting - Vendors are contractually obligated to promptly report any security incidents or breaches that might impact SSU.

6.3 Data Access and Management

6.3.1 Principle of Least Privilege - Vendors are given access only to the data and systems absolutely necessary for the services they provide, and for a limited time.

6.3.2 Data Transfer Protocols - Establish strict guidelines for how data is transferred between SSU and third parties, ensuring encrypted, secure channels.

6.3.3 Data Retention and Deletion - Stipulate the duration for which vendors can retain SSU's data and mandate secure methods for data deletion post-contract or after project completion.

6.4 Training and Collaboration

6.4.1 Vendor Security Training - Vendors with access to SSU systems are required to undergo SSU-specific security training to familiarize them with our protocols and expectations.

6.4.2 Collaboration Forums - Establish regular collaborative sessions between SSU and vendors to share updates on emerging threats and best practices, and to review performance metrics.

6.5 Offboarding and Contract Termination

6.5.1 Data Return/Deletion/Access Revocation - Upon the completion of a contract, or when a vendor relationship is terminated, ensure that all SSU data in the vendor's possession is securely returned or deleted, and immediately revoke all system and data access privileges granted to the vendor.

6.5.2 Post-contract Audit - Perform an audit to ensure no residual data remains with the vendor and that all obligations have been met.

6.6 Compliance and Regulatory Adherence

6.6.1 Regulatory Adherence - Vendors who handle data subject to regulations including but not limited to FERPA, HIPAA, GLBA and Safeguards Rule must be prepared to provide documented proof of their adherence to these regulations.

6.6.2 Indemnity Clauses - Contracts should incorporate indemnity clauses, ensuring that vendors are held responsible for breaches or non-compliance on their part, shielding SSU from potential liabilities.

6.7 Relationship Management

6.7.1 Dedicated Vendor Managers - Assign dedicated personnel to manage specific vendor relationships, fostering better communication and oversight.

6.7.2 Performance Metrics - Establish clear metrics to evaluate vendor performance, both in terms of service delivery and security adherence.

6.7.3 Feedback Loops - Facilitate channels through which both SSU and the vendor can provide feedback, ensuring continuous improvement.

7.0 INCIDENT RESPONSE

Incidents in the realm of information security can range from minor discrepancies in data access to major breaches that threaten the confidentiality, integrity, and availability of our data assets. SSU's incident response strategy is designed to provide a structured and effective approach to detect, respond to, and recover from these incidents. This section delineates the processes, roles, and protocols to manage and mitigate incidents promptly.

7.1 Incident Definition and Classification

7.1.1 Definition - An incident is defined as any real or suspected adverse event related to the security of information assets or systems.

7.1.2 Classification - Incidents are classified based on their severity and potential impact:
- Minor: Affects individual users or non-critical systems.
- Moderate: Affects several users or contains potential to escalate.
- Major: Affects large parts of the community or critical university functions.

7.2 Incident Detection and Reporting

7.2.1 Monitoring - Employ continuous monitoring tools and techniques to detect unusual activities or breaches.

7.2.2 Reporting - Any SSU community member who identifies or suspects an incident must report it immediately to the designated authority, using predefined channels which can be found on the IT Incident Reporting website.

7.2.3 Whistleblower Protection - Ensure individuals reporting incidents are protected against potential backlash or retaliation.

7.3 Incident Response Team (IRT)

7.3.1 Composition - IRT is comprised of members from IT, Legal, Communications, and relevant departments, depending on the nature of the incident.

7.3.2 Roles and Responsibilities - Define clear roles, such as Incident Manager, Communications Lead, Technical Lead, etc., ensuring each stage of the response is effectively handled.

7.4 Response Process

7.4.1 Initial Assessment - Upon receipt of an incident report, IRT conducts a preliminary assessment to determine its veracity and severity.

7.4.2 Containment - Immediate actions are taken to contain the incident, preventing further damage or data loss. This involves both short-term (temporary measures) and long-term (permanent measures) containment strategies.

7.4.3 Eradication - Identify and remove the root cause of the incident, ensuring the threat is entirely neutralized.

7.4.4 Recovery - Restore affected systems and validate their security before bringing them back online.

7.4.5 Communication - Inform stakeholders, including potentially affected individuals, regulatory bodies, and the larger SSU community, based on the severity and nature of the incident. Maintain transparency while ensuring no compromising details are disclosed.

7.5 Post-Incident Analysis

7.5.1 Debriefing - Once an incident is resolved, the IRT conducts a thorough debriefing to understand the sequence of events, what went well, and areas of improvement.

7.5.2 Documentation - Document all actions taken, decisions made, and findings in an Incident Report. This report will be crucial for auditing, training, and potential legal proceedings.

7.5.3 Lessons Learned - Identify lessons from the incident and integrate them into future response strategies, training modules, and potential system enhancements.

7.6 Periodic Testing and Drills

7.6.1 Simulations - Periodically simulate security incidents to test the efficiency and effectiveness of the response strategy.

7.6.2 Training - Based on the outcomes of these simulations, adjust training modules for both the IRT and the larger SSU community.

7.7 External Communication and Legal Considerations

7.7.1 Media Interaction - Designate specific spokespeople to interact with the media to ensure accurate, consistent, and non-detrimental information is conveyed.

7.7.2 Legal Obligations - Understand and adhere to legal obligations concerning breach notifications, especially considering regulations like FERPA, HIPAA, GLBA, and the Safeguards Rule.

8.0 POLICY ENFORCEMENT

Ensuring the integrity, confidentiality, and availability of our information assets requires not just a strong policy framework but also rigorous enforcement mechanisms. Without strict adherence and accountability, even the most comprehensive policies risk being ineffective. This section of the Information Security Program outlines the processes, procedures, and consequences associated with policy enforcement.

8.1 Monitoring and Auditing

8.1.1 Continuous Monitoring - Employ state-of-the-art monitoring tools to oversee all activities on the network, especially focusing on sensitive information access points.

8.1.2 Periodic Audits - Conduct comprehensive internal audits periodically to verify adherence to the information security policy. External third-party audits should also be arranged annually to ensure impartiality and comprehensive scrutiny.

8.2 Violation Reporting

8.2.1 Reporting Channels - Establish secure and confidential channels, both electronic and manual, through which potential policy violations can be reported.

8.2.2 Whistleblower Protection - Ensure that those reporting potential violations are safeguarded against retaliation or backlash.

8.3 Investigation of Reports

8.3.1 Immediate Action - Any reported violation triggers an immediate preliminary investigation to ascertain its veracity.

8.3.2 Comprehensive Examination - If the preliminary investigation warrants, initiate a full-scale inquiry, ensuring thoroughness while respecting individual rights and privacy.

8.4 Consequences of Violations

8.4.1 Graded Responses - All policy violations are not equal. Develop a graded consequence system based on the severity and impact of the violation:

- Minor Violations: These could result in warnings or mandatory attendance at additional training sessions.
- Moderate Violations: Consequences might include temporary suspension, probationary monitoring, or a revocation of certain access privileges.

- Major Violations: These could lead to termination of employment or expulsion from the institution, alongside potential legal action.

8.4.2 Escalation Procedures - Ensure that more severe actions, such as termination or expulsion, follow a clear escalation process, involving higher administrative levels and, when appropriate, the Board of Trustees.

8.5 Feedback Mechanisms

8.5.1 Continuous Feedback - Provide avenues for the SSU community to give feedback on the enforcement processes, ensuring they are fair and transparent.

8.5.2 Periodic Reviews - Based on feedback and the changing information landscape, periodically review the enforcement mechanisms to maintain their effectiveness and relevance.

8.6 Training and Awareness

8.6.1 Regular Sessions - Hold regular training sessions for all SSU community members, emphasizing the importance of policy adherence and the potential consequences of violations.

8.6.2 Onboarding - As part of the orientation process for new employees or students, introduce them to the Information Security Program and ensure they understand their roles and responsibilities.

8.7 Legal Recourse

8.7.1 Legal Action - Retain the right to pursue legal action against severe violations that might endanger the institution's reputation, assets, or members.

8.7.2 Cooperation with Authorities - In instances where a violation breaks not only SSU policies but also state or federal laws, commit to fully cooperating with the relevant authorities.

9.0 REVIEW AND UPDATES

The digital landscape is ever-evolving, with emerging technologies, challenges, threats, and regulatory requirements. As such, the Information Security Program cannot remain static; it must adapt and grow in response to these changes. This section describes the rigorous processes that SSU employs to ensure that our Information Security Program remains current, comprehensive, and effective.

9.1 Periodic Review Schedule

9.1.1 Annual Review - At a minimum, conduct a comprehensive review of the entire Information Security Program annually to ensure alignment with current best practices and emerging challenges.

9.1.2 Trigger-based Review - Beyond the annual examination, reviews will also be initiated based on specific triggers, such as significant security incidents, major technological implementations, or new regulatory requirements.

9.2 Stakeholder Involvement

9.2.1 Interdepartmental Collaborations - Ensure that reviews involve representatives from all relevant departments, including IT, Legal, Human Resources, and Academic Affairs, among others.

9.2.2 External Expertise - Engage with third-party cybersecurity experts or consultants during reviews to bring in fresh perspectives and specialized knowledge.

9.2.3 Community Feedback - Create channels for feedback from students, faculty, and staff to incorporate the broader SSU community's experiences and concerns.

9.3 Documentation and Versioning

9.3.1 Version Control - Implement strict version control procedures to ensure that only the latest, approved version of the Information Security Program is in circulation and use.

9.3.2 Change Logs - Maintain detailed change logs for every update, detailing what was changed, why, and by whom.

9.3.3 Archiving - Archive older versions of the program in a secure manner to ensure historical reference and potential audit needs.

9.4 Communication of Changes

9.4.1 Notification - Upon approval of significant changes, notify all SSU community members promptly, emphasizing critical adjustments.

9.4.2 Training on Updates - Conduct training sessions or workshops for specific updates, ensuring that all relevant parties understand and can effectively implement the changes.

9.4.3 Updated Policy Availability - Ensure that the most current version of the Information Security Program is easily accessible, preferably through the university's internal portal or website.

9.5 Regulatory Alignment

9.5.1 Continuous Monitoring - Monitor local, state, and federal regulatory environments continuously to ensure that the Information Security Program aligns with all legal and regulatory requirements.

9.5.2 Regulatory Engagement - Engage with regulatory bodies, where appropriate, to gain insights into upcoming changes and ensure SSU's proactive compliance.

9.5.3 External Audits - Undergo external audits periodically to independently assess SSU's alignment with regulatory standards and best practices.

9.6 Continuous Improvement

9.6.1 Improvement Metrics - Define and measure key metrics that indicate the program's effectiveness, using them to guide areas of improvement.

9.6.2 Best Practices Adoption - Stay abreast of global best practices in information security, integrating them into SSU's program as relevant.

9.6.3 Lessons from Incidents - Leverage learnings from any security incidents, whether faced by SSU or other institutions, to fortify the Information Security Program.

10.0 COMPLIANCE

Compliance ensures that Shawnee State University (SSU) not only adheres to its own policies and standards but also meets external regulatory and legal requirements. A strong compliance framework acts as a testament to SSU's unwavering commitment to information security, upholding its reputation and fostering trust within its community and external stakeholders. This section elaborates on the processes and mechanisms that ensure SSU remains in complete compliance.

10.1 Regulatory Framework

10.1.1 Comprehensive- Maintain a detailed, continuously updated list of all relevant local, state, federal, and international regulations that SSU must comply with, including FERPA, HIPAA, GLBA, and the Safeguards Rule.

10.1.2 Regulatory Mapping – Map specific provisions of each regulation to corresponding elements of the Information Security Program, ensuring every requirement is addressed.

10.2 Compliance Monitoring

10.2.1 Dedicated Compliance Team – Establish a team solely dedicated to monitoring and ensuring SSU's adherence to internal and external compliance requirements.

10.2.2 Periodic Checks – Conduct regular compliance checks, both announced and unannounced, to ensure ongoing adherence and to identify potential areas of non-compliance.

10.3 Reporting and Documentation

10.3.1 Compliance Reports – Generate quarterly compliance reports highlighting SSU's adherence status, any non-compliance areas, and corrective actions taken.

10.3.2 Record Keeping – Maintain detailed records of all compliance activities, checks, and training sessions, ensuring they are readily available for audits or reviews.

10.3.3 Regulatory Reporting - When required by specific regulations, prepare and submit detailed compliance reports to relevant regulatory bodies.

10.4 Training and Awareness

10.4.1 Regular Training – Hold periodic training sessions specifically focusing on compliance for staff, faculty, and other relevant stakeholders.

10.4.2 Onboarding Process – Integrate compliance awareness and training into the onboarding process for new employees, ensuring they start with a clear understanding of SSU's compliance obligations.

10.4.3 Compliance Resources - Provide readily accessible resources, guidelines, and manuals related to compliance for the SSU community.

10.5 Third-party Compliance

10.5.1 Vendor Assessment - Before engaging with any third-party or vendor who will have access to our network and/or regulated data, assess their compliance posture, ensuring they meet SSU's standards and any relevant regulations.

10.5.2 Compliance Clauses – Incorporate compliance obligations into all contracts with vendors, partners, and third-parties, who have access to our network and/or regulated data making them accountable for maintaining the required compliance standards.

10.5.3 Periodic Audits – Conduct regular compliance audits of third-parties, ensuring they consistently adhere to required standards.

10.6 Non-compliance Management

10.6.1 Immediate Rectifications - Upon detecting a non-compliance issue, initiate immediate remedial measures to rectify the situation.

10.6.2 Escalation Mechanism - Implement a clear escalation mechanism for severe or repeated non-compliance issues, ensuring they receive appropriate attention from senior management.

10.6.3 Continuous Feedback - Establish channels for feedback after any non-compliance incident, enabling a culture of continuous learning and improvement.

10.7 Review and Amendments

10.7.1 Regulatory Updates – Monitor for updates or changes in relevant regulations, ensuring that SSU's Information Security Program is amended promptly to stay in line with them.

10.7.2 Feedback Loop - Solicit feedback from the SSU community and external stakeholders on compliance processes, incorporating constructive suggestions into the compliance framework.

History
Effective: 06/21/2024