RESOLUTION OF THE BOARD OF REGENTS OF NAVAJO TECHNICAL UNIVERSITY

Adopting the Real Information Security Plan_R2 as the University's Official Information Security Program to Meet GLBA Compliance Requirements and Resolution of Audit Findings, attached as Exhibit A

WHEREAS:

1. The Board of Regents of the Navajo Technical University is responsible for the administration, operations and the development of policy as stated in Navajo Nation Council Resolution CO-58-16, enacted on November 10, 2016, that amended the University's enabling legislation, codified at 15 N.N.C. §§1201-1210; and

2. Pursuant to the University's enabling legislation, Navajo Technical University (NTU) is organized as an institution of higher learning for the primary purpose of providing post-secondary and post-graduate education programs that serve both the academic and vocational/technical needs of the Navajo Nation and its citizens, 15 N.N.C. §1203(A); and

3. Pursuant to the University's enabling legislation, the Board of Regents of Navajo Technical University is authorized to review and approve course curricula, assessment structures, program plans, research and development projects, in accordance with established program priorities and policies of the University, 15 N.N.C. §1205(F), and to review and approve contracts, 15 N.N.C. §1205(R); and

4. The Gramm–Leach–Bliley Act (GLBA) requires all institutions of higher education to establish, implement, and maintain a comprehensive Information Security Program to safeguard nonpublic personal information; and

5. The Federal Trade Commission (FTC) enforces the GLBA Safeguards Rule, requiring colleges and universities to adopt a formalized plan addressing administrative, technical, and physical safeguards; and

6. Navajo Technical University ("NTU"), in fulfillment of these federal requirements, has developed the Real Information Security Plan_R2 to provide the framework for protecting sensitive student, employee, and financial data; and

7. NTU's most recent independent financial audit identified the absence of a formally adopted GLBA compliance policy as a repeat finding, requiring the Board's immediate review and corrective action; and

8. The NTU Board of Trustees recognizes that the adoption of the Information Security Plan (ISP) as an institutional standard is essential for compliance with GLBA, protection of information assets, and the mitigation of cybersecurity risks

NOW THEREFORE BE IT RESOLVED THAT:

1. The Board of Regents of the Navajo Technical University hereby adopts the Real Information Security Plan_R2 as the University's official Information Security Program to meet GLBA compliance requirements and resolution of audit findings, attached as exhibit A.

2. The President of Navajo Technical University is hereby authorized, directed and empowered to do all things necessary to effectuate the purpose of this resolution.

CERTIFICATION

I hereby confirm that this resolution was discussed and considered by the Board of Regents of the Navajo Technical University at a duly called meeting held in Churchrock, New Mexico at which a quorum was present, and that this resolution was passed by a vote of **4** in favor, **0** opposed and **0** abstained on the 25th day of August 2025.

Dr. Delores Greyeyes, Vice Chairperson
NTU Board of Regents

Information Security Plan (GLBA)

Federal law requires Navajo Technical University, hereby referred to as "NTU," to develop and implement an information security plan (ISP) to create effective administrative, technical, and physical safeguards for the protection of client information. This ISP sets forth procedures for evaluating and addressing the electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting client information.

101) *Designation of representatives:* The Director of Information Technology (ITDir), Jared Ribble, Senior System Administrator (Sysadmin), Dody Begay are designated persons responsible for coordinating and overseeing the ISP. These persons are now referred to as the "representatives." The designated representatives may assign or delegate other NTU representatives to oversee and coordinate elements of the ISP. Any questions regarding the implementation of the ISP or the interpretation of this document should be directed to the representatives or their designees.

102) *Risk identification and assessment and current safeguards*: NTU has identified, as part of the ISP, the internal and external risks to the security, confidentiality, and integrity of client information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromises of such information and implemented the following safeguards for controlling these risks:

1. **Multifactor authentication (MFA)**: *Using two or more authentications such as pin/password/biometric/token are always used.*

   The following is NTU's high-level policy that is vendor agnostic and combines the use of multifactor authentication (MFA) with passwords and personal identification numbers (PINs) to protect sensitive information:

   Purpose: This policy aims to certify that access to sensitive information is protected through multifactor authentication, passwords, and PINs.

   Scope: This policy concerns all employees, contractors, and third-party vendors who access the school's systems and applications that contain sensitive information.

   Authentication Factors: Multifactor authentication requires the use of two or more of the following factors:

   - Something the user knows (password, PIN)

- Something the user has (smart card, token)
- Something the user is (biometric information such as fingerprint, iris scan)

Password and PIN Requirements: Passwords and PINs must meet the following requirements:

- Be at least 12 characters in length.
- Contain a combination of uppercase and lowercase letters, numbers, and special characters.
- Be unique and not reused.
- Be changed every 90 days or sooner if there is suspicion of compromise.

Systems and Applications: MFA, passwords, and PINs are required for all NTU systems and applications that contain sensitive information, including but not limited to:

- Financial systems
- Student Information systems
- Classroom content, management systems
- Student and Staff Electronic mail systems

Exceptions: Omissions to this policy may be granted in rare situations where using MFA, passwords, or PINs is not practical or possible. The ITDir and department heads of the request must approve exceptions.

Implementation: The implementation of MFA, passwords, and PINs will be overseen by the Information Technology (IT) department. According to this policy, IT will work with system owners and application administrators to implement MFA, passwords, and PINs.

Monitoring and Reporting: IT will monitor the use of MFA, passwords, and PINs to confirm compliance with this policy. Any policy violations will be reported to the appropriate senior administrator and ITDir.

Review: The representatives and an IT-contracted cyber security firm will review this policy annually and update it to certify compliance with applicable laws, regulations, and industry standards.

By following this policy, NTU can help ensure sensitive information's security and comply with applicable laws, regulations, and industry standards.

2. **Least amount of access**: *The least amount of access is given to specific client files/folders and environments.*

   The following is NTU's high-level policy that is vendor-agnostic and outlines the least amount of access to files and folders for sensitive information:

   Purpose: This policy aims to ensure that access to files and folders containing sensitive information is limited to the least access necessary for authorized users to perform their job duties.

   Scope: This policy applies to all employees, contractors, and third-party vendors accessing files containing sensitive information.

   Access Control: Access to files and folders containing sensitive information must be limited to authorized personnel who require access to perform their job duties. This can be accomplished through role-based access control, access controls, and user authentication.

   Need-to-Know: Access to files and folders containing sensitive information must be restricted to only individuals with a valid need-to-know. This includes access to specific files or folders based on the individual's job responsibilities and business needs.

   File and Folder Permissions: File and folder permissions must be set to limit access to sensitive information to the least amount of access necessary for authorized users to perform their job duties. This includes reading, writing, and deleting permissions.

   Monitoring and Reporting: Access to files and folders containing sensitive information will be monitored and logged to confirm compliance with this policy. Any policy violations will be reported to the appropriate senior administrator and ITDir.

   Review: The representatives and an IT-contracted cyber security firm will review this policy annually and update it to certify compliance with applicable laws, regulations, and industry standards.

   By following this policy, NTU can limit access to sensitive information to the least amount necessary for authorized users to perform their job duties and reduce the risk of security breaches.

3. **Data loss prevention (DLP)**: *This describes how data is controlled, recorded and monitored as it moves through the organization and externally.*

The following is NTU's high-level policy that is vendor agnostic and outlines data loss prevention measures for protecting sensitive information:

Purpose: The purpose of this policy is to ensure that sensitive information is protected from unauthorized disclosure, theft, or loss through data loss prevention measures.

Scope: This policy applies to all employees, contractors, and third-party vendors with sensitive information access.

Classification: Sensitive information must be classified based on the level of sensitivity and the potential impact of a security breach. This classification will help to determine the appropriate data loss prevention measures for protecting sensitive information.

Data Encryption: Sensitive information must be encrypted when it is in transit and at rest to prevent unauthorized access. This can be accomplished through the use of encryption technologies such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), or Advanced Encryption Standard (AES).

Access Controls: Access to sensitive information must be limited to authorized personnel who require access to perform their job duties. This can be accomplished through user authentication, access controls, and role-based access control.

Data Backup and Recovery: Sensitive information must be backed up regularly and stored securely to prevent loss or corruption. Backups must be tested regularly to ensure that data can be restored in the event of a disaster or other data loss event.

Data Retention: Sensitive information must be retained only as long as necessary to meet business or regulatory requirements. Once information is no longer needed, it must be securely deleted or destroyed to prevent unauthorized access or disclosure.

Monitoring and Reporting: Data loss prevention measures will be monitored and logged to ensure compliance with this policy. Any violations of this policy will be reported to the appropriate management and the Information Security Officer (ISO).

Review: This policy will be reviewed annually by the ISO and updated as needed to ensure compliance with applicable laws, regulations, and industry standards.

In conclusion, a high-level policy for data loss prevention can help to protect sensitive information from unauthorized disclosure, theft, or loss. This policy outlines the requirements for data classification, encryption, access controls, data backup and recovery, data retention, monitoring and reporting, and review. By following this policy, organizations can ensure that sensitive information is protected from unauthorized access or disclosure, comply with regulatory requirements, and reduce the risk of security breaches.

4. **Network access restrictions**: *This describes the use of firewalls and a virtual private network (VPN) to ensure only managed and controlled devices/environments have access to client data.*

   The following is NTU's high-level policy that is vendor agnostic and outlines Network access restrictions for protecting sensitive information:

   Purpose: The purpose of this policy is to ensure that client data is accessed only through secure, managed, and controlled devices and environments. By enforcing strict network access controls using firewalls and Virtual Private Network (VPN) technology, NTU protects against unauthorized access, interception, and misuse of sensitive information.

   Scope: This policy applies to all employees, contractors, and third-party vendors who access NTU systems and applications containing client data, whether on campus or remotely.

   Requirements:

   1. ***Firewalls*** – Configured to filter and control incoming and outgoing network traffic according to defined security rules. Only authorized ports, protocols, and IP addresses are permitted. All access attempts are logged and reviewed.

   2. ***VPN Access*** – Required for all remote connections to NTU networks containing client data. VPN access is granted only to NTU-managed devices that meet security requirements, including updated operating systems, security patches, and endpoint protection.

   3. ***Encryption*** – All network connections transmitting client data must use strong encryption to protect against unauthorized interception.

4. ***Device Compliance*** – Only devices that meet NTU's security posture requirements are permitted to connect to networks containing client data. Unmanaged or non-compliant devices are blocked.

5. ***Segmentation & Access Controls*** – Access is restricted to the minimum systems and resources necessary for an authorized user's role. Network segmentation and access control lists (ACLs) are implemented to limit exposure.

Monitoring and Reporting: The IT department will continuously monitor firewall and VPN activity to ensure compliance with this policy. Any violations or suspicious activities will be investigated and reported to the appropriate senior administrator and the ITDir.

Review: This policy will be reviewed annually by the designated representatives and an IT-contracted cybersecurity firm. Updates will be made as needed to maintain compliance with applicable laws, regulations, and industry standards.

In conclusion, by implementing strict network access restrictions through the combined use of firewalls and VPN technology, NTU ensures that only authorized, secure, and compliant devices and environments can access client data. This layered security approach reduces the risk of unauthorized disclosure, interception, or misuse of sensitive information and supports NTU's commitment to maintaining compliance with applicable laws, regulations, and industry standards.

5. **Encryption**: *Anything that stores, transmits or accesses client data must be encrypted.*

The following is NTU's high-level policy that is vendor agnostic and outlines Encryption for protecting sensitive information:

Purpose: The purpose of this policy is to ensure that all systems, devices, and applications that store, transmit, or access client data use strong encryption to protect that data from unauthorized access, disclosure, or alteration. Encryption safeguards sensitive information both in transit and at rest, reducing the risk of compromise.

Scope: This policy applies to all NTU employees, contractors, and third-party vendors who handle client data, as well as any systems, storage devices, or communication channels where client data resides or passes through.

Requirements:

1. ***Encryption in Transit*** – All client data transmitted over public or untrusted networks must be encrypted using strong, industry-accepted protocols (e.g., TLS 1.2+ or equivalent).

2. ***Encryption at Rest*** – All client data stored on servers, workstations, mobile devices, and removable media must be encrypted using strong algorithms (e.g., AES-256 or equivalent).

3. ***Key Management*** – Encryption keys must be generated, stored, rotated, and retired securely, following industry best practices to prevent unauthorized disclosure.

4. ***Device Compliance*** – Only NTU-approved and managed devices meeting encryption requirements are authorized to store or process client data.

5. ***Third-Party Systems*** – Any external system or cloud service that stores or transmits NTU client data must comply with this encryption policy and demonstrate equivalent security measures.

Monitoring and Reporting: The IT department will periodically verify that encryption measures are implemented and functioning as intended. Any deficiencies, failures, or non-compliance will be documented and addressed promptly.

Review: This policy will be reviewed annually by the designated representatives and an IT-contracted cybersecurity firm. Updates will be made as necessary to ensure compliance with applicable laws, regulations, and industry standards.

In conclusion, by enforcing strong encryption standards for all storage and transmission of client data, NTU ensures that sensitive information remains protected even if intercepted or accessed without authorization. This approach supports NTU’s compliance obligations and commitment to safeguarding the confidentiality, integrity, and availability of client data.

103) *Design and implementation of safeguards program*: The risk assessment and safeguard control policies described above shall apply to all methods of handling or disposing of client information, whether in electronic, paper, or other forms. The representatives will regularly implement safeguards to control the risks identified through such assessments and regularly test or

otherwise monitor the effectiveness of such safeguards in relevant areas of the school's operations, including:

1. **Employee management and training**:

   The following is NTU's high-level policy that is vendor agnostic and outlines Employee management and training for protecting sensitive information:

   Purpose: To build and maintain a continuous cybersecurity and privacy learning program (CPLP) that ensures all personnel understand their roles, are aware of organizational risks, and follow best security practices throughout their employment lifecycle.

   Scope: This policy applies to all NTU employees, contractors, and third-party vendors with access to systems, applications, or data that involve client information, as well as personnel with significant cybersecurity or privacy responsibilities.

   Procedures: Based on NIST SP 800-50 Revision 1, "Building a Cybersecurity and Privacy Learning Program"

   1. Strategy & Governance

      a. Establish a Senior Leadership Committee to oversee the learning program and meet regularly with Learning Program Managers to align strategy and priorities

   2. Role-Based Training Planning

      a. Identify roles with significant cybersecurity/privacy responsibilities via leadership and HR partnership.

      b. Integrate training requirements into job descriptions and position hierarchy documentation

   3. Development of Learning Content

      a. Implement a full CPLP life cycle: Plan & Strategy → Analyze & Design → Develop & Implement → Assess & Improve

      b. Use a mixture of awareness activities, practical exercises (e.g., tabletop drills, phishing campaigns), and role-based training modules

4. Onboarding & Refresher Training

    a. New personnel (including contractors) must complete foundational cybersecurity/privacy orientation during onboarding

    b. Personnel with significant responsibilities must receive specialized training before access is granted, plus annual refresher training

5. Development & Professional Growth

    a. Develop Individual Development Plans (IDPs) for identified key roles, to assess knowledge gaps and guide training

    b. Encourage staff to pursue industry-recognized certifications where appropriate

6. Assessment & Continuous Improvement

    a. Capture qualitative feedback (e.g., surveys, focus groups), activity metrics, and participant observations

    b. Review outcomes with senior leadership to refine and optimize the CPLP

Monitoring & Reporting: The IT department, in coordination with Human Resources, will maintain records of all employee security and privacy training activities, including completion dates, assessment results, and any remedial actions taken. Training completion rates and evaluation metrics will be reviewed quarterly, with summary reports provided to the designated representatives and senior leadership. Any deficiencies, non-compliance, or emerging training needs will be documented, escalated, and addressed promptly to ensure the program remains effective and compliant with applicable laws, regulations, and NTU policy.

Review: The training program is reviewed annually and updated by Learning Program Managers in consultation with the Senior Leadership Committee, ensuring alignment with legal, regulatory, and operational changes.

In conclusion, adopting a structured, lifecycle-based learning program—anchored in leadership, role-based design, and feedback

loops—ensures NTU builds a security-conscious workforce capable of managing cybersecurity and privacy risks effectively.

.

2. **Information System Risk Assessment**:

The following is NTU's high-level policy that is vendor agnostic and outlines Information System Risk Assessment for protecting sensitive information:

Purpose: To systematically identify, evaluate, and manage cybersecurity risks to NTU's information systems by implementing a repeatable, tiered risk assessment process. This process informs control selection, prioritization of mitigation strategies, and supports ongoing risk-based decision-making.

Scope: This policy applies to all NTU information systems—both on-premises and cloud environments—including related infrastructure, third-party services, and data repositories that handle client, student, or sensitive university data.

Procedures: Aligned with NIST SP 800-30 Rev 1, NTU implements the following structured and repeatable risk assessment cycle:

1. Prepare for the Assessment

    a. Clearly define the purpose and decision-making goals the risk assessment will support.

    b. Establish the scope of the assessment (systems, data types, processes, and applicable threats).

    c. Document any assumptions and constraints, such as organizational risk tolerance, resource limitations, or environmental considerations.

    d. Identify necessary information sources, risk models, and analytical approaches to be used.

2. Conduct the Assessment

    a. Identify relevant threat sources and events (e.g., insider threats, environmental hazards, adversarial incidents) and vulnerabilities impacting NTU systems.

b. Evaluate the likelihood of each threat exploiting a vulnerability, and assess the potential impact to confidentiality, integrity, and availability.

c. Prioritize risks by combining likelihood and impact to determine the risk level and identify which systems or assets require attention first.

3. Communicate Results

    a. Document findings comprehensively—including identified risks, their severity, and recommended mitigation strategies—in clear reports or dashboards.

    b. Share risk results with relevant stakeholders, such as system owners, IT leadership, and executive sponsors.

4. Maintain the Assessment (Continuous Monitoring)

    a. Continuously monitor the risk environment for changes in threats, vulnerabilities, or system configurations.

    b. Periodically update risk assessments to reflect new findings or operational changes.

    c. Use monitoring outcomes to recalibrate risk models, adjust mitigation strategies, and inform senior leadership of evolving risk posture

Monitoring & Reporting: The IT Risk Team will track completion and updates of risk assessments, including scheduled reviews and status of identified risk mitigation. Summary reports will be delivered quarterly to senior leadership, including any newly emerging risks or failed controls, to drive informed governance and resource allocation.

Review: This policy and the risk assessment process will be formally reviewed annually by the IT security leadership in collaboration with external security assessors, ensuring alignment with changing threats, regulatory updates, and institutional priorities.

In conclusion, by following a structured, repeatable risk assessment approach—grounded in preparation, execution, communication, and continuous monitoring—NTU ensures that information system risks are proactively managed. This contributes to better control alignment, faster response to emerging risks, and a more resilient security posture overall.

3. **Detecting and managing system failures**:

The following is NTU's high-level policy that is vendor agnostic and outlines Information System Risk Assessment for protecting sensitive information:

Purpose: To ensure NTU has effective processes in place to detect, prevent, respond to, and recover from system failures, security incidents, or attacks, thereby minimizing disruption to operations and protecting the confidentiality, integrity, and availability of client information.

Scope: This policy applies to all NTU networks, servers, endpoints, applications, and third-party systems that process, transmit, or store client data. It also applies to all staff and contractors involved in monitoring, incident response, or recovery activities.

Procedures: Aligned with IRS Publication 4557 – Safeguarding Taxpayer Data, NIST SP 800-61 Rev 2 – Computer Security Incident Handling Guide, and NIST SP 800-53 Rev 5 Incident Response Controls

1. System and Network Monitoring

    a. Deploy and maintain security monitoring tools (e.g., intrusion detection systems, intrusion prevention systems, SIEM platforms) to identify unusual or suspicious activity.

    b. Enable and review system, application, and network logs daily to detect anomalies or known attack patterns.

    c. Configure alerts for unauthorized access attempts, excessive login failures, and unusual data transfers.

2. Vulnerability Management

    a. Conduct regular vulnerability scans on all systems that handle client data.

    b. Prioritize and remediate identified vulnerabilities according to severity.

    c. Apply security patches and updates promptly, in accordance with NTU's patch management policy.

3. Incident Detection and Reporting

    a. Establish a clear reporting process for suspected system failures or security incidents, including immediate escalation to the designated representatives.

    b. Maintain a centralized incident log documenting the date, time, nature of the incident, and actions taken.

4. Incident Response

    a. Maintain and regularly update an Incident Response Plan (IRP) that outlines containment, eradication, recovery, and post-incident analysis procedures.

    b. Assemble an Incident Response Team (IRT) with clearly defined roles and responsibilities.

    c. Coordinate response efforts with relevant departments and third-party service providers when required.

5. Attack Prevention Measures

    a. Implement layered defenses such as firewalls, endpoint protection, network segmentation, and multifactor authentication.

    b. Restrict administrative access to critical systems to authorized personnel only.

    c. Disable unused services, ports, and protocols to reduce attack surface.

6. Business Continuity and Recovery

    a. Maintain regular, secure backups of all critical systems and data.

    b. Test restoration processes at least annually to ensure recoverability.

    c. Ensure backup data is stored securely offsite or in a hardened cloud environment with encryption.

7. Threat Intelligence and Information Sharing

a. Subscribe to relevant threat intelligence feeds (e.g., US-CERT, MS-ISAC) to stay informed of emerging threats.

b. Disseminate alerts and recommended actions to relevant technical and administrative staff.

Monitoring & Reporting: The IT department will continuously monitor systems for failures or attacks and produce monthly status reports detailing incidents, vulnerabilities addressed, and corrective actions taken. Significant incidents will be escalated to senior leadership within 24 hours.

Review: This policy and associated procedures will be reviewed annually by the designated representatives, incorporating updates from IRS Publication 4557, NIST incident handling guidance, and evolving threat intelligence.

In conclusion, by implementing structured processes for detecting, preventing, and responding to system failures and security incidents, NTU reduces downtime, mitigates data loss, and strengthens overall cybersecurity resilience.

104) *Protocols to select service providers that can maintain appropriate safeguards:* The representatives shall coordinate with those responsible for the third-party service procurement activities to raise awareness of and institute methods for selecting and retaining only those service providers that maintain appropriate safeguards for client information. The representative will also oversee the handling of client information by third-party service providers as follows.

Purpose: To ensure that third-party service providers engaged by NTU maintain appropriate administrative, technical, and physical safeguards for client information, in compliance with applicable laws, regulations, and NTU policies.

Scope: This policy applies to all departments and personnel involved in the selection, contracting, or management of third-party service providers that store, process, transmit, or have access to NTU client data.

Procedures: To ensure that service providers meet NTU's security and compliance requirements, the following procedures will be implemented:

1. Vendor Identification & Initial Screening

    a. Select potential service providers through reputable sources, preferably local when feasible.

b. Conduct preliminary research to ensure the provider operates within an acceptable legal and regulatory framework.

2. Reference & Reputation Verification
    a. Obtain and verify at least three professional references from existing or past clients.

    b. Review any publicly available reports, industry reviews, or security incident history.

3. Security Policy Review

    a. Provide the potential service provider with a copy of NTU's Information Security Plan (ISP) for review.

    b. Request the provider's own ISP or equivalent security documentation, specifically regarding the handling of client data.

4. Capability & Experience Assessment

    a. Confirm that the provider has proven experience handling sensitive information similar to NTU's operational needs.

    b. Verify the provider's ability to support NTU's specific hardware, software, and network requirements.

5. Compliance & Certification Verification

    a. Validate the provider's compliance with relevant regulations (e.g., GLBA, FERPA, HIPAA if applicable).

    b. Review any industry certifications such as ISO 27001, SOC 2 Type II, or partnerships with major technology vendors.

6. Contractual Safeguards

    a. Ensure contracts include explicit data protection clauses, confidentiality requirements, incident response timelines, and the right for NTU to audit security practices.

7. Ongoing Monitoring

    a. Conduct annual or semiannual reviews of the provider's performance and compliance.

b. Require providers to notify NTU immediately of any security incidents affecting NTU data.

Monitoring & Reporting: The designated representatives will track all approved service providers and document due diligence activities for each engagement. Any identified deficiencies in provider safeguards will be reported to senior leadership, and corrective measures will be required before continued engagement.

Review: This policy and its procedures will be reviewed annually by the designated representatives and updated as necessary to address changes in technology, regulatory requirements, and NTU operational needs.

In conclusion, by applying a structured vendor selection and oversight process, NTU ensures that all third-party service providers maintain robust safeguards for client information, reducing the risk of data breaches and ensuring compliance with applicable laws and best practices.

105) *Procedures for the evaluation and periodic adjustment of the ISP:* The representatives will evaluate and adjust the ISP based on the risk identification and assessment activities undertaken according to the ISP, as well as any material changes to the school's operations or other circumstances that may have a material impact on the ISP as follows.

Purpose: To ensure that NTU's Information Security Plan (ISP) remains effective, relevant, and compliant with applicable laws, regulations, and best practices through regular evaluation and updates based on risk assessments, operational changes, and evolving threats.

Scope: This policy applies to the designated representatives, IT leadership, and any departments or personnel involved in implementing, reviewing, or maintaining the ISP. It also applies to third-party service providers that handle client data.

Procedures: Aligned with NIST SP 800-53 Rev 5 – CA-2 Security Assessments, ISO/IEC 27001:2022 Clause 9.3 Management Review, and FTC Safeguards Rule requirements, NTU will conduct the following activities to evaluate and adjust the ISP:

1. Independent Evaluation

    a. Designate an unrelated, impartial party (internal audit team or external assessor) to evaluate ISP compliance and the effectiveness of security controls at least annually.

b. Review findings and document recommendations for improvement.

2. Scheduled Review Meetings

    a. Conduct semiannual review meetings with service provider personnel to discuss operational security concerns, incident reports, and compliance requirements.

    b. Invite relevant NTU department heads to provide feedback on ISP implementation challenges.

3. Risk-Based Updates

    a. Adjust ISP controls and procedures based on the results of risk identification and assessment activities.

    b. Integrate lessons learned from incidents, system failures, or audits into revised policies and procedures.

4. Change Management Integration

    a. Require an ISP review when there are material changes to NTU's operations, systems, data processing methods, or regulatory environment.

    b. Ensure all changes are documented, approved, and communicated to affected stakeholders.

5. Staff Feedback Mechanism

    a. Maintain a formal channel (e.g., email alias, secure feedback form) for staff to report security concerns or suggest improvements to the ISP.

    b. Review and address submissions during each ISP evaluation cycle.

6. Service Provider Compliance Review

    a. Require service providers to confirm annually that their safeguards align with NTU's ISP requirements.

    b. Document the results of these confirmations and address any identified gaps.

7. Documentation and Version Control

    a. Maintain a version-controlled repository of all ISP revisions, including a summary of changes, rationale, and approval records.

Monitoring & Reporting: The designated representatives will track the completion of evaluations, maintain meeting records, and prepare an annual ISP review report for senior leadership. This report will summarize findings, updates made, and outstanding improvement actions.

Review: This policy will itself be reviewed annually to ensure its procedures remain aligned with best practices, regulatory requirements, and NTU's operational needs.

In conclusion, regularly evaluating and adjusting the ISP ensures that NTU's security posture evolves alongside emerging threats, technological advancements, and organizational changes, maintaining compliance and safeguarding client data effectively.

References:

Risk Identification and Assessment:

1. NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments
    a. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
2. NIST SP 800-53 Rev. 5 – RA-1: Risk Assessment Policy and Procedures, RA-3: Risk Assessment
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. ISO/IEC 27005:2018 – Information Security Risk Management
    a. https://www.iso.org/standard/75281.html

Multifactor Authentication, Passwords, and PIN Requirements

1. NIST SP 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management
    a. https://pages.nist.gov/800-63-3/sp800-63b.html
2. NIST SP 800-53 Rev. 5 – IA-2: Identification and Authentication, IA-5: Authenticator Management
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. CIS Critical Security Controls v8 – Control 6: Access Control Management
    a. https://www.cisecurity.org/controls

Least Amount of Access (Least Privilege)

1. NIST SP 800-53 Rev. 5 – AC-6: Least Privilege
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
2. ISO/IEC 27002:2022 – Information Security Controls – Control 8.2: Privileged Access Rights
    a. https://www.iso.org/standard/75652.html
3. CIS Critical Security Controls v8 – Control 6: Access Control Management

a. https://www.cisecurity.org/controls

Data Loss Prevention (DLP)

1. NIST SP 800-53 Rev. 5 – MP-5: Media Transport Protection, SC-28: Protection of Information at Rest, SC-31: Cryptographic Module Authentication

    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. ISO/IEC 27002:2022 – Information Security Controls – Control 8.12: Data Leakage Prevention

    a. https://www.iso.org/standard/75652.html

3. CIS Critical Security Controls v8 – Control 3: Data Protection

    a. https://www.cisecurity.org/controls

Network Access Restrictions (Section 102 #4)

1. NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Federal Information Systems and Organizations

    a. AC-17: Remote Access, SC-7: Boundary Protection

    b. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. CIS Critical Security Controls v8 – Control 12: Network Infrastructure Management, Control 13: Network Monitoring and Defense

    a. https://www.cisecurity.org/controls

3. FTC Safeguards Rule – Gramm-Leach-Bliley Act

    a. https://www.ftc.gov/business-guidance/resources/financial-institutions-customer-information-safeguards

4. ISO/IEC 27002:2022 – Information Security Controls

    a. Control 8.23: Segregation in networks, Control 8.21: Use of cryptography in network services

    b. https://www.iso.org/standard/75652.html

Encryption (Section 102 #5)

1. NIST SP 800-53 Rev. 5 – SC-12: Cryptographic Key Establishment and Management, SC-13: Cryptographic Protection
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
2. NIST SP 800-57 Part 1 Rev. 5 – Recommendation for Key Management
    a. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
3. CIS Critical Security Controls v8 – Control 3: Data Protection
    a. https://www.cisecurity.org/controls
4. ISO/IEC 27002:2022 – Information Security Controls
    a. Control 8.24: Protection of information in transit, Control 8.25: Cryptographic controls
    b. https://www.iso.org/standard/75652.html
5. FTC Safeguards Rule – GLBA
    a. https://www.ftc.gov/business-guidance/resources/financial-institutions-customer-information-safeguards

Employee Management & Training (Section 103 #1)

1. NIST SP 800-50 Rev. 1 – Building a Cybersecurity and Privacy Learning Program
    a. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.ipd.pdf
2. NIST SP 800-53 Rev. 5 – AT-2: Awareness Training, AT-3: Role-Based Training
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. ISO/IEC 27001:2022 – Information Security Management Systems – Clause 7.2: Competence
    a. https://www.iso.org/standard/27001

Information Systems Risk Assessment (Section 103 #2)

1. NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments
    a. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
2. NIST SP 800-53 Rev. 5 – RA-3: Risk Assessment, RA-5: Vulnerability Monitoring and Scanning
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. ISO/IEC 27005:2018 – Information Security Risk Management
    a. https://www.iso.org/standard/75281.html
4. CIS Critical Security Controls v8 – Controls 15 & 16
    a. https://www.cisecurity.org/controls

Detecting & Managing System Failures (Section 103 #3)

1. IRS Publication 4557 – Safeguarding Taxpayer Data: A Guide for Your Business
    a. https://www.irs.gov/pub/irs-pdf/p4557.pdf
2. NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide
    a. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
3. NIST SP 800-53 Rev. 5 – IR-4: Incident Handling, IR-5: Incident Monitoring
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
4. CIS Critical Security Controls v8 – Control 17: Incident Response Management
    a. https://www.cisecurity.org/controls

Service Provider Selection (Section 104)

1. NIST SP 800-171 Rev. 2 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
    a. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
2. NIST SP 800-53 Rev. 5 – SA-9: External Information System Services
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

3. ISO/IEC 27036 – Information Security for Supplier Relationships
    a. https://www.iso.org/standard/59693.html
4. FTC Safeguards Rule – GLBA
    a. https://www.ftc.gov/business-guidance/resources/financial-institutions-customer-information-safeguards

Evaluation & Adjustment of the ISP (Section 105)

1. NIST SP 800-53 Rev. 5 – CA-2: Security Assessments, CA-7: Continuous Monitoring
    a. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
2. ISO/IEC 27001:2022 – Information Security Management Systems – Clause 9.3: Management Review
    a. https://www.iso.org/standard/27001
3. FTC Safeguards Rule – Periodic Evaluation Requirement
    a. https://www.ftc.gov/business-guidance/resources/financial-institutions-customer-information-safeguards