Policy # 56014

WRITTEN INFORMATION SECURITY PROGRAM

Effective Date:

Version Number	Revision Date
1.0	02/03/2023
2.0	02/27/2023

Responsible Office: Information Technology
Division: Operations and Administration

I. PURPOSE/OBJECTIVE

This document outlines the policy and procedures governing Grambling State University's development, maintenance and implementation of its comprehensive written information security program ("WISP"), including but not limited to the create effective administrative, technical, and physical safeguards for the protection of personal information of our employees, faculty, and students. This WISP sets forth Grambling State University's procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

II. APPLICABILITY

This policy is applicable to address that all policies, procedures and processes insure effective administrative, technical and physical safeguards for protection of employees, faculty and student data.

III. STATEMENT OF POLICY

The WISP is designed to:

- Ensure the security, confidentiality, integrity, and availability of personal information Grambling State University collects, creates, uses, and maintains;
- Protect against any reasonably anticipated threats to hazards to the security, confidentiality, integrity, or availability of such information;
- Protect against unauthorized access to or use of Grambling State University's maintained personal information in a manner that could result in substantial harm or inconvenience to any customer or employee; and
- Define an information security program that is appropriate to Grambling State University's size, scope, and business its available resources; and the amount of personal information that Grambling State University owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

IV. SCOPE

This WISP applies to all employees, contractors, officers and directors of Grambling State University. It applies to any records that contain personal information in any format and on any media, whether electronic or paper form.

For purposes of this WISP, "personal information" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

- Social Security number;
- Student ID Number;
- Driver's license number, other government-issued identification number, including passport number or tribal identification number;
- Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account.
- Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer.
- Biometric data collected from the individual and used to authenticate the individual during transaction, such as an image of a fingerprint, retina, or iris; or
- Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.
- Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, , or local government records.

V. INFORMATION SECURITY COORDINATOR

Grambling has designated a Chief Information Security Officer responsible to implement, coordinate, and maintain this WISP. This designated employee (the "Data Security Coordinator") will be responsible for the following initial implementation of this WISP, including:

- Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation plans;

- Coordinating the development, distribution, and maintenance of information security policies and procedures;

- Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information;

- Ensuring that the safeguards are implemented and maintained to protect personal information throughout the campus community, where applicable;

- Overseeing service providers that access or maintain personal information;

- Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis;

- Defining and managing incident response procedures;
- Establishing and managing enforcement policies and procedures for this WISP, in collaboration with HR and management;

- Employee and contractor Security Awareness training;

- Providing periodic training regarding this WISP, institutional safeguards, and relevant information security policies and procedures for all employees, and contractors who have or may have access to personal information to ensure users are made aware of the security risks associated with their activities and the security systems and networks (NIST 3.2.1/CMMC 3.2.1)(NIST 3.3.3/CMMC 3.3.3);

- Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through written acknowledgement forms or tracking

- Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information and update security plans as appropriate (NIST 3.12.4/CMMC 3.12.4)

- Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or information security policies and procedures.

- Periodically reporting to management regarding the status of the information security program and safeguards to protect personal information.

VI. RISK ASSESSMENT

As a part of developing and implementing this WISP, Grambling State University will conduct a periodic, documented risk assessment on a regular basis, or whenever there is a material change in GSU business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information. (NIST 3.11.1/CMMC 3.11.1)

The risk assessment shall:

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information.
- Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information.
- Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified (NIST 3.11.2/CMMC 3.11.2)
- Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:
    - Employee and contractor training and management;
    - Employee and contractor compliance with this WISP and related policies and procedures;
    - Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
    - Ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

Following each risk assessment, GSU will:

- Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
- Reasonably and appropriately address any identified gaps and remediate vulnerabilities and risks in accordance with assessments (NIST 3.11.3/CMMC 3.113)
- Regularly monitor the effectiveness of GSU’s safeguards, as specified in this WISP.

VII. INFORMATION SECURITY POLICIES AND PROCEDURES

As part of this WISP, Grambling State University will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees and contractors, to:

- Detail the implementation and maintenance of GSU's administrative, technical, and physical safeguards.
- Provide privacy and security notices consistent with applicable rules, laws and regulations. (NIST 3.1.9/CMMC 3.1.9)
- Identify, report, and correct information and information system flaws in a timely manner (NIST 3.14.1/CMMC 3.14.1)

Establish policies regarding:

- The collection of personal information that is reasonably necessary to accomplish GSU's legitimate business transactions or to comply with any and all federal, or local regulations;
- The storage of personal information that is limited to the time reasonably necessary to accomplish GSU's legitimate business transactions or to comply with any and all federal, or local regulations;
- Information classification;
- Information handling practices for personal information, including the storage, access, disposal, and external transfer or transportation of personal information;
- User access management, including identification and authentication (using passwords or other appropriate means);
- Encryption;
- Computer and network security;
- Incident Reporting and Response;
- USB/External Storage Device (NIST 3.1.21/CMMC 3.1.21)
- Physical security, including;
    a. Limiting physical access to organizational systems, equipment, and the respective operating environments to authorized individuals only (NIST 3.10.1/CMMC PE.1.131)
    b. Ensuring that all non-authorized individuals will be escorted, monitored and required to sign, in and out of any secure facilities or location housing CUI, PII, or Critical Infrastructure (NIST 3.10.3/CMMC 3.10.3)
    c. Recording visits and maintaining physical audit logs (NIST 3.10.4/CMMC 3.10.4)

VIII. SAFEGUARDS

Grambling State University will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that GSU owns or maintains on behalf of others.

- Safeguards shall be appropriate to the size, scope, and business; its available resources; and the amount of personal information that is owned or maintained on behalf of others, while recognizing the need to protect both customer and employee information;
- Grambling State University shall document its administrative, technical, and physical safeguards in information security policies and procedures;
- Implement Segregation of Duties and;
- Administrative safeguards and technical safeguards shall include appropriately configured controls and processes that match and align with the necessary requirements needed for effective security, which may include:
    - Designating one or more employees to coordinate the information security program;
    - Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks;
    - Training employees in security program practices and procedures, with management oversight;
    - Selecting third party service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract; and
    - Adjusting the information security program in light of business changes or new circumstances;
    - Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;
    - Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and
    - Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system. (NIST 3.1.8/CMMC 3.1.8)
    - Limiting use of portable storage device use (NIST 1.3.1/CMMC 1.3.1)
- Secure access control measures may include:
    - Identifying system users, processes acting on behalf of users, and devices (NIST 3.5.1/CMMC 3.5.1)

- Limiting system access to authorized users, processes acting on behalf of authorized users, and devices, including other information systems. (NIST 3.1.1/CMMC 3.1.1)
- Limiting system access to the types of transactions and functions that authorized users are permitted to execute. (NIST 3.1.2/CMMC 3.1.2)
- Restricting access to records and files containing personal information to those with a need to know to perform their duties; and
- Access to systems containing PII are limited to authorized users as configured and enforced by the systems/ERP application.
- Monitoring and enforcement of such access will be performed on an annual basis.
- Ensuring that CUI is only permitted to flow from the server to end user based on approved authorization (NIST 3.1.3/CMMC 3.1.3)
- Assigning unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) to each individual with computer or network access that are reasonably designed to maintain security.
- Using non-privileged accounts or roles when accessing nonsecurity functions. (NIST 2.3.1/CMMC 2.3.1)
- Separating the duties of individuals to reduce the risk of malevolent activity without collusion (NIST 3.1.4/CMMC 3.1.4)
- Preventing non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. (NIST 3.1.7/CMMC 3.1.7)
- Terminating (automatically) user sessions after a defined condition. (NIST 3.1.11/CMMC 3.1.11)
- Ensuring least privilege administration will be regularly practiced on systems and applications and privileged access will be reviewed annually or after any system changes or significant upgrades (NIST 3.4.6/CMMC 3.4.6)
- Employing the principle of least privilege, including for specific security functions and privileged accounts. (NIST 3.1.5/CMMC 3.1.5)
- Ensuring privileged user account will only be used when performing privileged tasks and responsibilities
- Ensuring privileged users will maintain separate accounts in order to limit privileged access to privileged tasks only. (NIST 3.1.6/CMMC 3.1.6)
- Requiring MFA for all netwok access for all accounts and local access for privileged accounts. (NIST 3.5.3/CMMC 3.5.3)
- Utilizing replay resistant authentication mechanisms. (NIST 3.5.4/CMMC 3.5.4)
- Not reusing identifiers. (NIST 3.5.5./CMMC 3.5.5)
- Disabling user accounts after a defined period of time. (NIST 3.5.6/CMMC 3.5.6)
- Enforcing a minimum password complexity and change of characters when new

passwords are created. (NIST 3.5.7/CMMC 3.5.7)

- Maintaining audit logs and records that are created and retained to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized systems activity (NIST 3.3.1/CMMC 3.3.1)

- Segregation of Duties may include:
  - Ensuring segregation of duties based on its internal User Roles and Responsibilities table and it will encompass the auditing of systems activity, events and administrator access to different systems and functions.
  - Auditing to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions (NIST 3.3.2/CMMC 3.3.2)
  - Providing a secure access environment by enforcing segregation of duties where appropriate and possible

- Secure Remote Access/Connection to Systems and Networks may include:
  - Verify and control/limit connections to and use of external information systems (NIST 3.1.20/CMMC 3.1.20)
  - Authorize wireless access prior to allowing such connections (NIST 3.1.16/CMMC 3.1.16)
  - Monitor and control remote access sessions (NIST 3.1.12/CMMC 3.1.12)
  - Route remote access via managed access control points (NIST 3.1.14/CMMC 3.1.14)
  - Protect wireless access using authentication and encryption (NIST 3.1.17/CMMC 3.1.17)
  - Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (NIST 3.1.13/CMMC 3.1.13)
  - Authorize remote execution of privileged commands and remote access to security-relevant information. (NIST 3.1.15/CMMC 3.1.15)
  - Controlling connection of mobile devices. (NIST 3.1.18/CMMC 3.1.18)

- Login and Access behavior safeguards may include:
  - Limit unsuccessful logon attempts (NIST 3.1.8/CMMC 3.1.8)
  - Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity (NIST 3.1.10/CMMC 3.1.10)

- Encryption as a safeguard may include:
  - Encryption of all CUI
  - Encryption (Data in Transit & at Rest) of all personal and CUI information traveling

across networks, including email, as well as personal and CUI in storage on laptops, desktops and mobile devices. (NIST 3.13.8/CMMC 3.13.8)

- Use encrypted sessions for the management of network devices (CMMC SC.2.179)
- Encrypt CUI on mobile devices and mobile computing platforms (NIST 3.1.19/CMMC 3.1.19)

- System Monitoring, Prevention & Detection safeguards may include:
  - Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures.
  - Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information running malicious code protection (NIST 3.14.2/CMMC 3.14.2)
  - Firewall and malicious code protection shall be configured for automatic updates (NIST 3.14.2/CMMC 3.14.2) (NIST 3.14.6/CMMC 3.14.6)
  - Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis. (NIST 3.14.2/CMMC 3.14.2)
  - Control information posted or processed on publicly accessible information systems. (NIST 3.1.22/CMMC 3.1.22)

- Physical safeguards shall, at a minimum, provide for:
  - Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers.
  - Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal.
  - Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards, and sanitize or destroy information system media containing private or regulatory restricted data before disposal or release for reuse. (NIST 3.8.3/CMMC 3.8.3)

IX. SERVICE PROVIDER OVERSIGHT

Reasonable steps will be taken to select, retain and oversee each third party service provider that may have access to or otherwise create, collect, use, or maintain personal information on its behalf, by:

- Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws, regulations, mandates and institutional policy and obligation.
- Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws, regulations, mandates and institutional policy and obligations.
- Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws, regulations, mandates and institutional policy and obligations.

X. MONITORING

Regular testing and monitoring of the implementation and effectiveness of the information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal information. Reasonably and appropriately address any identified gaps.

XI. INCIDENT RESPONSE

Establish and maintain policies and procedures regarding information security incident response. Such procedures shall include:

- The preparation, detection, analysis, containment, recovery and user response activities (NIST 3.6.1/CMMC 3.6.1)
- Specific response actions to security alerts and advisories shall be maintained either by institution personnel or contracted third party SOC provider (NIST 3.14.3/CMMC 3.14.3)
- Alerts are monitored by institution personnel or third party SOC (NIST 3.14.3/CMMC 3.14.3)
- Response actions will be taken by institution technology and security personnel. (NIST 3.14.3/CMMC 3.14.3)
- Ensuring the analysis and triage of events to support event resolution and incident declaration (CMMC IR.2.094)
- Documenting the response to any security incident or event that involves a breach of security;
- Performing a post-incident review of events and actions taken;
- Reasonably and appropriately addressing any identified gaps.

XII. ENFORCEMENT

Violations of this WISP may result in disciplinary action, in accordance with information security policies and procedures and human resources policies. Please see Grambling State University's HR policy for details regarding GSU's disciplinary process.

XIII. PROGRAM REVIEW & CHANGE MANAGEMENT

Grambling State University will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in GSU's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of institutional assets and data.

- Grambling State University shall retain documentation regarding any such program review, including any identified gaps and action plans.
- Grambling State University will track, review, approve, or disapprove, and log changes to organizational systems (NIST 3.4.3/CMMC 3.4.3)
- Prior to approving and implementing any system changes, Grambling State University will analyze the security impact of such requested or required change (NIST 3.4.4/CMMC 3.4.4)

XIV. REVISION/REVIEWED

SEPTEMBER 11, 2023