Third Party & Vendor Management Policy

Grambling State University Information Technology

Jay Ellis, Chief Information Officer

Revision History:

Version Number	Revision Date
1.0	

Introduction

Third party entities play an important role in assisting and supporting Grambling State University business and academic operations. Each service provider (vendors, consultants, third parties) shall implement written policies and procedures designed to ensure the security, confidentiality and integrity of Grambling State University data and assets. When properly authorized, covered entities may be able to view, copy, and modify data and audit logs. Additionally, they may assist in correcting software and operating system problems, monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems, and reset alarm thresholds. Setting limits and controls on covered entities helps reduce the risk of security incidents, financial liability, loss of trust and other damaging consequences.

This policy also requires third parties, vendors, contractors, etc., and any subcontractors with whom it is authorized to share the data, to share only the minimum information necessary, to securely return or destroy the data upon expiration of the contract, and to provide immediate notification to the campus, whenever there is a breach of sensitive data or services that may affect or impact the University.

Purpose

The purpose of this policy is to provide a set of measures, standards and guidelines that will help mitigate information security risks associated with third party & vendor access and their responsibility for the protection and security of Grambling State University.

This policy and corresponding procedures will help ensure that Grambling State University has safeguards in place to oversee service providers, by:

1. Taking reasonable steps to select and retain service providers that can maintain appropriate safeguards for the customer information at issue.

2. Requiring service providers by contract to implement and maintain such safeguards

3. Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.

Policy

Third party access to Grambling State University's network and system resources must comply with all University's applicable rules, policies, standards, and agreements.

Grambling State University will provide a point of contact for each third party or vendor as part of the onboarding process. The point of contact will work with the third party or vendor to make certain that he or she is in compliance with these rules.

1. Each third party user with access to Grambling State University sensitive information must be cleared to handle that information.
2. All third party personnel with access to any information system, must adhere to all regulations and governance standards associated with accessible data (e.g. PCI and security requirements for cardholder data, FERPA requirements, HIPPA, GLBA, etc.)
3. Third party personnel must report all security incidents directly to their assigned point of contact.
4. Third party personnel must follow all applicable University change management processes and procedures.
5. Third party credentials must be uniquely identifiable, and password management must follow Grambling State University's password procedures and policies.
6. Upon termination of a contract or at the request of Grambling State University, the third party must surrender all equipment and supplies immediately.
7. Third parties are required to comply with Grambling State University's auditing requirements.

Procedures

To properly oversee service providers, third parties, consultants, contractors, etc., Grambling State University will follow these procedures in the selection and monitoring each entities security program and the appropriate safeguards and controls that help protect and secure University data, assets and resources.

1. No entity, that deals with technology or University data, will be onboarded without the approval of Grambling State University Information Technology/Security Department.
2. Due Diligence efforts will include a review of all necessary documentation deemed appropriate to make a reasonable determination of each entities security posture.
3. Security review will happen prior to onboarding new provider.
4. Existing providers will undergo an annual review to continually monitor their security program and controls.

5. Documentation reviewed may consist of contracts, hecvats, vpats, soc reports, etc., and will be stored and maintained throughout the lifecycle of the partnership.

Enforcement

Violation of this Policy may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants. Additionally, individuals are subject to loss of Grambling State University information resources, access privileges, and potential civil and criminal prosecution.

Exclusions or Special Circumstances

Exceptions to this Policy shall only be allowed if approved by the Chief Information Officer or delegate, and this approval must be documented, saved, and monitored.