Third Party Vendor Access Policy

Introduction

Third party entities play an important role in the support of hardware and software management, and operations for the University. When properly authorized they can remotely view, copy, and modify data and audit logs; they correct 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 what can be seen, copied, modified, and controlled by a third party will eliminate or reduce the risk of loss of revenue, liability, loss of trust and potential damage to University of Arkansas at Pine Bluff assets.

This policy must also require the third-party, and any of its subcontractors with whom it is authorized to share the data, to share only the minimum information necessary, to securely return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the campus, whenever there is a breach of sensitive data.

Purposes

The purpose of this policy is to provide a set of measures that will mitigate information security risks associated with third party access and third party responsibilities and protection of University of Arkansas at Pine Bluff information. This policy also applies to all individuals who are responsible for the installation of new University Information Resources assets and who allow third party access for maintenance, monitoring and troubleshooting purposes of existing Information systems.

This policy is subject to change as new technologies and methods of implementing these technologies emerge.

Policy

Third party physical access to the data center will be enforced as stated in the Data Center Access policy and require the approval and authorization by the Technical Services Director. Third party access to the data center facilities must sign a Confidential Information Agreement prior to accessing the University of Arkansas at Pine Bluff network. Third party access is temporary.

Third parties must comply with all applicable rules, policies and the University standards and agreements, including, but not limited to:

- Data Center Access
- Code of Business Conduct
- Acceptable use of Technology
- VPN Access
- Confidential Information Agreement

University of Arkansas at Pine Bluff will provide a Technical Services point of contact for the third party. The point of contact will work with the third party to make certain that he or she is in compliance with these rules.

1. Each third party user with access to University of Arkansas at Pine Bluff sensitive information must be cleared to handle that information.
2. All third party personnel with access to any High Security System must adhere to all regulations and governance standards associated with that data (e.g. PCI and security requirements for cardholder data, FERPA requirements and HIPPA privacy rule for student records).
3. Third party personnel must report all security incidents directly to their assigned point of contact.
4. If third party vendor is involved in a University security incident, it will have to be reported and documented in accordance to the Confidential Information Agreement.
5. Third party personnel must follow all applicable University change management processes and procedures.
6. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the corresponding department head. If access to the internal network is required user must abide by the VPN access policy.
7. Third party credentials must be uniquely identifiable, and password management must follow University of Arkansas at Pine Bluff password policy. Third party's major work activities must be documented. Project milestones, deliverables, and "as build" documents must be submitted during an upon project completion.
8. Upon termination of a contract or at the request of University of Arkansas at Pine Bluff, the third party will return or destroy all University information and provide written certification of that return or destruction within 24 hours.
9. Upon termination of a contract or at the request of University of Arkansas at Pine Bluff, the third party must surrender all equipment and supplies immediately.
10. Third parties are required to comply with University of Arkansas at Pine Bluff auditing requirements.

Implementation

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 University of Arkansas at Pine Bluff Information Resources access privileges and civil and criminal prosecution. Third Party Vendors shall be held accountable for payment for reimbursement of damages resulting from a disclosure, breach, data loss or other events that puts the university data at risk.

REFERENCES AND RELATED DOCUMENTS

Researched on the internet and reviewed various Universities' policies online.

POLICY DOCUMENT INFORMATION

Continuous improvement. The content of this document subject to regular review based on input from UAPB Technical Services staff and the campus community. Suggestions for enhancement should be submitted to the Director of Technical Services.