Vendor Access Policy

Introduction
Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to Texas A&M University-Kingsville.

1. Purpose
1.1. The purpose of the Texas A&M University-Kingsville Vendor Access Policy is to establish the rules for vendor access to Texas A&M University-Kingsville Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of Texas A&M University-Kingsville information.

2. Audience
2.1. The Texas A&M University-Kingsville Vendor Access Policy applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

3. Vendor Access Policy
3.1. Vendors must comply with all applicable Texas A&M University-Kingsville policies, practice standards and agreements, including, but not limited to:
- Safety Policies
- Privacy Policies
- Security Policies
- Auditing Policies
- Software Licensing Policies
- Acceptable Use Policies

4. Vendor agreements and contracts must specify:
4.1. The Texas A&M University-Kingsville information the vendor should have access to
4.2. How Texas A&M University-Kingsville information is to be protected by the vendor
4.3. Acceptable methods for the return, destruction or disposal of Texas A&M University-Kingsville information in the vendor’s possession at the end of the contract
4.4. The Vendor must only use Texas A&M University-Kingsville information and Information Resources for the purpose of the business agreement
4.5. Any other Texas A&M University-Kingsville information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others
4.6. Texas A&M University-Kingsville will provide a CIS point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
4.7. Each vendor must provide Texas A&M University-Kingsville with a list of all employees working on the contract. The list must be updated and provided to Texas A&M University-Kingsville within 24 hours of staff changes.
4.8. Each on-site vendor employee must acquire a Texas A&M University-Kingsville identification badge that will be displayed at all times while on Texas A&M University-Kingsville premises. The badge must be returned to Texas A&M University-Kingsville when the employee leaves the contract or at the end of the contract.
4.9. Each vendor employee with access to Texas A&M University-Kingsville sensitive information must be cleared to handle that information.
4.10. Vendor personnel must report all security incidents directly to the appropriate Texas A&M
4.11. If vendor management is involved in Texas A&M University-Kingsville security incident management the responsibilities and details must be specified in the contract.

4.12. Vendor must follow all applicable Texas A&M University-Kingsville change control processes and procedures.

4.13. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Texas A&M University-Kingsville management.

4.14. All vendor maintenance equipment on the Texas A&M University-Kingsville network that connects to the outside world via the network, telephone line, or leased line, and all Texas A&M University-Kingsville IR vendor accounts will remain disabled except when in use for authorized maintenance.

4.15. Vendor access must be uniquely identifiable and password management must comply with the Texas A&M University-Kingsville Password Policy and Admin/Special Access Policy. Vendor’s major work activities must be entered into a log and available to Texas A&M University-Kingsville management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

4.16. Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Texas A&M University-Kingsville or destroyed within 24 hours.

4.17. Upon termination of contract or at the request of Texas A&M University-Kingsville, the vendor will return or destroy all Texas A&M University-Kingsville information and provide written certification of that return or destruction within 24 hours.

4.18. Upon termination of contract or at the request of Texas A&M University-Kingsville, the vendor must surrender all Texas A&M University-Kingsville Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Texas A&M University-Kingsville management.

4.19. Vendors are required to comply with all State and Texas A&M University-Kingsville auditing requirements, including the auditing of the vendor’s work.

4.20. All software used by the vendor in providing service to Texas A&M University-Kingsville must be properly inventoried and licensed.

4.21. Violations of this policy must be reported to the IRM or ISO.

**Disciplinary Actions**

Violation of this policy may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.