SECTION: Information Technology **Policy 04.06.27**
AREA: Information Security

SUBJECT: Vendor Access Policy

I. 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, correct software and operating systems 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 vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the University.

II. PURPOSE

The purpose of the Vendor Access Policy is to establish the rules for vendor access to University Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of University information. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

III. SCOPE

The Vendor Access Policy applies to all individuals who 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.

IV. POLICY PROVISIONS

A. Vendors must comply with all applicable University policies, practice standards and agreements, including, but not limited to:
   1. Safety policies;
   2. Privacy policies;
   3. Security policies;
   4. Auditing policies;
   5. Software licensing policies, and;
   6. Acceptable use policies.

B. The University will provide an Office of Information Technology ("OIT") 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.

C. Vendor agreements and contracts must specify:

1. University information the vendor may have access to.
2. How University information is to be protected by the vendor.
3. Acceptable methods for the return, destruction or disposal of University information in the vendor's possession at the end of the contract.
4. That the vendor must only use University information and Information Resources for the purpose of the business agreement.
5. That any other University information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
6. If vendor management is involved in University security incident management, the responsibilities and details must be specified in the contract.
7. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate University management.

D. Other requirements:

1. Each vendor must provide the University with a list of all employees working on the contract. The list must be updated and provided to the University within twenty-four (24) hours of staff changes.
2. Each on-site vendor employee must acquire a University identification badge that will be displayed at all times while on University premises. The badge must be returned to the University when the employee leaves the contract or at the end of the contract.
3. Each vendor employee with access to University sensitive information must be cleared to handle that information.
4. Vendor personnel must report all security incidents directly to the appropriate University personnel.
5. Vendor must follow all applicable University change control processes and procedures.
6. All vendor maintenance equipment on the University network that connects to the outside world via the network, telephone line, or leased line, and all University Information Resources vendor accounts will remain disabled except when in use for authorized maintenance.
7. Vendor access must be uniquely identifiable and password management must comply with University Password Security Policy (MAPP 04.06.17) and Admin/Special Access Policy (MAPP 04.06.06).
8. Vendor's major work activities must be entered into a log and available to University 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.
9. 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 the

University or destroyed within twenty-four (24) hours.

10. Upon termination of contract or at the request of the University, the vendor will return or destroy all University information and provide written certification of that return or destruction within twenty-four (24) hours.
11. Upon termination of contract or at the request of the University, the vendor must surrender all University Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized University management.
12. Vendors are required to comply with all State and University auditing requirements, including the auditing of the vendor's work.
13. All software used by the vendor in providing services to the University must be properly inventoried and licensed.

V. DISCIPLINARY ACTION

Violation of this policy may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline and Termination Policy). It may also result in termination of the contract with the vendor.

VI. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 1
- Security Standard 2
- Security Standard 3
- Security Standard 4
- Security Standard 5
- Security Standard 6
- Security Standard 7
- Security Standard 9
- Security Standard 16
- Security Standard 17
- Security Standard 21

VII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every year, on or before September 1

VIII. APPROVAL

Jim McStan

Vice President of Finance

Joe Ludley

President

2/18/11

Effective Date