Policy

Vendor Access

Date: April 23, 2010

Purpose: The purpose of the Vendor Access Policy is to establish the rules for vendor access to Otis College's Information Resources, vendor responsibilities, and protection of Otis College information.

Scope: The 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.

Discussion: Vendors play an important role in the support of hardware and software management, and operations for the Otis College community. 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 the College.

Definitions: **Information Resources (IR):** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Vendor: someone who exchanges goods or services for money.

Details: Vendors will follow the following requirements:

- Vendors must comply with all applicable College policies, practice standards and agreements, including, but not limited to:
  - Safety Policies
  - Privacy Policies
  - Security Policies
  - Auditing Policies
  - Software Licensing Policies
  - Acceptable Use Policies

- Vendor agreements and contracts must specify:
  - The College information the vendor should have access to
  - How the College information is to be protected by the vendor
  - Acceptable methods for the return, destruction or disposal of the College information in the vendor's possession at the end of the contract
  - The Vendor must only use the College information and Information Resources for the purpose of the business agreement
  - Any other College information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- The College will provide an Information Systems 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.
- Each vendor must provide the College with a list of all employees working on the contract. The list must be updated and provided to the College within 24 hours of staff changes.
- Each vendor employee with access to the College's sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate College personnel.
- If vendor management is involved in the College security incident management the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable College change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate management.
- All vendor maintenance equipment on the College's network that connects to the outside world via the network, telephone line, or leased line, and all College IR vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the College policies and procedures. Vendor's major work activities must be entered into a log and available to College 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.
- College staff will review vendor logs when the vendor has worked with sensitive data.
- 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 College or destroyed within 24 hours.
- Upon termination of contract or at the request of the College, the vendor will return or destroy all College information and provide written certification of that return or destruction within 24 hours.

- Upon termination of contract or at the request of the College, the vendor must surrender all College Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized College management.
- Vendors are required to comply with all State and College auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to the College must be properly inventoried and licensed.

Disciplinary Actions:

Violation of this policy may result in disciplinary action which may include 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 College Information Resources access privileges, civil, and criminal prosecution.

Revisions: 04/23/10 - Created