

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

| | | | |
|----------------------|--|-----------------|------------------------------------|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | May 2011 |
| Policy 5.8.18 | Third-Party Management of Information Resources | Responsibility: | Chief Information Security Officer |

THIRD-PARTY MANAGEMENT OF INFORMATION RESOURCES

Policy

All vendors and third-party information technology service providers must comply with all applicable Health Science Center policies, practice standards and agreements, including, but not limited to:

- Safety policies
- Privacy policies
- Security policies
- Auditing policies
- Software licensing policies
- Acceptable use policies

The third-party providers are bound by any applicable federal, state, and local regulations, as well as business associate agreements entered into with the Health Science Center.

All Health Science Center organizations (schools, departments, offices, and centers) engaging vendors, contractors, consultants or other third-party information technology service providers are responsible for managing that relationship, including appropriate termination notifications. Departments should evaluate potential third-party provider agreements to ensure adequate security controls are in place prior to finalizing contract agreements. The Information Security Office has developed the "[Third-Party Risk Assessment Security Standard](#)" and related "[Information Security Third-Party Assessment Survey](#)" to assist in that evaluation process. This process is recommended for all third-party relationships, but mandatory for relationships involving confidential/high-risk data, see the *Handbook of Operating Procedures* (HOP), [Section 5.8.21](#), "Data Classification". These documents, as well as other security standards, guidelines, and surveys pertaining to information security policies may be found at the Information Management and Services Web site <http://ims.uthscsa.edu/policies.aspx>.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

| | | | |
|----------------------|--|-----------------|------------------------------------|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | May 2011 |
| Policy 5.8.18 | Third-Party Management of Information Resources | Responsibility: | Chief Information Security Officer |

Third-party agreements and contracts must specify:

- the requirement to comply with applicable federal, state, and local regulations and Health Science Center policies;
- the Health Science Center information the third-party provider should have access to;
- how Health Science Center information is to be protected by the third-party;
- acceptable methods for the return, destruction or disposal of Health Science Center information in the third-party provider's possession at the end of the contract;
- the third-party provider must use Health Science Center information and information resources only for the purposes of the business agreement; and,
- any Health Science Center information acquired in the course of the contract cannot be used for the third-party provider's own purposes or divulged to others.

The Health Science Center, including UT Medicine, will provide an information systems (e.g., Systems and Network Operations (SNO) or Information Management Client Support Services (IMCSS) staff, Technical Support Representative (TSR), etc.) point of contact for the third-party provider. The point of contact will work with the third-party provider to ensure compliance with these policies.

Each third-party provider must provide the Health Science Center with a list of all employees working on the contract. The list must be updated and provided to the Health Science Center within 48 hours of staff changes. Each on-site third-party employee must acquire a Health Science Center identification badge that will be displayed at all times while on Health Science Center premises. Refer to the HOP, [Section 8.7.10](#), "Identification Badge Policy" for information.

Each third-party employee with access to Health Science Center sensitive information must be approved by the data owner (Principal

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

| | | | |
|----------------------|--|-----------------|------------------------------------|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | May 2011 |
| Policy 5.8.18 | Third-Party Management of Information Resources | Responsibility: | Chief Information Security Officer |

Investigator (PI), Access Control Executive (ACE), department head, etc.) to handle that information. Access to information will be based on job responsibilities and a need-to-know. Changes in job duties or status will require appropriate access modifications.

The third-party personnel must report all security incidents directly to the appropriate Health Science Center personnel. If third-party management is involved in Health Science Center security incident management, the responsibilities and details must be specified in the contract.

The third-party provider must follow all applicable Health Science Center change control processes and procedures.

All third-party maintenance equipment on the Health Science Center network that connects to the outside world via the network, telephone line, or leased line, and all Health Science Center information resource third-party accounts will remain disabled except when in use for authorized maintenance. All remote third-party access the Health Science Center network must use a Health Science Center approved form of secure access, such as VPN or secure shell.

Third-party access must be uniquely identifiable and password management must comply with the Health Science Center password practice standard and administrative/special access practice standard.

Third-party access to the Health Science Center's network must comply with existing process requirements including information security awareness training, acceptable use acknowledgement and a non-disclosure agreement.

The third-party provider's major work activities must be entered into a log and available to Health Science Center 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.

Upon departure of a third-party employee from the contract for any reason, the third-party will ensure that all sensitive information is collected and returned to the Health Science Center or destroyed (at the

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

| | | | |
|----------------------|--|-----------------|------------------------------------|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | May 2011 |
| Policy 5.8.18 | Third-Party Management of Information Resources | Responsibility: | Chief Information Security Officer |

University's discretion) within 48 hours. Upon termination of contract or at the request of the Health Science Center, the third-party provider will return or destroy (at the University's discretion) all Health Science Center information and provide written certification of that return or destruction within 48 hours.

Upon termination of contract or at the request of the Health Science Center, the third-party provider must surrender all Health Science Center identification badges, access cards, equipment and supplies immediately. Authorized Health Science Center management must document equipment and/or supplies to be retained by the third-party provider.

Third-party providers are required to comply with any auditing requirements, including the auditing of the third-party's work.

The third-party provider must take reasonable precautions to ensure that all software used on Health Science Center property is properly licensed.

Authority

Violations of this policy are subject to disciplinary action as described in the HOP, [Section 2.1.2](#), "*Handbook of Operating Procedures*".
