Hope International University

Vendor Management Policy

Vendor Relationships

Objective: Ensure that vendor relationships are covered by appropriate security requirements and controls.

Information security in Vendor relationships

University departments must ensure that agreements with Vendors contain security requirements that are consistent with this policy and supporting standards for the protection of and access to Institutional Information and IT Resources (HIU Appendix – Data Security and Privacy or the CISO-approved equivalent).

Vendor service delivery management

Departments must ensure that Vendor agreements:

• Incorporate into the purchase agreement the applicable Institutional Information and IT Resource security requirements (HIU Appendix – Data Security and Privacy or the CISO-approved equivalent).

• Consider the term of the agreement and changes in information security requirements.

• Receive approval from the CISO on the information security requirements for Critical IT Infrastructure.

Vendors subject to the Payment Card Industry (PCI) Data Security Standard must sign, or have incorporated into the purchase agreement, the applicable PCI security requirements, terms and conditions.

Vendors who qualify as a Business Associate under GLBA, HIPAA/HITECH must sign a HIU-approved Business Associate Agreement (BAA).

Vendors subject to other terms and conditions specified by law or regulation must have the applicable terms included in the agreement.

Department responsibilities when using Vendors.

Departments must work with the Business Office/Information Technology departments to ensure that agreements and other arrangements with persons or Vendors conform to the requirements of this policy.

Departments using Vendors must:

• Use only approved and disclosed access methods.

• Comply with the applicable HIU Minimum Security Standard.

Hope International University – Vendor Management Policy

• Complete a Risk Assessment.

• Ensure that Vendor access to IT Resources or Institutional Information is consistent with HIU security policies.

• Notify Vendors when Workforce Members separate if the Vendor facilitates access to IT Resources.

• Ensure that Vendors report Breaches and Information Security Incidents to the CISO.

• Report observed Vendor security lapses to the CISO.

• Document clearly the responsibilities of each party.

• Ensure review and adjustment of applicable security requirements upon agreement renewal, considering changes to:

    o Institutional Information.

    o IT Resources.

    o Policy.

    o Laws and regulations.

• As appropriate, obtain assurance from a third-party audit report, or other documentation acceptable to HIU, demonstrating that appropriate information security safeguards and controls are in place.

• Follow HIU records retention requirements contained in HIU's Records Management Polices (RMP).

Departments using Vendors must ensure that Vendors do not:

• Share passwords or authentication secrets that provide access to Institutional Information or IT Resources.

• Use passwords or other authentication secrets that are common across customers or multiple unrelated HIU sites.

• Create backdoors or alternate undisclosed access methods for any reason.

• Access systems when not authorized to do so.

• Make unauthorized changes.

• Reduce, remove or turn off any security control without approval from the appropriate Unit Information Security Lead.

• Create new accounts without Unit approval.

• Store, harvest or pass through HIU credentials (username, password, authentication secret or another factor).

• Use or copy Institutional Information for non-authorized purposes.