THIRD PARTY DATA SECURITY REQUIREMENTS

Introduction

The VSC engages in business in which data are being collected, transmitted or stored under contracted third party arrangements. In many of these situations, a web-based system is developed by a third party to collect data on behalf of a VSC operation. The VSC may also send data collected by the VSC for further processing or storage by a contracted third party.

“Third party” is defined as any vendor or entity doing business with or collecting, transmitting or storing data on behalf of the VSC or any of its member colleges. Data can be in electronic or paper formats.

A checklist has been created to assist in risk management, contract review and ongoing third party management, with a goal of minimizing the risk to VSC data.

The individual or office seeking to provide data to a third party must document data elements to be collected, transmitted or stored (e.g., names, addresses, social security numbers, credit card processing, student data, alumni data, etc.).

IT will review VSC security requirements with the technology staff of any new third parties, using the Third Party Review checklist. This review will be completed by OCIT for enterprise contracts, and by the appropriate college IT department in the case of a product used by only that college.

Section III: Contract Development

Any contract with a third party to collect, transmit or store data shall address the following

7.