# Secure Remote Access Policy

## Purpose
The purpose is to ensure the security of BSU enterprise data, users accessing date remotely must adhere to established procedures to safeguard that data.

## Policy Statement
All persons accessing BSU enterprise business systems data from a non-campus location must be authorized to access the data and authorized to work remotely. He or she must then comply with BSU Security standards for secure communications.

## Applies to
All employees and other users that need access to BSU enterprise data.

## Responsibilities
Responsibilities of the Information Technology Division:

- Users will access BSU enterprise data from persistent locations such as a home office or hotel room. Kiosks are not considered persistent locations.

- Users will abide by the BSU Standards for Secure Remote Access.

- Users will complete the Remote Access Authorization Form and send the completed form to: Security Manager, Room #009, Boyden Hall.

- Vendors will abide by the BSU Standards for Vendor Remote Access.

- Information Technology staff must use second level authentication tokens when managing infrastructure resources from off-campus.

---

**Title:** Data Responsibility  
**Approved By:** Patrick Cronin  
**Approved Date:** April 2011  
**Date of Last Revision:** July 30, 2013  
**Policy Category:** Information Technology Division