ITS Vendor Access Policy

COLLEGE POLICY

Policy Title:	**ITS Vendor Access Policy**
Type or category of Policy:	**This is a College Policy**
Approval Authority:	**This policy and any major changes will be approved by the Chief Information Officer (CIO)**
Responsible Executive:	The **Chief Information Officer** is the **Responsible Executive** for this policy.
Responsible Office:	**Responsible Office:** Information Technology Services (ITS)
Owner Contact:	**Questions or Concerns should be addressed to:** Information Security Administrator informationsecurity@siena.edu
Reviewed By:	**Information Security Committee (ISC)**
Reviewed Date:	**10/7/15**
Last Revised and Effective Date of Revision:	**10/7/15**

Reason for Policy

The purpose of this policy is to define standards for vendors accessing resources on Siena College's network. These standards are designed to minimize the potential exposure to Siena College from damages which may result from unauthorized use of Siena College resources. Damages include but not limited to the loss and or breach of sensitive or confidential data, intellectual property, damage to public image, damage to critical Siena College systems.

Scope of the Policy

This policy applies to all Siena College vendors, contractors, subcontractors, volunteers, visitors or agents herein referred to as "third parties" with a Siena College owned or personally owned device used to connect to the Siena College network. This policy applies to any connections used to perform work on behalf of Siena College.

Siena College increasingly continues to depend on the security and integrity of the computer network, servers, and workstations, it is important that the College be proactive in their approach about identifying and enforcing security standards.

The Official Policy

To assist and support Siena College in its mission third parties may need access onsite or via remote to the systems of Siena College for maintenance and/or emergency support. These systems may

cover hardware and/or software management with the ability to view, copy, and make modifications to the systems and data.

It is the responsibility of third parties with access to Siena College resources that due care is ensured to properly secure Siena College systems and at all times, comply with FERPA, GLBA, HIPAA and other applicable federal and state privacy statutes.

The third parties agree that they will protect the Confidential Information they receive according to commercially acceptable standards and no less rigorously than they protects their own Confidential Information. Specifically, third parties shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of all electronically managed Confidential Information.

All parties are subject to all Siena College policies.

The access should be activated on an as-needed basis and disabled when not in use. Third parties access is temporary and shall be reviewed on an annual regular basis if access is required for more than one year.

All third party access to network systems must be approved by the Information Security Officer or designee.

Exceptions

Exceptions can be granted in limited circumstances by the CIO based upon the needs of the College.

Adopted: 10/7/15

Reviewed:

Revised: