

***BGSU Information Technology Policies
Policy and Procedure Definitions***

Appropriately Affiliated Members - those associated with the University through the status of current student, faculty, staff, BGSU retiree, BGSU alumni, active BGSU account holder.

Core Values - The Core Values to which the University adheres include respect for one another, cooperation, intellectual and spiritual growth, creative imaginings, and pride in a job well done.

Executive Steering Committee (ESC) - The BG@100 Executive Steering Committee decides project scope, timelines, priority and has overall responsibility for the success of the BG@100 PeopleSoft project effort.

General Public – Any person not directly affiliated with the Office of the CIO

Information - Data, in all its forms, collected, maintained, accessed, combined, or modified by and for members of the University community.

Information Technology Resource - All aspects associated with management and processing of information. This includes facilities, technologies, and data used for University processing, transfer, storage, and communications. Examples of these resources, include, but are not limited to, computers, networking equipment, telecommunications equipment, electronic mail, electronic information sources, network bandwidth, wireless devices, video communications, IP telephony, University assigned accounts, voice mail, passwords, access controls, storage media, documentation, personal digital assistants.

Network - a configuration of communications equipment and communication links by any wired or wireless means, that enables resources to be geographically separated, while still connected to each other.

PeopleSoft -- PeopleSoft is the company that produces the administrative software application that is being implemented by the BG@100 PeopleSoft project for use as administrative systems at BGSU. The software itself is also referred to as PeopleSoft.

Public Computers – Any computer that is available to the general population. Example of public computers include, but not limited to, airport kiosks, library computers, internet cafes etc.

Reconnaissance – An inspection or exploration to gain knowledge of a network's topology, configuration or components.

Safe Computing – Using information technology in a secure manner consistent with its intended purpose. Examples of security measures to be taken, include, but are not limited to, the use of strong passwords that are not easily guessable, are changed regularly and are kept private; the application of all relevant security patches in a timely manner; maintenance of up-to-date virus definitions; backup and protection of important/critical data; security of passwords; protection of data and files.

Security Controls - Any procedure or technology that mitigates the risk of unauthorized users from accessing information technology resources, including, but not limited to, firewalls, encryption, policies, and passwords.

Sensitive University Data - includes personal information and proprietary information of the University included but not limited to: Social Security numbers, Driver License numbers, credit card or other financial account numbers, BGSU ID numbers, protected health information, financial data, educational records, intellectual property or research records, donor profiles, or any information that could result in a material risk of identity theft, a violation of the Family Educational Rights and Privacy Act, or otherwise harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally.

Technology - a method or methodology that applies technical knowledge or tools.

Unlicensed spectrum space - Unlicensed spectrum includes the FCC unlicensed 2.4 Ghz Industrial/Scientific/Medical (ISM) band and the 5.1 Ghz Unlicensed National Information Infrastructure (UNII) band.

User - A user is any person, either authorized or unauthorized, who utilizes information technology resources from any location.

Virtual Private Network (VPN) – a “tunnel” connection created to allow secure communications over public networks.

Vulnerability Scanning – The process of proactively identifying vulnerabilities of computing resources in a network in order to determine if and where a resource can be exploited and/or threatened.