

BGSU PEOPLESOFT ACCOUNT ADMINISTRATION

Applicability	All BGSU stakeholders
Last Revised	December 14, 2007
Policy Owner	Office of the Chief Information Officer (CIO) cio@bgsu.edu
Governing Body	N/A

Number	IT – xx - xx
--------	--------------

INTRODUCTION

Bowling Green State University (BGSU) Information Technology Services (ITS) within the Office of the CIO will establish and follow detailed processes to activate and deactivate PeopleSoft application accounts and to grant access privileges.

POLICY**Standards:**

- The computer and communication system privileges of all users, systems, and programs must be restricted based on the principle of least privilege. A user, system, or program should have access only to the resources that are necessary to perform daily tasks.
- Key system resources and utilities, as well as privileged user IDs must be strictly limited to those individuals who must have such privileges for authorized business purposes.
 - For example: only security administrators will have a privileged user ID that allows them to change user access
- Access roles must be created in such a way as to enforce segregation of duties
 - For Example: A role can not be created that allows someone to approve the creation of an account and actually create the account as well
- All user accounts and roles will be administered by ITS Security Personnel. Access to user accounts and roles will only be granted through the documented approval process.
 - See HCM Security Flowchart and Narrative & FMS Security Flowchart and Narrative documents
- Exceptions to this policy must be approved by:
 - Chief Information Officer

Guidelines:

- ITS will make a reasonable effort to ensure that deployed solutions support the following password rules:
 - Passwords must be 6 to 8 characters in length.
 - Passwords must begin with an alphabetic character.
 - Passwords must contain at least one lowercase letter.
 - Passwords must contain at least one uppercase (capital) letter.
 - Passwords must contain at least one of the following characters:
 - ! (exclamation point)
 - . (period)
 - , (comma)
 - \$ (dollar sign)
 - % (percent sign)
 - ? (question mark)
 - * (asterisk)
 - # (pound sign)
 - < ("less than" sign)
 - > ("greater than" sign)
 - ((left parenthesis)
 -) (right parenthesis)
 - Passwords must **not** contain any of the following characters:
 - ; (semicolon)
 - : (colon)
 - ' (quote)
 - " (double quote)
 - - (dash)
 - / (slash)
 - \ (backslash)
 - @ ("at" sign)
 - Accounts should be locked out after 3 unsuccessful login attempts. The account should stay locked out until it is reset by an ITS Security Analyst. Users should be automatically logged off after 60 minutes of inactivity.

ADDITIONAL INFORMATION

Once printed, this policy may be outdated. The official policy can be found at <http://www.bgsu.edu/offices/cio/page32228.html>.