OnBase Policy

I. Introduction

OnBase is the enterprise imaging and electronic document retrieval solution that the college utilizes to archive large amounts of data that the College is required to maintain.

This policy will provide a framework for OnBase administration, support, security and further development. As with all enterprise software applications, Information Resources will administer the server, implement approved modules/features and provide application support.

II. OnBase Advisory Committee

The OnBase Advisory Committee is responsible for the providing strategic direction for OnBase including: expanding licensing for additional campus departments to use OnBase and adding modules/features to the college OnBase solution, and ensuring adherence to this OnBase Policy.

III. Security

A. Content **-** Sensitive Electronic Information (SEI) requires responsible management by all members of the SUNY Cortland community.

i. SEI shall be categorized as follows:
  a. Public (information that can be shared) - Minimal risk
  b. Cortland Confidential (sensitive data as determined by the OnBase Advisory Group)- Medium to high risk
  c. Regulated (information protected by regulatory compliance) - High risk

ii. All SEI shall be regulated by all SUNY Cortland Personally Identifiable Information Security Policies and all federal and state regulations and compliances such as: FERPA, HIPPA, GLB, PCI, FOIA, FOIL

iii. Regulated Content - all of these items must be redacted within OnBase unless a written exception is granted by the college Cyber-Security Officer. The Cyber-Security Officer will review audit reports to ensure proper security and access.
  a. Social Security numbers
  b. Credit and Debit Card numbers
  c. Drivers license number or state ID card number
  d. Bank account numbers
  e. Passport numbers
  f. Insurance policy numbers
  g. Protected health information covered under HIPPA

iv. Cortland Confidential Content – this content has been determined by the college to be sensitive in nature. The Cyber-Security Officer will review audit reports to ensure proper security and access. Improper handling of this content may result in user account closure.
  a. Digital or electronic copies of a personal handwritten signature
  b. Sensitive Donor information

B. Data Retention – OnBase content will abide by all SUNY and SUNY Cortland document retention policies. Departments will work with the SUNY Cortland Data Retention Officer to develop a schedule and purge content in compliance with these policies.

C. User accounts

i. New account requests
   a. Each individual accessing OnBase must have their own user account. Sharing an account is strictly prohibited and may result in account closure and access denial.
   b. Unit Liaisons may submit user account requests through the Information Resources Support Center.
   c. Unit Liaisons must identify the appropriate level of access and privileges being requested for each individual user. Access to Regulated and/or Cortland Confidential content must be approved in writing by the department head as well as the college Cyber-Security Officer.

ii. User Code of Conduct - Before being granted access to OnBase, users must agree to abide by the security regulations outlined below:
   a. Users will not share their account access or password with anyone.
   b. Users will access information appropriate to their responsibilities.
   c. Users will exercise caution when printing, copying or emailing any Regulated or Cortland Confidential content from OnBase.
   d. Users with access to Regulated and/or Cortland Confidential content will comply with all applicable federal and state laws in appropriate handling of information.

IV. License expansion for new campus departments

Campus departments may request access to OnBase by writing to the Chair of the OnBase Advisory Committee. Requesting departments should include a brief description of their needs. The Chair may arrange for a meeting with the requesting department with the OnBase System Administrator and the OnBase Coordinator to gather more information. Once all information is complete, the Chair will provide the OnBase Advisory Committee with the requesting department's information.

The OnBase Advisory Committee will then approve or decline the request. Should the Committee decline the request, the Committee will provide the requestor with a written response detailing the decision. Approved requests will be forwarded by the Committee to Information Resources to begin OnBase client training and implementation.

V. Development/Acquisition of new modules

The OnBase Advisory Committee is responsible for planning the development of the college OnBase solution. OnBase users may request additional OnBase features/functions/modules by writing to the Chair of the OnBase Advisory Committee. Requests should include a brief description of the requested feature/function/module and why it is needed. The Chair will ask the OnBase Administrator to develop a scope of work and determine the cost of the project. This information will be shared with the OnBase Advisory Committee. The OnBase Advisory Committee will also review the ongoing budget implications of the new feature/function/module. The Committee may invite the user to present the request in person.

The OnBase Advisory Committee will approve or decline the request. Approved requests will be forwarded to the OnBase Administrator for acquisition and implementation. The Committee will provide written explanation for declined requests.

VI. Support

A. Scanners and other peripherals

Campus Technology Services, in consultation with the OnBase Coordinator, will work with campus departments concerning their needs for a new or replacement scanner or other peripheral. Campus Technology Services shall place all orders for this equipment on the behalf of the campus department. Campus departments will bear the cost of their own scanners and peripherals.

Campus Technology Services shall install, provide basic troubleshooting, and assist users in obtaining repair of defective scanners and peripherals. Campus departments will bear the cost of repairs and or replacements.

Campus departments may purchase a third-party maintenance agreement for high-end scanners. Departments will work with the OnBase Coordinator to arrange maintenance arrangements with the third-party vendor. The Unit Liaison will report maintenance problems directly to the third-party vendor. Should the scanner need to be replaced, the Unit Liaison will receive the replacement scanner and work with the OnBase Coordinator to replace the hardware. Campus departments shall bear the full cost of the maintenance agreement and coordination for obtaining vendor purchased support.

B. OnBase Application

i. User responsibilities-

a. Users may view or add to existing OnBase records. User access and privileges is defined in accordance with their authorized activities.
b. User escalates to the Unit Liaison should any problems or issues arise. If Unit liaison is unavailable, they may contact the Information Resources Support Center.

ii. Unit Liaison responsibilities -

a. Unit Liaisons are considered the "go-to" persons for their departments. When the OnBase Coordinator sets up an initial discussion with a department, a Unit Liaison is identified.
b. He/She is trained and functions as a liaison with OnBase Coordinator for their department - to include providing support to the end-user, understanding the roles in accordance with their authorized activities.
c. He/She is involved with any testing that may take place in the test environment before roll-out takes place into production.

iii. OnBase Coordinator responsibilities-

a. Serve on planning and implementation team with OnBase System Administrator when there is a plan for new roll-out and upgrades of OnBase to desktops on campus departments as defined by the OnBase Steering Committee
b. Installation of client on user systems as part of the Technical Help Center team; Creation of User Groups; Access to Document types; Access to User Groups; and password resets
c. Coordinate with PC Services desktop for scanner and installation of software that is used with scanner. Coordinate maintenance of scanners and provide additional minor maintenance on scanners (such as changing rollers, cleaning, scanning) on an as-needed basis. Participate in user group and On-base Training to stay abreast of software changes and upgrades.
d. Work with the Onbase Administrator and Administrative Computing to ensure end-user security access and issues
e. Together with the OnBase Administrator define OnBase hardware/software client standards
f. In tangent with area Unit Liaisons, this individual will be responsible for the evaluation of computer systems to ensure appropriate level of computing power;

iv. OnBase Administrator responsibilities-

a. Project Lead for planning and implementing OnBase upgrades and installation of new modules as approved by the OnBase Steering Committee.
b. Assure that all state, federal, and local security regulations and guidelines are being followed in consultation with the ISO and/or Deputy ISO

c. Together with the OnBase Administrator Coordinator define OnBase hardware/software client standards
d. Assure that OnBase server is professionally maintained, assuring that the server is scaled properly, OS levels are maintained, security and critical updates are up-to-date, and provide the steering committee with future strategic planning recommendations.

Last revision: 11/2010