RIT Information & Technology Services

OnBase Account Request Form

Please return this form to the ITS Service Desk in the Frank E. Gannett Building, room 1113, or fax it to 475-7884
Questions? Call us at 475-4357 (voice) or 475-2810 (tty)

Section I - Required Information (Please Print)

Name: _____ (First) _____ (MI) _____ (Last)

UID: _____ **RIT Username:** _____ **Phone:** _____

Department: _____ **Department Number:** _____

Section II - License Information

Note: If new licenses are required for this user, please complete Section V (License Order) on page 2 of this form

User Action:
- ◯ Add New User
- ◯ Delete User
- ◯ Modify User

Licenses Needed:
- ◯ Client
- ◯ Client and Workflow

License Assignment:
- ☐ Buy New Licenses
- ☐ Use Unassigned Department License, if Available
- ☐ Use Existing Concurrent/Workstation License
- ☐ Transfer License(s) from: _____

Section III - Access Requested

Approval from the ITS Application Administration team required for the roles noted below with an asterisk (*)

OnBase User Role:
- ◯ Office Leader
- ◯ Office Staff
- ◯ Student Worker
- ◯ Access Approver *
- ◯ ITS Administrator *

Functional Area(s):
- ☐ Admissions - Graduate
- ☐ Admissions - NTID
- ☐ Admissions - Undergraduate
- ☐ Controller's Office
- ☐ Disability Services Office
- ☐ English Language Center
- ☐ Financial Aid
- ☐ Human Resources
- ☐ International Student Services
- ☐ Student Conduct Office
- ☐ Student Employment Office
- ☐ Student Financial Services
- ☐ Student Records
- ☐ System Documents

Other (Describe): _____

Other Modules / Rights:
- ☐ Virtual Print Driver

Subscription Server:
Select the offices to which you will be emailing files
- ☐ Admissions (All)
- ☐ English Language Center
- ☐ Int'l Student Services
- ☐ Other (Describe): _____

Section IV - Authorization

I have read both the FERPA Governance Policy and the OnBase Usage Policy included with this form. I acknowledge that a violation of either policy may result in action up to, and including termination of my employment.

_____ *Print Name of Requestor* _____ *Requestor's Signature* _____ *Date*

I approve this request, the assignment of the above privileges, as well as any necessary charges to the above request.

_____ *Department Head* _____ *Department Head's Signature* _____ *Date*

RIT
Information &
Technology Services

OnBase Account Request Form

Please return this form to the ITS Service Desk in the Frank E. Gannett Building, room 1113, or fax it to 475-7884
Questions? Call us at 475-4357 (voice) or 475-2810 (tty)

Section V - License Order

Note: This section is optional, and only necessary if additional licenses are needed for this user, or for other anticipated new users. When submitting multiple OnBase Account Request Forms for multiple users at the same time, you can either complete this section on each of the Account Request forms, or simply complete this section on one form, and include the total number of licenses required for all users.

Order Process

After this OnBase Account Request Form is submitted, the following will take place:

1. ITS will proceed with creating the user's account and soliciting approvals for the desired Functional Area(s)
2. At the same time, ITS will reach out to Hyland Software, the OnBase vendor, and request a quote for the license(s) requested below (along with any additional licenses requested by the department)
3. Once ITS receives the quote, it will be forwarded on to the department, who will approve the charges
4. Upon approval, ITS will process the quote, import the license(s), and perform an internal chargeback to the department for the licenses.

License Descriptions

Client Licenses: Allow users to log into the OnBase system and utilize document retrieval and basic import functions, depending on their permissions in the system. All users require some type of client license to log in. Client licenses can be:

- Workstation: Allows any user to log into the OnBase Client from a designated workstation. Note that Workstation licenses do not allow access to the OnBase Web Client
- Named User: Allows a designated user to log into any OnBase client (including the web client) from any workstation. Named User licenses allow the user to have up to two active sessions at one time.
- Concurrent: Allows any authorized user to log into any OnBase client (including the web client) from any workstation, as long as the license is available.

Workflow Licenses: Allow users to access the Workflow system and perform actions on documents in any lifecycle and queue which they have access to. In order to access workflow, a user must have BOTH a Workflow license and a Client license. Workflow licenses are available in the same types as Client licenses (workstation, named user, and concurrent).

Document Imaging: Allows a dedicated workstation to scan using a high-volume scanner via the "Batch Scanning" interface. Note that a Document Imaging license is only available as a Workstation license, and also comes bundled with a Workstation Client license, to be assigned to the scanning station.

Client Licenses	**Workflow Licenses**	**Document Imaging Licenses**
_____ Workstation	_____ Workstation	_____ Workstation
_____ Named User	_____ Named User	
_____ Concurrent	_____ Concurrent	

Account Number: Please indicate the account number which should be charged for the new license(s).

_____

RIT Information & Technology Services

OnBase Account Request Form

Please return this form to the ITS Service Desk in the Frank E. Gannett Building, room 1113, or fax it to 475-7884
Questions? Call us at 475-4357 (voice) or 475-2810 (tty)

Instructions:

Section I - Required Information
Fill out all required information for the user requesting the OnBase account.

The RIT username you enter must match the username that you log into RIT services with (such as FootPrints, People-Soft, MyRIT, etc).

Section II - License Information
User Action: Choose whether the request is to add a new user, or modify or delete an existing account.

Licenses Needed: All users require a client license. If your department also uses the Workflow system, you will also need a Workflow license.

License Assignment:
[Buy New Licenses] - if you department needs more licenses, check this box, and Section V (License Order) of this form.

[Use Unassigned License, if Available] - if your department has an unassigned license, it will be assigned to this new user.

[Use Existing Concurrent/Workstation license] - check this box if your dpeartment has concurrent licenses, or shared workstations which the user will also use.

[Transfer License] - if you have an existing user that you want to move an existing license from, check this box and enter their username here.

Section III - Access Requested
OnBase User Role: select the role for the user, based on the role descriptions on page 3, below.

Functional Areas: select the areas containing the documents you are requesting access to. These offices will then be solicited for approval and appropriate access.

Other Modules/Rights: if you require access to any special functions or modules, indicate them here:

[Virtual Print Driver] - Allows documents to be imported from any application directly into OnBase. Your department must participate in this module's shared chargeback in order for you to be given access to this module.

[Subscription Server] - Allows emails and their associated attachements to be imported into OnBase.

Section IV - Authorization
Account creations and access modifications require both the requestor's signature and the signature of their Department Head. Deletions of an existing account/user only require the signature of the Department Head.

Section V - License Order
Complete this section if additional licenses are required for the new user, or if you anticipate additional licenses being required for additional users in the future.

RIT
Information &
Technology Services

OnBase Account Request Form

Please return this form to the ITS Service Desk in the
Frank E. Gannett Building, room 1113, or fax it to 475-7884
Questions? Call us at 475-4357 (voice) or 475-2810 (tty)

OnBase User Role Descriptions

Office Leader: This role allows all basic client functions, in addition to being able to purge committed scanned batches. This role is also being set up to allow additional administrative-type functionality, coming in future versions of OnBase.

Office Staff: This is the standard OnBase role, granting access to all basic functions in the system, such as scanning and indexing. *Unless otherwise necessary, staff members should be placed in this role.*

Student Worker: This is the standard role for student workers in OnBase, allowing for most client functionality, including Workflow and scanning and indexing. *Unless otherwise necessary, student workers should be placed in this role*

Access Approver: This role includes the functions in the Office Leader role, in addition to a few other administrative functions within the client. Users in this role are permitted to reject or deny access requests and change requests for their office.

ITS Administrator: This role is limited to selected ITS and system administrators, and allows full system, configuration, and maintenance access to the system.

RIT
Information &
Technology Services

FERPA Governance Policy

Student records are confidential, protected under federal law known as the Family education Rights and Privacy Act (FERPA). Under FERPA you may access the information within the OnBase system only in the legitimate education interest of the student. You must keep all information confidential. You are given access to this system and its documents on the condition that you do not share your access (including User ID and/or password) with others, as you will be held responsible for changes made using your User ID and password.

RIT Information & Technology Services

OnBase Usage Policy

I. Introduction

Document management and storage are vital components to the success of the University. Documents must be made readily available to those individuals who need them, at any given moment, and without difficulty. To facilitate this function, the Enterprise Content Management (ECM) solution OnBase, by Hyland Software, is used within various business units throughout Rochester Institute of Technology (RIT).

Because of the nature of the documents being stored within the OnBase system, special care and attention must be taken in order to ensure privacy, and business continuity. An outage, for any reason and for any duration of time, can lead to a severe impact on business processes. As such, it is vital that all users, at all levels, help to ensure the integrity and security of the OnBase system and the data and documents stored within it.

II. Definitions

To avoid confusion and question, the following terminology will be used throughout this policy:

A. **User:** Any individual, whether internal or external to the institute, who is authorized to use the OnBase system in any capacity.
B. **Functional Group:** A single, contiguous business unit (for example, Admissions) whose staff utilizes the OnBase system.
C. **Functional Administrator:** A user within each functional group who is authorized to manage his or her group's users and their security settings, and their interactions with the OnBase system. Currently, there are four Functional Administrators from the Registrar, Admissions, Financial Aid, and NTID offices.
D. **Support Staff:** Any individual, whether internal or external to the institute, whose role is supporting and/or troubleshooting the OnBase system in any capacity.
E. **HSI:** Acronym used to denote Hyland Software, Inc., the vendor and developer of the OnBase application.
F. **PI:** Private Information, which New York State defines as any personal information concerning a natural person combined with one or more of the following data elements: Social Security number, driver's license number, account number, or credit or debit card number in combination with any required security code.[1]
G. **The System:** Refers to any aspect of the OnBase system, including (but not limited to) the Thick (Windows) Client and the Thin (Web) Client.

1 http://security.rit.edu/Pim-table.html

III. Scope

This policy shall be binding to any and all users, internal or external to the institute, who access any component of the On-Base system, in any capacity. This includes, but is not limited to, RIT faculty and staff working both within the institution, and from remote locations; Information and Technology Services (ITS) and other internal support staff; and support from vendors, including HSI.

This policy implies those supplemental policies and regulations in effect throughout the University. These include, but are not limited to, the University's policies and guidelines on privacy, intellectual property, data handling and Private Information, prohibition of harassment and discrimination, as well as the Code of Conduct for Computer and Network Use.

IV. OnBase Policies

A. Protected Information and Data Security

Data and documents contained within the System contain a significant amount of data about students at the University. As such, the System, as any other student management system on campus, is subject to the regulations of FERPA (the Family Education Rights and Privacy Act). Under FERPA, you may access the information contained within the system only for legitimate purposes and only in the interest of the student.

Additionally, Users must make a reasonable effort to ensure that PI data is scrubbed, where appropriate, from any document before it enters the system. For PI data that is encountered throughout the course of the User's interaction with the System, the User is responsible for executing appropriate PI handling procedures, as defined by their Functional Administrator.

Where appropriate, Users are responsible for ensuring the continuity and security of all data that comes into the system. This includes, but is not limited to, AutoFill data feeds, scanned documents, and documents imported through the "Virtual Print Driver" functionality.

B. User Security

Each User is issued a User ID by their Functional Administrator. It is the responsibility of the User to keep their User ID secure. This information, in addition to any password or cryptographic string, must not be shared with anyone, for any reason. To ensure the security of the User's workstation and the data within the System, Users must make reasonable efforts to utilize built-in security functions in the application and their workstation, including, but not limited to the "Lock Workstation" functionality. These steps must be taken any time the User is away from their workstation for any period of time.

Passwords and other cryptographic strings must not be stored in plain-text anywhere in the application, on the User's workstation, or in plain-sight on the User's work area. Passwords and other cryptographic strings must meet, and will be enforced by, a set of criteria to ensure the utmost security. The criteria will be determined by the User's role and Functional Group, and will, at minimum, meet the RIT Password Standard.

C. Document Sharing

The System includes a number of built-in functions which allow Users to share documents with other, or with other authorized members of the University. These functions include, but are not limited to, Internal Mail and Printing. It is the responsibility of the User to ensure that any document(s) shared using these functions is protected and handled correctly, in accordance with the University's policies on data handling and Private Information. The User is responsible for ensuring the security of the document(s) until ownership is formally transferred over to the intended recipient.

V. User Responsibilities

In addition to the responsibilities listed above in Section IV, Users are responsible for acknowledging that they have read and agree to this Policy. The User's acceptance will be collected at the time that they are initially brought into the System, and each time they log into the application. The User's acceptance, in any form (ex. signing a paper or clicking an "Accept" or "I Accept" button) indicates that they understand this policy and agree to be bound by its terms.

The User also understands that their access to the System is at-will, and controlled by their Functional Administrator. At any time, and for any reason, the Functional Administrator may alter the User's access, update information about the User, or suspend or revoke the User's access to the System. The User also understands that most actions performed within the System are tracked in an audit history, and may be referred to at any time, and for any reason.

The User further understands that they have the responsibility for bringing to the attention of their Functional Administrator any infraction of this Policy that he or she observes. Should the User's immediate Functional Administrator be unreachable, the User shall contact another Functional Administrator, or ITS. Failure to report a violation of this Policy may result in actions being taken according to Section 6, Enforcement.

VI. Enforcement

This policy is a binding contract between the User, their Function Administrator, applicable Support Staff, and the University. Violations of this Policy shall be handled by the User's immediate Functional Administrator, and many include suspension or termination of access to the System, degradation of User access, written or verbal warnings, and other actions as deemed appropriate, up to, and including termination of employment.

VII. Questions and Interpretation

Questions about this policy and its implications should be brought to the User's immediate Functional Administrator. In instances where the Functional Administrator is unable to determine the interpretation of User's question, he or she will bring the issue to other appropriate individuals, including other Functional Administrators and University Administration.

VIII. History

Revision #	Revision Date	Revision Author	Notes
0.1	January 21, 2011	Michael Bruckner	Initial Policy
0.2	January 25, 2011	Michael Bruckner	Updates from first draft sweep