

# OnBase Access Request Form

Lucas County Information Services  
 One Govt. Center, Suite 400 Toledo, OH 43604  
 Phone: 419-213-4037

Instructions: Complete sections and forward to LCIShelpdesk@co.lucas.oh.us (One Government Center Suite 400).

Section 1: User Information				
Select one:	<input type="checkbox"/> New User	<input type="checkbox"/> Delete user	<input type="checkbox"/> Modify User (Change Existing Access)	<input type="checkbox"/> Add Permission (Retain Existing Access)
First Name:	MI:		Last Name:	
Department:	Address:			
Phone:	Email:			
If modeling access after a current employee - enter the employees name here:				

Section 2: OnBase Information				<i>Check all that apply</i>			
AGENCY	Admin	Scan	View/ Print	AGENCY	Admin	Scan	View/ Print
Auditor Finance				Dog Warden			
Auditor Real Estate				Imaging Lab			
Auditor REA Finance				Juvenile Court			
Board of Health				Juvenile Court / JFS			
Board of Health Admin				Juvenile Court Fiscal			
Building Regulation				Juvenile Court Legal			
Clerk of Court				Juvenile Court Prosecutor			
Clerk of Court Backfile				LC Commissioners			
Clerk of Court Appellate				LC Information Services			
Clerk of Court Online Docket				Risk Management			
County Engineer				Sanitary Engineers			
Court Services				Victim Witness			
Domestic Relations							

**Notes/Business Purpose:**

Section 3: Signature	
Check here to indicate that you have read and understand the attached OnBase User Access Policy	
Employee Signature:	Date:
<p>A user account will not be created or modified without the Director/Supervisor signature(s). Please allow up to one week for the changes to take effect. Expedited requests will be handled on a case-by-case basis. The signing Director/Supervisor acknowledges that OnBase license usage for new users may result in an increased charge to your department. For information on department charges contact LCIS at 419-213-4025.</p>	
Check here to indicate that you have read and understand the attached OnBase User Access Policy	
Director/Supervisor Name Printed:	Phone:
Director/Supervisor Signature:	Date:
<b>Note:</b> Employees that request access to another agencies documents within OnBase are required to obtain appropriate signatures from the other agencies Director/Supervisor.	
Other Director/Supervisor Name Printed:	Phone:
Other Director/Supervisor Signature:	Date:

## **OnBase User Account Access Policy**

**Access Approval:** System access will not be granted to any user without appropriate approval of a Director or Supervisor. Users granted access to the OnBase systems must be issued a unique OnBase account user ID; in most cases, the user ID is the same Novell user account, and will work as a single sign on. Management is to immediately notify the LCIS Help Desk and report all significant changes in end-user duties or employment status. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job. A signature on the OnBase Access Request form indicates the Director/Supervisor understands and agrees to abide by these policies and procedures for access to the OnBase system, and is accountable for the employees and/or users they grant access to the OnBase system.

**Personal Identifiable Information (PII):** Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g. a social security number, name, age, date and place of birth, mother's maiden name, marital status, race, salary and employment information, home phone numbers; other demographic, biometric, personnel, medical, financial information; law enforcement information; and educational information.

**Need-to-Know:** In the OnBase System, owners of data with personal identifiable data, will only grant access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required to perform their job.

**Audit Trails and Logging:** The OnBase System access will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access
- Documents accessed