Request for Access to IT Resources

- This form is required to formally request any type of departmental access to another user’s OHIO accounts or systems. Any request for access must strictly be due to operational need, continuity of business, or departmental contracts and will be granted for a limited time. Access may be revoked or denied at any time by OIT or Human Resources.
- Access to IT Resources is limited to viewing of work product for bona fide business purposes. Those granted access shall refrain from viewing personal and/or confidential information belonging to the user. Moreover, under no circumstances, does this access grant permission to act on behalf of or in the name of the user.
- Should access reveal inappropriate or illegal material, the Information Security Office shall be contacted immediately at security@ohio.edu or 740-566-7233 (SAFE).

SUBMIT COMPLETED FORM TO YOUR AREA’S HR LIAISON, WHO WILL APPROVE OR DENY THE REQUEST FOR ACCESS.

CLICK HERE FOR LIAISON LIST

Requestor (Who is making the request?):
Name: ___________________________  Email: ___________@ohio.edu  Phone: (740)____ - ________

Title / Planning Unit / Department: _______________________________________________________

Request Details:
What access, data, or change is being requested?
(Example: Access to Ex-employee’s email account, copy of files on a computer, set an email vacation message)

Who should be granted access? (Name and OHIO ID)

What type of access is needed?  □  Read only  □  Other: _________________________________

Why is access essential to business operations?

How long is access needed?  □  10 days  □  20 days  □  30 days (Access beyond 30 days requires new request)

HR LIAISON USE ONLY

Approved:  □  Yes  □  No  Access Expiration: ________________________ (Date)

Date completed form scanned and sent to OIT Security (security@ohio.edu) ________________

Comments:

Signature of HR Liaison  Date

OHIO email address  Phone

By signing and approving the above request, I hereby attest I have thoroughly reviewed the detailed request and I verify the business necessity for the access requested. Further, I confirm that the individual(s) granted access have an operational need to do so and are the most appropriate individual(s) to have access.