



1. INTRODUCTION

The University of Notre Dame provides information technology resources to employees, students, affiliates, and student groups for activities related to its mission of teaching and learning, research, and service. The University has an interest in conserving resources and permitting secure access to only those individuals and entities who are actively involved in supporting the institution's mission and goals.

The NetID is a unique and permanent electronic identifier issued to members of the Notre Dame community. In combination with a password, the NetID is the primary authentication mechanism at the University. Possession of a NetID should not, in and of itself, authorize its owner to do, or have access to, any specific service.

2. POLICY STATEMENT

The University of Notre Dame enables access to University-owned information technology resources by issuing NetIDs to members of the Notre Dame community, persons affiliated with the University, and external consultants under contract. An individual will normally be assigned one individual NetID, and it will never be reassigned or transferred to another individual.

Individual Identities eligibility

1. Active Regular and non-regular faculty;
2. Postdoctoral scholars ("post-docs");
3. Active Full-time, part-time and temporary on-call staff;
4. Currently enrolled students, and prospective students who are admitted and confirmed;
5. Retired faculty and staff;
6. Members of the Congregation of Holy Cross who are directly engaged with the University;
7. International personnel who staff Notre Dame's Global Gateways
8. Persons associated with external entities that collaborate with the University may be eligible for affiliate access with appropriate sponsorship. This includes consultants and employees or members of specific institutions or programs associated with the University.

Unless they also belong to one of the foregoing groups, alumni of the University are not eligible for NetIDs.

Registered student organizations may obtain a NetID by working through the Student Activities Office and completing the appropriate form.

The University will determine the level of *authorized* access, based on role, status or other criteria. Scope of NetID access varies with the affiliation, and may change. The Chief Information Officer, or their delegate, is responsible for periodic reviews. Responsible University officials will reevaluate their sponsored affiliates annually to ensure that they remain eligible.

The Chief Information Officer can revoke NetID privileges at their discretion.

Activation and Deactivation

NetIDs are created automatically after Faculty, Staff, Students, and Affiliates are entered into the ERP system and have an active role assigned to the record. NetID accounts that no longer have an active role will be disabled.

Retention of affiliated data

Documents and data will be permanently deleted one year after an account is disabled, unless the Office of General Counsel places a legal hold on those documents or for any other reason at the University's sole discretion.

3. SCOPE

This Policy applies to all users of information technology resources owned and provided by the University of Notre Dame. In particular, individuals or departments of the University who are in a position to authorize access to University-owned information technology resources should familiarize themselves with this Policy.

4. TABLE OF CONTENTS

1. INTRODUCTION	1
2. POLICY STATEMENT	1
3. SCOPE	2
4. TABLE OF CONTENTS.....	2
5. DEFINITIONS.....	2
6. RESPONSIBILITIES	3
7. PROCEDURAL GUIDELINES	3
7.1. Faculty and Staff Access.....	3
7.2. Students' Access	4
7.3. Retirees' Access.....	4
7.4. Other Affiliates' Access.....	4
7.5. Student Groups.....	4
7.6. Immediate Suspension	5
8. POLICY ENFORCEMENT.....	5
9. REFERENCE DOCUMENTS.....	5
10. CONTACTS	6

5. DEFINITIONS

Account	The credentials to access services or resources available on University computer(s) or network(s).
Access Suspension	When an individual's access to ALL services requiring a NetID and password are suspended and the owner is denied access to the account. Essentially, the account is disabled (see definition below).

Administrative Systems	Enterprise software applications used in the operation of the University's business functions, such as human resources, payroll, financial management, business operations, and procurement.
Affiliation	An individual's or entity's relationship to the University. Primary affiliates are faculty, staff, and students.
Authenticate	Verify that an individual is who he/she claims to be, often by use of a NetID and password.
Authorize	Verify that a specific individual is allowed to access specific computing resource(s) or service(s).
Data Steward	An individual who is responsible for ensuring the accuracy, integrity, and confidentiality of University data. A data steward defines access to and restrictions on use of the data for which he or she is responsible.
Disable	Remove all access by the account holder, while keeping the resources intact. Authentication is disabled; the account holder cannot log in to any services or resources. However, a disabled account may (for example) continue to receive email sent to it. The time period an account is disabled may vary depending on policy for each type of affiliation.
Faculty	Regular and Non-Regular Faculty as defined in the Academic Articles
Grace Period	A designated period of time after employment or affiliation ceases, during which user and/or departmental access to all resources persists. The time period may vary depending on policy for each type of affiliation. During the grace period, the University sends email reminding the account holder of impending loss of access.
Inactive	An inactive account is no longer accessible by any user for any purpose, including directory entry or receipt of email, although the associated information technology resources may be intact.
Information Technology Resources	Defined as, but not limited to, applications, computer systems, servers, storage media, networks and related devices owned by or entrusted to the University.
ndID	A unique number assigned to faculty, staff and students, displayed on Notre Dame ID cards.
NetID	A unique identifier that, used with a password, provides access to technology resources.
Affiliate	An individual who is not faculty, staff, or student, but for purposes of eligibility has an affiliated status with the University. Examples may include, but are not limited to:

1. Retired faculty and staff
2. Some members of the Congregation of Holy Cross
3. Consultant retained under contract with the University.
4. Employee of an institution or program affiliated or collaborating with the University.

Information can be found here: https://nd.service-now.com/nd_portal?id=kb_article&sys_id=d9416d96878c79506cc90fa40cbb35a8

6. RESPONSIBILITIES

Business Managers	1. Complete and submit appropriate forms to Data Steward to obtain approval for faculty and staff to access administrative systems.
Data Stewards	1. Review and approve the application for administrative systems access, and notify the OIT.
Administrative Department Head/Dean	<ol style="list-style-type: none"> 1. Authorize access to technology resources for affiliates. 2. Annually review the need for affiliate access.
Office of Human Resources	1. Approves access to administrative systems for staff.
Office of the Provost	1. Approves access to administrative systems for faculty.
Office of the Registrar	<ol style="list-style-type: none"> 1. Approves account creation for students, in conjunction with the appropriate admissions offices. 2. Authorizes disabling accounts of confirmed, admitted students who do not register for classes.
OIT	<ol style="list-style-type: none"> 1. Enables and activates accounts. 2. Disables and inactivates accounts. 3. Acts on authorized requests to enable/disable accounts. 4. Deletes accounts and all associated user documents from University storage media.
Sponsors	<ol style="list-style-type: none"> 1. Complete and submit an Affiliate NetID Request Form to request access to technology resources for affiliates. 2. Annually review the need for affiliate access.

7. PROCEDURAL GUIDELINES

7.1. Faculty and Staff Access

1. Regular and other faculty, post-docs, full-time, part-time and temporary/on-call staff are eligible to use technology resources until the termination of their employment or appointment with the University. Eligibility is based on information supplied by the Office of Human Resources or the Office of the Provost.
2. Continued eligibility is automatic and is based on official university records. Campus units are responsible for ensuring that official university personnel records reflect new hires, terminated personnel, and changes in personnel status or position.
3. All employees are expected to adhere to the normative separation processes outlined within the

[Office of Human Resources Separation Checklist](#) regarding how to remove and/or transfer ownership of collaborative content. [Preparing to Leave Notre Dame for Faculty and Staff](#) enlists actions for a range of applications to ensure smooth handover of business data to coworkers, departments and other stakeholders.

4. Managers and departments are provided a grace period of 60 days following the disabling of a NetID account to recover or transfer ownership of files left behind by an employee. More information can be found here: [NetID: Access to another account](#).

7.2. Students' Access

1. Undergraduate, graduate, and non-degree students are eligible to use information technology resources while they are in active status. Eligibility is based on information supplied by the University Registrar.
2. New students receive an email from their admitting office with instructions on how to activate their account. As part of the process, they are required to read and agree to the Responsible Use of Information Technology Resources policy.
3. Continued eligibility is automatic for active students, and active status is based on official University records.
4. The University disables access to a student's account following a 60 day grace period after he/she has graduated, or 30 days after official university records indicate the student is no longer eligible.

7.3. Retirees' Access

1. Retirees may continue to use electronic resources as provided in the [University's retirement eligibility documents](#) and the Academic Articles.
2. While all retirees will retain their NetID account, they should still adhere to the normative separation processes by removing personal content and transferring ownership of business-related content prior to their departure.

7.4. Other Affiliates' Access

1. Congregation of Holy Cross member accounts are requested by, or on behalf of, the Religious Superior of the Holy Cross Priests and Brother of Notre Dame through the Affiliate Access Request form.
2. Persons associated with external entities that collaborate with the University may be eligible to use technology resources for the duration of their contract with justification of need from the relevant campus unit sponsor. The sponsor submits the request to add an affiliate account by completing the Affiliate Access Request form. The sponsor is required to provide a secondary contact as back-up sponsor should the primary sponsor leave or change roles at the University during the affiliate's access period. Annually, the campus unit must review and reauthorize the affiliate's access. More information can be found here: [Affiliate Access Request](#). The campus unit sponsor must immediately submit a [Suspend Access Form](#) should the affiliate's role with the University end prior to the account expiration initially requested.

7.5. Student Groups

1. The Student Activities Office approves and processes request for NetIDs for registered student groups: More information can be found here: https://nd.service-now.com/nd_portal?id=kb_article&sysparm_article=KB0010124

7.6. Immediate Access Suspension

1. Authorized faculty or staff can request that access to IT services be immediately revoked by completing the Suspend Access form online. More information is available here: https://nd.service-now.com/nd_portal?id=kb_article&sysparm_article=KB0010152.
2. The Immediate Computer Access Suspension Request Form can be found here: https://nd.service-now.com/nd_portal?id=sc_cat_item&sys_id=13f063ce37919240f8b78ff1b3990e3b.

8. POLICY ENFORCEMENT

The University reserves the right to suspend or block access to an account when the University deems it necessary.

The University reserves the right to reduce or extend the grace period(s) at its sole discretion.

Exceptions to the stated grace periods are granted by the appropriate area(s) of responsibility (e.g., Student Affairs, Office of the Provost, Office of Human Resources). The relevant granting authority keeps a list of such exceptions.

9. REFERENCE DOCUMENTS

Policy or Document	Web Address
Academic Articles	http://facultyhandbook.nd.edu/governance/
Department/Organization Account Request	https://nd.service-now.com/nd_portal?id=product_page&sys_id=c759d9c7db22a34099dcf25bbf9619e7&table=
Immediate Computer Access Suspension Request	https://nd.service-now.com/nd_portal?id=kb_article_view&sys_kb_id=bb7fab94970035580009b8bfe153af6e
Information Security Policy	https://policy.nd.edu/assets/185243/information_security_policy_2015.pdf
Password Reset Procedures	https://nd.service-now.com/nd_portal?id=kb_article&sys_id=767bd827974f95140009b8bfe153af64

Responsible Use of
Information Technologies
at Notre Dame

https://policy.nd.edu/assets/185268/responsible_use_it_resources_2015.pdf

Strong Password Standard

https://nd.servicenow.com/nd_portal?id=kb_article_view&sysparm_article=KB0013552

10. CONTACTS

Subject	Office	Telephone Number	E-mail
Policy Clarification	Office of the Chief Information Officer, OIT	(574) 631-9700	cio@nd.edu
Account Creation	Help Desk, OIT	(574) 631-8111	oithelp@nd.edu
Web Address for this Policy		https://policy.nd.edu/assets/185252/net_id_access_to_university_it_resources_2015.pdf	