

Northeastern State University

Verification of Student Identify for Distance Education

All essential systems that contain protected, private information at NSU are behind a password protected firewall / portal branded as [goNSU](#). GoNSU has separate sections for students, employees, and faculty and advisors as well as important links within each of these sections for needed information. To log-in to goNSU, individuals must enter their user identification plus their unique password.

The institution's password policy (Attachment A) requires passwords between 12 and 30 characters and 3 of the 4 following things must be used.

- Must contain a lowercase letter
- Must contain a uppercase letter
- Must contain a number
- Must contain a special character ~!#\$%^&*()_+=-?><

Within the learning management system environment (LMS), Blackboard, NSU utilizes several tools to maintain the integrity of its courses, no matter the delivery mode. Students must log-in with their user ID and password to access the learning management system. The [Resources for Online Instructor](#) webpage summarizes some of these resources, and faculty and students have access to the following:

- Safe Assign – plagiarism prevention tool
- Respondus Lockdown Browser – prevents cheating on the device
- Respondus Monitor - camera required, allows remote exams with monitoring

Attachment B provides more information about LockDown Browser and Respondus Monitor. NSU has unlimited seats for Respondus Monitor which allows faculty to use it across the campus for all their distance exam needs. All products include trainings for faculty as well as student support.

Attachment A

<https://nsuok.teamdynamix.com/TDClient/2026/Portal/KB/ArticleDet?ID=123188>

NSU Password Policy

[? Password ?](#) [Password-Manager](#)

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Northeastern State University (NSU) resources. All users, including contractors and vendors with access to NSU's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Scope

The scope of this policy includes any NSU account on any system that resides at any NSU campus, has access to the NSU network, or stores any nonpublic NSU information.

Password Requirements

Passwords must be between 12 and 30 characters and 3 of the 4 following things must be used.

- Must contain a lowercase letter
- Must contain a uppercase letter
- Must contain a number
- Must contain a special character ~!#\$%^&*()_+=-?><

Employees must choose unique passwords for all of their NSU accounts and may not use a password that they are already using for a personal account.

NSU users must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa\$\$w0rd" are equally bad from a security perspective.

Password Change

All passwords must be changed every twelve months. An email will be sent 30 days prior and 7 days prior to your account being disabled informing you that it is time to change your password.

Some users are required to change their password every 90 days. (i.e. those who deal with PCI or PII data). Default is 12 months.

If the security of a password is in doubt— for example, if it appears that an unauthorized person has logged in to the account — the password will be reset by an administrator and the user will be required to change the password.

Password Protection

ITS will never ask for your password.

Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, etc. Everyone will create their own password in accordance with this policy.

Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

Employees must take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. ITS provides [training](#) and collaboration on how to recognize these attacks.


Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices.

Password managers may be used to store and remember passwords.

Password Expiration

To prevent an attacker from making use of a password that may have been discovered, passwords are deemed temporary and must be changed regularly. ITS reserves the right to reset a user's password in the event a compromise is suspected or reported. Passwords are required to be changed every 12 months. If your password is not changed before the 12- month period is passed, your account will be disabled until your password has been changed.

Attachment B



Respondus

FEATURE CHECKLIST

LockDown Browser + Respondus Monitor

It's hard to keep up with latest features of Respondus Monitor, much less the ones that have been around for years. Here's a checklist that highlights both the old and new.

Operating Systems & Devices

- ✓ Windows
- ✓ macOS
- ✓ Chromebook
- ✓ iPad

Launches from any major browser

- ✓ Chrome
- ✓ Firefox
- ✓ Edge
- ✓ Safari

LockDown Browser

- ✓ Quick, one-time install
- ✓ Prevents cheating on the device itself
- ✓ More stable and secure than "locked browser plugins"

Partner Integrations

- ✓ Blackboard Learn Original View
- ✓ Blackboard Learn Ultra View
- ✓ Brightspace
- ✓ Canvas Classic Quizzes
- ✓ Canvas New Quizzes
- ✓ Moodle
- ✓ Schoology Assessments
- ✓ Schoology Tests/Quizzes
- ✓ McGraw Hill ALEKS (HE Edition)
- ✓ McGraw Hill ALEKS (PPL Edition)
- ✓ Pearson MyLab
- ... and more

Student Support

- ✓ 24/7 Live Chat support for students
- ✓ Help Center & Troubleshooting Knowledgebase
- ✓ Ticket-based support

Instructor Trainings (all free)

- ✓ Weekly training webinars
- ✓ Office Hours
A 15-minute, personal appointment with a Respondus trainer
- ✓ Lunch and Learn training for your department/institution
- ✓ In-app training resources
Videos, sample syllabus text, Quick Start Guides, etc.

One Technology, Lots of Flexibility

- ✓ Classrooms (in-person, online exams)
- ✓ Testing Centers
- ✓ Remote Exams with automated proctoring
- ✓ Remote Exams with Zoom/Teams/Meet/etc.
- ✓ Hybrid Classrooms (some students in class, others remote)

Language Localizations

- ✓ English
- ✓ Spanish
- ✓ French
- ✓ German
- ✓ Italian
- ✓ Portuguese

Security and Privacy

- ✓ Privacy by Design
- ✓ SOC 2 Certified
- ✓ GDPR, CCPA, FERPA
- ✓ AWS Certified engineers

Scalable and Cost-effective

- ✓ Selected by 1,500 universities
- ✓ 50 million proctored exams over 12 months
- ✓ Transparent pricing (3 options to choose from)

✓ New feature added within the past 18 months
 Available from within the application

respondus.com/monitor