

Student Information System Extended Access Request Form for UW-Madison

Mail or fax completed form with all signatures to: Security Authorizations, 1210 W Dayton St. **FAX 265-0667**

Please allow 7-10 business days for authorization to be completed.

Name	Student 3-Character ID
Job Title	Campus/Photo ID
Dept Name	Dept UDDS
Dept Address	Dept Phone
Email Address (wisc.edu)	

SIS student standard access hours are Monday through Friday 7am to 5pm. If the student employee end user requires additional access outside the standard hours, indicate the extended access option with an "X" or write in special request. A begin date is required. If no end date is indicated, it will be assumed that the request is intended to be permanent.

	Extended access 2 – Monday – Friday 6am – 11pm	Begin date:	End date:	BASE2
	Extended access 3 – Sunday – Saturday 6am – 7pm	Begin date:	End date:	BASE3
	Extended access 4 – Sunday – Saturday 6am – 11pm	Begin date:	End date:	BASE4

Special Request: Your school/college may require additional documentation for review of special requests. Check with your Dean/Director/or Designee. This area can be used to request shorter as well as longer access periods.

Description	Begin Date	End Date

With appropriate signatures, access will be granted as requested. We ask that you take this authorization process as an opportunity to consider and discuss with staff the following items:

- Care should be taken when working in a non-standard location. The potential for access to data by non-University employees, or University employees who do not have access to this data is increased.
- Access is a privilege granted to members of the University community. It carries with it the responsibility to use it for authorized University business related activities.
- Authorization for use is provided to each individual for his or her own use. No person may use or share an authorization belonging to someone else.
- Any account can serve as an entry point for theft, damage or unauthorized use. Users must protect the confidentiality of their user ID's and passwords and are expected to exercise care to insure that others cannot use their account.
- You must always log off when your work is complete.
- Secure disposal of any data printed is your responsibility.

USER AGREEMENT TO ACCEPT RESPONSIBILITY

Increased risk of exposure of data to unauthorized persons accompanies extended access times and especially access from non-standard work areas. You must always log off your access device when your work is complete. As the authorized user, responsibility for security of all data accessed and secure disposal of any data printed is your responsibility. Your use of University computing resources and access to authorized data is restricted to UW business (See <https://it.wisc.edu/about/office-of-the-cio/it-policies/>). You may access only the data for which you have specific authorization. You will personally be held responsible for any security breach, willful misuse and/or deliberate system damage traceable to your assigned logon identification.

**Violation of this agreement may result in disciplinary action or legal action – or both.
I HAVE READ AND UNDERSTAND THE ABOVE TERMS AND AGREE TO THESE TERMS.**

User Signature	User Name – Print	Date
Department SIS Authorizer Signature	Department SIS Authorizer – Print	Date
Dean/Director Signature	Dean/Director – Print	Date

Only complete forms will be processed. Incomplete forms will be returned to the sender. SIS Authorization Form and Access Compliance forms must be on file for processing to proceed.