University of Wisconsin Stevens Point

UWSP Business Affairs Policy and Procedures

Access - Key & Access Cards – Stevens Point Campus

1. PURPOSE

The purpose of this policy is the protection of the lives and property of the campus community. Maintaining accurate, effective access control for exterior and interior doors is critical to protecting the campus. It is the policy of the University of Wisconsin-Stevens Point to issue the lowest tier of key that will be effective for the type of access that is needed for any given application.

This policy is in place to:

- ensure that people requesting access are authorized to do so
- ensure an individual(s) requesting access are receiving the correct tier of access
- ensure the lowest tier of access that is effective is provided to the requestor
- ensure a process of accountability for the return of keys or removal of door permissions
- resolve problems resulting from a lack of access control
- ensure accountability when Departments have an access control breach
- ensure compliance of Federal, State, or other agencies guidelines

Applicable to all current and future sites under the operational jurisdiction of the University of Wisconsin-Stevens Point.

2. DEFINITIONS

- *Access:* The ability granted to an individual to independently access a secured space. Access may be provided through the use of keys, access cards, or a mobile app.
- *Access Card:* A card that interfaces with electronic locks to provide access to secured spaces. This includes PointCards and Prox cards.
- *Access Holder:* An individual or group being given access to secured spaces.
- *Building Hours*
  - *Public Building Hours:* The hours a building’s public entrances are unlocked and allow the general public access to the building.
  - *Campus Community Building Hours:* The hours a building’s public entrances are accessible to the campus community via electronic access. Campus Community Building Hours include public building hours.

- *Building Contact:* A contact person(s) for a physical building who assists with dissemination of information for building occupants in case of an emergency, can provide insight on the building services, and reviews requests for temporary building hours change.
- *Campus Community*: All current UWSP faculty, staff, and students. Does not include emeritus, retirees, contracted partners, or volunteers.
- *Campus-Wide Support Unit*: A UWSP division, department, or unit that provides frequent, campus-wide, in-person support of facilities, infrastructure, hardware, or safety; often outside of business hours, independent of the space occupants, or in emergency situations. These units are: Environmental Health and Safety, Facility Services (including Custodial), Facilities Planning, Information Technology, Risk Management, and University Police (including Emergency Management).
- *Checkout Card*: A prox card which is assigned to a campus department or group who then issues the card to an individual to provide temporary access.
- *Contracted Partner*: A party or individual with a contracted relationship with UWSP but who is not a member of the campus community or a contractor. For example, an organization leasing space or with a cooperative agreement with UWSP.
- *Contractor*: A party or individual performing paid, contracted work for UWSP.
- *Electronic Access:* Please refer to Access Card.
- *High-Risk Spaces:* Spaces deemed high-risk by the campus risk manager, or any area with hazardous levels of radiation; hazardous chemicals or substances; hazardous biological agents or vectors; or, hazardous equipment or processes. Examples of such spaces include:
    - laboratories where the hazards listed above are present
    - animal care, housing or animal research facilities;
    - mechanical rooms;
    - chemical and hazardous material or waste storage areas;
    - construction areas;
    - maintenance garages and shops;
    - custodial storage areas;
    - machine shops, woodworking shops, or similar workshop areas;
    - other areas as determined by UWSP.
    - food preparation areas;
    - fitness and strength centers;
    - loading docks and warehouses;
    - recycling centers;
    - art studios and shops;
    - steam plants;
    - high security areas;
    - areas that are excluded for general employee or student access; and
- *Key Tender*: A key cabinet from which keys can be checked out electronically using an access card. Key tenders are typically used to secure master and/or shared key sets.
- *Mobile App*: An application usable from smartphones, tablets, or other electronic devices which allow an authenticated user to access secured spaces and to manage their access card.
- *PointCard:* UWSP's Campus ID card which serves as an individual's access card.
- *Prox Card:* An access card solely used to provide access to electronic locks.

- *Public Entrance*: An exterior building door that enters a common space such as a public corridor or courtyard.
- *Space Access Managers*: The individual(s) responsible for reviewing and approving or denying permission requests for a space based on appropriateness of access to the space as well as safety and risk.
- *Special Access*: Access types that have special restrictions or approval requirements. See section 5.
- *Supervisor*: The faculty or staff member who is responsible for reviewing and approving or denying permission requests for an individual based on the need for the permissions. A supervisor may be an individual a position reports to for a faculty or staff position (including student staff), or a department chair, instructor, research advisor, or a volunteer coordinator.
- *Temporary building hours:* A requested change made to a building manager(s) to change building hours for a special event open to the public.
- *Volunteer*: An unpaid individual working to support UWSP's mission but who is not a member of the campus community. This may include retired individuals and emeriti faculty who are continuing research or doing other unpaid work for the University. Volunteers must be approved through Human Resources' Volunteer Approval process.

3. POLICY

a. General

i. Access will be issued only to authorized persons in alignment with their role within UWSP.

ii. All keys and access cards are the property of the University and must be returned upon termination of their employment or relationship with UWSP. Obsolete or unneeded keys must be returned to Facility Services for disposal.

iii. Individuals may only use access assigned to them. Transfer of keys, access cards, or authentication credentials (e.g., network IDs or passwords) to other individuals or groups is not permitted.

iv. Circumvention of access controls to obtain or allow unauthorized access is not permitted.

v. Duplication of any key or access card issued by the University is not permitted except for authorized personnel as listed in section 3.

b. Access Holder Responsibilities

i. General

1. Access holders will not compromise the security of any area or building and further agrees to secure each door upon leaving the area.
2. Access may only be used by the person it is assigned to and is non-transferrable. If an unauthorized user presents an access card that is not assigned to them, the card will be confiscated.
3. Access holders must take reasonable steps to ensure the security of keys and access cards provided to them as well as their UWSP network account.
4. Access holders must immediately deactivate lost or stolen access cards and report lost or stolen keys and access cards as soon as possible.

ii. Keys

1. Duplicate keys for a building or area within a building shall not be issued to an individual without prior approval of the Director of Facilities Services.
2. A new or duplicate exterior of a building shall not be issued to an individual or department without prior approval of the Director of Facility Services.
3. Duplicate or replacement key(s) for an area within a building, which replace current assigned keys to the building, shall only be issued to a space manager after a work order is placed with Facility Services.

iii. Access Cards

1. Anyone requesting a PointCard must provide a current government-issued photo ID at the time the ID is issued.

c. **Responsible Parties for Overall Process**

i. Facilities Services is the authorized agent for installation, maintenance, and control of all physical locks and keys for university buildings. This responsibility includes design of physical lock systems, including selection of lock hardware, creation and issuing of keys, and maintaining physical lock records.

ii. Information Technology is responsible for issuing access cards and electronic lock permissions management e-forms. This includes maintaining a building hours website.

iii. Information Technology and Facilities Services are responsible for the design, installation, and maintenance of the electronic lock system.

iv. University Police is the authorized agent for assigning and controlling electronic lock access and building hours.

v. Risk Management and Environmental, Health, and Safety (EHS) are responsible for identifying hazardous or high-risk spaces, requesting door groups controlling access to these areas be flagged with the appropriate policy, and monitoring access requests for these areas to ensure risk and safety compliance.

vi. Supervisors are responsible for reviewing access requests from subordinates, verifying requests are based on need, meet policy requirements, and approving or denying access requests.

vii. Space Access Managers are responsible for reviewing access requests for the spaces they are responsible for, verifying requests are appropriate for the space and meet policy requirements (including any safety and risk concerns), and approving or denying access requests.

   a. Depending on the building, a space manager may be assigned as an authorizing agent for access requests in their space.
   b. Space managers are responsible for maintaining a log of keys assigned to their offices and are responsible for tracking and assigning keys for offices within their space.

viii. Supervisors and space access managers are responsible for performing a yearly audit of the access provided to their subordinates or spaces and removing access where it is no longer needed or appropriate.

d. **Building Hours**

i. Building hours may vary and will be determined by the uses of the facilities and coordinated between the building's leadership and University Police.
ii. Building hours are posted on the exterior facing doors and also online at building hours website.
iii. Public building hours may be temporarily extended upon request for events attended by the public.
   i. Temporary requests should be made to the building contact(s).
      a. The building contact reviews the request with the appropriate parties for the event which must include University Police, deans/directors within the building, Facilities Services and other impacted parties.
      b. Building contact sends any approved request, one week prior to the temporary change is planned, via email to University Police (police.and.security.services.office@uwsp.edu) and Information Technology (EMAIL) to allow accurate scheduling of doors.
   ii. Permanent building hours requests should be sent to the Vice Chancellor for Business Affairs for review.
iv. Public building hours and campus community building hours will be suspended by default during state-observed legal holidays and other campus closures.
   i. Space Access Managers must coordinate with University Police in advance if public or campus community hours are required during these suspended times.
v. Building hours may be suspended in the event of an emergency as determined by Emergency Management or University Police.

e. **Access**

i. General building access may be provided as outlined in section 3.f.
ii. Access to Special Access areas is restricted and is only provided according to section 3.g.
iii. Electronic lock access permissions may be granted to an individual or to automated active directory groups (i.e. DIMS based department distribution lists, Campus Solutions based course and major/minor lists). The use of manually maintained lists outside of the e-form approval process is not allowed as they may be used to circumvent the approval process.

f. **General Access**

i. **Faculty and Staff** (including student staff)

1. May receive access to any areas required to fulfill the duties of their role.
2. Access must be approved by the individual's supervisor for the role access is being requested for and the space manager if access is to a space not within the scope of their work role.
3. Electronic lock access must be assigned to the individual via their UWSP faculty/staff network account.
4. Access card will be the individual's PointCard.

5. Access shall be reviewed annually.
6. Access shall be revoked upon termination of role or service.
7. While student staff access will follow the same working in isolation policy as other faculty and staff, their access should be more closely assessed, and access should only be granted where there is a strong need and unsupervised access is appropriate.
    1. Space managers and supervisors shall keep on file documentation of access requests if there is a need for unsupervised access.

ii. **Students**

1. May receive access to any areas required as needed to fulfill their curricular, extracurricular, residential, or volunteering needs with the following limitations:
    a. Access cannot be provided to high-risk spaces (see section 3.g.iii).
    b. Access shall be limited to campus community building hours unless an exception is approved by Assistant Dean, Director, or higher.
    c. Access shall not be provided under the student access policy for paid positions (i.e. student staff). For student staff access, please see Faculty and Staff policy (see section 3.f.i).
2. Access must be approved by a UWSP faculty or staff member (excluding student staff) using the official request process.
3. Electronic lock access must be assigned to the individual via their UWSP student network account.
4. Access card will be the individual’s PointCard.
5. Access expires at the end of each spring semester and must be re-requested if continued access is required.
6. Access shall be revoked if the student is not a current or continuing student, including upon graduation or withdrawal from the University.

iii. **Contracted Partners**

1. Access may be provided per the terms of an agreement with UWSP approved by a person with authorized signature authority for the agreement.
2. Access must be approved by a UWSP faculty or staff member (excluding student staff)
3. Access may be assigned to an individual or to the group depending on the agreement terms.
4. The access card may be provided in the form of a PointCard (when a UWSP affiliate account exists) or Prox Card.
5. Access expires at the end of each spring semester and must be re-requested if continued access is required.
6. Access shall be revoked upon expiration or termination of the agreement or when an individual separates from the group which is covered by the agreement.

iv. **Contractors**

1. Access must be requested by UWSP faculty or staff member (excluding student staff) within a Campus Wide Support Unit.
2. Access may be provided per the terms of an agreement with UWSP approved by a person with authorized signature authority for the agreement.

3. The access card may be provided in the form of a PointCard (when a UWSP affiliate account exists) or Prox Card.
4. Access must expire at the end of the current project or contract and be re-requested if continued access is required.
5. Access shall be revoked upon expiration or termination of the agreement or when an individual separates from the group which is covered by the agreement.

v. **Volunteers**

1. Access shall be restricted to situations where unsupervised access is appropriate and required to fulfill the duties of their role with the following limitations:

a. Access cannot be provided for convenience.

b. Access cannot be provided to high-risk spaces (see section 3.g.iii).

2. Access must be approved by a UWSP faculty or staff member (excluding student staff).
3. The access card may be provided in the form of a PointCard (when a UWSP account exists) or Prox Card.
4. Volunteers must be formally approved by Human Resources prior to access being requested or approved.
5. Access expires at the end of each spring semester and must be re-requested if continued access is required.
6. Access shall be revoked upon termination of role or service.

vi. **Retired and Emeritus Faculty**

1. Access is restricted to department-provided office space for the individual during public building hours for the building in with the office space is located.
2. Access cannot be provided to high-risk spaces (see section 3.g.iii).
3. Access must be approved by Assistant Dean, Director, or higher.
4. Electronic lock access must be assigned to the individual via their UWSP faculty/staff network account.
5. Access card will be the individual's PointCard.
6. Access expires at the end of each spring semester and must be re-requested if continued access is required.
7. Note: Where retired individuals or emeritus faculty are performing unpaid work on behalf of the University, additional access may be considered under the Volunteer policy (see section 3.f.iv).

g. **Special Access**

i. Access to specialized areas or locks are restricted according to table 1. Individuals in an "Authorized Users" role may automatically be granted these permissions with no additional approvals (notification only). Individuals not in a role listed under "Authorized Users" must receive approval from the listed approver prior to being granted special access.

Table 1: Special Access

Type of Access	Default Authorized Users	Exception Approver
Exterior Grandmaster – Physical key to all exterior entrances on all institutional buildings.	Campus Locksmiths and University Police	Chief of Police (or delegate)
Building Master – All spaces within a specific building (excluding off-master and special master spaces)	Chancellor, Vice Chancellors Deans, Chairs, Directors, Unit Administrator, and Building Managers for areas they supervise Campus-Wide Support Units	Space Access Manager and Chief of Police (or their delegate)
All Electronic Locks Access (ADAT)	• Public Safety Personnel (University Police) • Locksmiths • Electronic Lock System Administrators	Chief of Police (or delegate)

ii. Campus-Wide Support Unit Access

1. Members of campus-wide support units may receive access to all electronic locks (with exception to some high-risk spaces) and access to building master keys as needed by their role with the approval of their supervisor.
   a. Individuals of campus wide-support units which do not directly perform campus-wide support as part of their role shall not be granted campus-wide access.
   b. Where an individual is assigned primary and secondary work locations, access shall only be provided to those areas and campus-wide access shall not be provided.

iii. High-Risk Spaces

1. Access to high-risk spaces shall not be granted to students, contracted partners, volunteers, retirees, or emeritus faculty. Student staff access is permitted where appropriate.
2. Additional restrictions on these spaces may be enacted to meet the needs of the space and/or regulatory requirements (e.g. safety training, Working in Isolation permits). These requirements must be fulfilled prior to an individual being granted access to a space.

h. **Access Request Approval Process Requirements**

i. All general access requests must be approved by both a supervisor and the space access manager(s) of the requested area. Where an approver is both a supervisor and a space access manager of a request, only their approval is required.
ii. Special access may be granted to default authorized users as listed in table 1 with only supervisor approval. Individuals who are not a default authorized user must receive permission from both their supervisor and the exception approver listed in table 1.
iii. Campus-Wide Support Unit access as defined in section 3.g.ii may be granted with only supervisor approval.

i. **Checkout Access Cards**

i. Authorized departments may maintain checkout cards for residential building electronic locks for the purpose of providing urgent or emergency access to students residing within the residence halls, to provide access to non-UWSP community members for event housing, or to provide short-term contractor access.
1. Use of department checkout cards must be approved by University Police. The authorized department shall be responsible for
   a. maintaining logs of who they have issued checkout cards to (including card number and dates issued and returned) for a period of 6 months and provide the logs to University Police upon request,
   b. secure storage of checkout cards when not in use, and
   c. conducting routine audits of their checkout cards to ensure they are present and immediately notify University Police of any checkout cards which are identified as missing, lost, stolen, or unreturned so they can be deactivated.

ii. Campus departments may use checkout cards where appropriate to mitigate risks associated with assigning wide-spread access or access to sensitive areas to an individual’s access card.
1. Use of department checkout cards must be approved by University Police.
2. When not in use, checkout cards must be stored in an electronic key tender and checked out via an individual’s access card or mobile app.

j. **Termination, Retirement or Separation from University**

i. Access is valid throughout the cardholder’s length of affiliation, registration, or employment at the University (exception applies to authorized guests).
ii. Keys and PointCards are the property of the University of Wisconsin-Stevens Point, which reserves the right to revoke its use or any accounts at any time.

k. **Fees**

i. Access Card Equipment

1. Offices or departments seeking additional card access on interior doors should place a request with Information Technology. Offices or departments will be responsible for equipment, installation, software license and/or continuing maintenance cost.

ii. Access Card Fees

1. Initial access card costs are set by Information Technology based on the material, labor, equipment, and maintenance costs associated with creating each card.
2. Faculty, staff, student employees, and volunteers: Costs will be charged to their department.
3. Contracted Partners: Charges will be handled according to their contract terms.
4. Students: Provided through student fees.

ii. Replacement Access Card Fee

1. Replacement PointCard due to missing, stolen, lost, or negligently damaged card will be charged a replacement card fee set by Information Technology. This fee is charged to the individual.
2. Card replacements due to normal wear and tear or legal name change are provided at no cost. The original card must be exchanged for the replacement card for a no-fee replacement.

4. **REFERENCES and RELATED DOCUMENTS**

UWS 18.08 Personal conduct prohibitions.

(6) Physical security compliance.

(a) No person may ignore, bypass, circumvent, damage, interfere with, or attempt to deceive by fraudulent means, any university authorized security measure or monitoring device, whether temporary or permanent, that is intended to prevent or limit access to, or enhance the security of, university lands, events, facilities or portions thereof.

(b) No person may duplicate, falsify or fraudulently obtain a university key or access control device, or make any unauthorized attempt to accomplish the same.

(c) No person who is authorized to possess a university key or access control device may transfer a university key or access control device to an unauthorized person, nor may any unauthorized person be in possession of a university key or access control device.

(d) Any university key or access control device in the possession of an unauthorized person may be confiscated by any authorized university official.

UWS 18.07 Use of campus facilities.

(1) Access to roofs, service tunnels, and maintenance facilities prohibited. No person may climb into, out of, or onto any university building, service tunnels or maintenance facilities, or walk or climb upon any university building or roof, except when emergency access to a fire escape is necessary, for required maintenance, or when authorized by the chief administrative officer.

(2) Closing hours.

(a) Except as specifically provided in this code, the chief administrative officer may establish closing hours and closed periods for university lands, buildings, or portions thereof. These closing hours and closed periods shall be posted in at least one conspicuous place adjacent to or at the periphery of the area to be closed or, in the case of buildings, on the building.
(b) No person, unless authorized to be present during closed periods, may enter or remain within the designated university lands, buildings, or portions thereof during a closed period established under this section.
(c) For the purpose of par. (b), “person authorized to be present "means a person authorized to be present by an order issued pursuant to par. (a) or s. 36.35 (2), Stats.
(d) No person, except those authorized to be present after the posted closing hour, may enter or remain in any university arboretum or picnic area unless traversing those areas or on park roads at the times the roads are open to the public.
(3) Limited entrance. The chief administrative officer may, by posting appropriate signs, limit or prohibit entrance to university lands, or portions thereof, in order to maintain or preserve an instruction or research area.
(4) Picnicking and camping. No person may picnic or camp on university lands, except in those areas specifically designated as picnic or camping grounds, or as authorized by the chief administrative officer. No person may violate any rules and regulations for picnicking or camping established and posted by the chief administrative officer. For purposes of this subsection, camping shall include the pitching of tents or the overnight use of sleeping bags, blankets, makeshift shelters, motor homes, campers or camp trailers.
(5) Prohibitions on blocking entrances. No person may intentionally physically block or restrict entrance to or exit from any university building or portion thereof with intent to deny to others their right of ingress to, egress from, or use of the building.
(6) Restricted use of student centers or unions. No person, except members of the student center or union, university faculty and staff, invited guests, and university-sponsored conference groups, may use student center or union buildings and grounds except on occasions when, and in those areas where, the buildings or grounds are open to the general public.
(7) Structures. No person may place or erect any facility or structure upon university lands unless authorized by the chief administrative officer.
History: CR 08-099: (1) to (7) renum. from UWS 18.06 (9), (7), (6), (14), (24), (20), (15) and am. (1), (2), (3), (6), cr. (title) Register August 2009 No. 644, eff. 9-1-09; correction to (title) made under s. 13.92 (4) (b) 2., Stats., Register August 2009 No. 644.

UWS 18.13 Penalties.

Unless otherwise specified, the penalty for violating any of the rules in ss. UWS 18.06 to 18.12 shall be a forfeiture of not more than $500, as provided in s. 36.11 (1) (c), Stats. Note: Violations of the rules in ss. UWS 18.06 to 18.12 will be processed in accordance with the citation procedure established in s. 778.25, Stats.
History: Cr. Register, March, 1976, No. 243, eff. 4-1-76; am. Register, November, 1991, No. 431, eff. 12-1-91; CR 08-099: renum. from UWS 18.07 and am. Register August 2009 No. 644, eff. 9-1-09.

Working in Isolation | UW Policies (wisconsin.edu)

Working in Isolation policy - UWSP Risk & Safety and UWSA Policy 620
Individuals may work in isolation if an explicit written request from the person in charge of the work is approved. Confirmation of this approval will be in the form a permit issued to the individual working in isolation.

Acceptable Use of Information Technology Resources - Regent Policy Document 25-3
Authorized users must not engage in unacceptable use of UW System IT resources, which includes but is not limited to the following:

1. Sharing or transferring authentication details to others, or using another user's authentication credentials such as network IDs and passwords, or other access codes or circumventing user authentication which could allow unauthorized users to gain access to UW System IT resources, except as required for administrative or business purposes

5. POLICY HISTORY

Effective Date: 11/18/2024
Effective Date Approved: 11/7/2024
Approved by: Vice Chancellor for Business Affairs

Revision Date: 1/21/2025
Revision Approved by: Vice Chancellor for Business Affairs

6. SCHEDULED REVIEW

June 2025