

Title: Credential Management in PERSONA (PCO)
Department: PPM IT Services & PPM Lock Shop
Effective Date: May 1, 2025

PURPOSE

To define business processes and automation rules for managing cardholder access credentials using the PERSONA Campus Online (PCO) system at CSUN. This includes handling mobile and physical credentials, access levels, and the partitioned system architecture.

SCOPE

This SOP applies to all departments (partition & sub-partition administrators) and other affiliated personnel who are issued access to administer credentials in the PERSONA Campus Online (PCO) access control system.

RESPONSIBILITY

Lock Shop: Oversee system partition control, manage perimeter access control, and program locks and access cards not managed by a sub-partition administrator.

Department or sub-partition administrators: Manage partition-specific access levels and credentials.

PPM IT Services: IT support for PCO, handles unaffiliated cardholder creation requests.

DEFINITIONS

1. **PERSONA Campus Online (PCO):** The enterprise access control platform for managing door access.
2. **Cardholder:** A Cardholder is any person who will be given an [access credential](#). Access credentials are typically cards but may also be some other type of credential, such as a mobile credential, PIN code, or biometric identifier. Cardholders can have more than one credential assigned to them.
3. **Cards:** Cards are access control credentials that are typically some form of card but may also be some other type of credential, such as a mobile credential, PIN code, proximity fob, or biometric identifier.
4. **Access Level:** Access Levels consist of [Door Group/Time Schedules](#). Access levels assign access to cards to control where and when a card is granted access. Because Access Levels

comprise at least one Door Group and Time Schedule, the corresponding Door Group and Time Schedule must exist or be created before attempting to create an Access Level.

5. **Door Groups:** A collection of door(s). Door Groups are combined with [schedules](#) in the creation of [access levels](#).
6. **Areas:** (Anti-passback) is a feature that tracks cards in and out of given areas. To be effective, the area must have both an entrance reader and an exit reader, and those readers must be used each time a cardholder moves in and out of the area. Parking ramps are a typical application for anti-passback areas.
7. **Schedule:** A collection of days, time segments, and [Holiday Groups](#) used to define time frames for repeated actions. Schedules can be used in two ways: in [Scheduled Commands](#) to command hardware (readers, outputs, or specific events) and in [Access Levels](#) to define when cards have access to certain readers.
8. **Holiday Group:** A collection of one or more [Holidays](#). Holiday Groups can be used when creating [Schedules](#) to define behavior that is an exception to the regular schedule.
9. **Holiday:** Any day of the year that follows a different schedule than the typical day of the week the holiday falls on. Holidays are used to define access control exceptions in the system. They are added to [Holiday Groups](#), which are described in [Schedules](#) as unique days that override the normal days of the week and have different access times.
10. **MataCard:** Secure digital CSUN ID. Apple/Android devices and smartwatches supporting mobile credentials, or an NFC credential encoded to be compatible with CSUN's Transact infrastructure.
11. **Transact Card:** Same as MataCard
12. **Partition or Sub-Partition:** Segmented area of control in PCO assigned to different departments. The effect of partitioning is to divide the system hardware, cardholders, cards, and the complete set of program data, such as schedules, access levels, etc., so that users can only see a portion of what is contained in the entire system.
13. **System Partition:** Top-level partition, only authorized users in PPM Lock Shop and PPM IT Services have access to this partition.
14. **PERSONA Interface:** Aka "**Interface**". The PERSONA Campus Online Software allows for the import of user information such as name, ID number, access rights, and more. This eliminates the need for repetitive and error-prone data entry.
15. **V2000:** HID controller V2000 is a two-reader access control panel that enables interface with two doors, handles all online door decisions, door input monitoring, output control, and a reader interface for up to two doors. A V2000 is wired to the network and has near real-time synchronization to the PCO system/servers. The database is cached locally on the V2000, so if there is no connection to the server, the V2000 will still function. No updates to access can be made until the connection is restored.
16. **X1100:** A newer version HID controller, like V2000.
17. **Scheduled Commands:** A scheduled command can unlock a door for a specific schedule or activate/deactivate an output based on a schedule.
18. **Prox card:** An access card or key card is a contactless card that can be read without inserting it into a reader device. It is also referred to as a "tap" card.
19. **Card Set:** The definition of a group of cards. This definition contains the card format and facility code (if used).

PROCEDURES

1. System Access
 - 1.1. PERSONA Campus Online via access and credentials assigned by PPM.
 - 1.2. The System Partition “owns” cardholders and cards; however, the data is global, so sub-partitions can view and manage these objects.
 - 1.3. Department admins can manage access levels, schedules, and cardholders within their assigned partition. Access levels and Schedules may be owned by the System Partition but shared with the specific sub-partitions for management.
 - 1.4. Departments can only access doors, door groups, access levels, and schedules assigned to their partition.
 - 1.5. Perimeter doors remain in the system partition, and only PPM Lock Shop manages access to perimeter doors, unless all tenant(s) in the building agree to permit common perimeter doors to be managed by a partition department.
 - 1.6. Residential Life and Conference Services: notwithstanding the above, all door objects, access levels, schedules and access control panels will be “owned” by the Housing partition. Residential Life and Conference Services holds primary responsibility for configuring all objects assigned to their partition.
2. Card or Credential Types
 - 2.1. Prox Cards
 - 2.2. MataCards
 - 2.3. PIN Codes (deprecated in PERSONA Campus Online)
 - 2.3.1. PIN Codes have been phased to all cardholders identified by a cardholder number.
 - 2.3.2. PIN Codes not associated with a cardholder will be phased out soon.
 - 2.3.3. Modern mobile-capable locks are recommended for MataCard support.
 - 2.4. Card Set
 - 2.4.1. Prox Card: Prox-Facility 55, Prox-Simplex 36 bit, etc...
 - 2.4.2. MataCard: Transact Card
 - 2.4.3. PIN: PIN Only
3. Automation Workflow
 - 3.1. Data Imports to PCO
 - 3.1.1. HR (active employees) once a day.
 - 3.1.2. Auxiliary (active employees) once a day.
 - 3.1.3. Enrollment Services (active students) once a day.
 - 3.1.4. Housing (active reservation) every 15 minutes.
 - 3.1.5. MataCard (Transact cards) every 15 minutes.
 - 3.1.6. Meal Plan (access levels) every hour.
 - 3.1.7. CECS (access levels) every hour, 8 to 5 M-F.
 - 3.1.8. Transact Unaffiliated cardholders (TBA)
 - 3.2. PERSONA Interface
 - 3.2.1. Scheduled to run every 15 minutes.
 - 3.2.2. Add cardholder information based on data integration (imports).
 - 3.2.3. Add access levels based on data integration and predefined rules.
 - 3.2.3.1. Access level(s) added to one credential (prox or MataCard) will be copied to existing credentials. This makes all credentials issued to the same cardholder have the same access levels. Access is granted to a cardholder not per credential.

3.2.4. Removes access levels when cardholders are no longer in the source data (imports). The Interface expects to be provided 100% of the records every time, not just the changes and removals since the last run. If a user’s record disappears from the source data or the rules used to process their data are no longer met, the interface will remove that user’s access rights.

3.3. Credential Expiration Rules

3.3.1. Access credentials will auto-expire when cardholders are no longer active in HR (employees and auxiliary employees) or Enrollment Services (students).

3.3.1.1. If a record no longer exists in the import files.

3.3.1.1.1. Access cards will expire with a date of 1/1/2013.

3.3.1.1.2. If there are multiple cards, all cards will expire.

3.3.2. Manual expiration may be applied before automated processes to cancel access immediately.

3.3.2.1. If there are multiple cards, PERSONA Interface will expire all cards associated with the cardholder. Expired credentials will disable all associated access, including MataCards and prox cards.

3.3.2.2. Please double-check after 30 minutes that all cards have expired.

3.4. Lock Updates

3.4.1. Wireless locks updates occur not less than once daily as scheduled by PPM or Housing, or immediately after denied access triggers communication.

3.4.2. Wired locks connected to a V2000 or X1100 are updated immediately.

3.4.3. Mobile credentials (MataCards) are created within 30 minutes, and if there are existing credentials (such as a prox or MataCard), existing access levels will be copied to the new credential(s).

3.5. “z” Access Level Naming Convention

3.5.1. The following table describes the naming convention used for “z” access levels in the System Partition to enable automation based on HR or Enrollment Services data.

Cardholder Type	Format	Example
Staff/Faculty/MPP	zNNNNN-Employee	z10022-Employee
Student Employees	zNNNNN-StudentEmployee	z10022-StudentEmployee
All MPPs	zAll-MPP	zAll-MPP
All Active Students	zAll-Student	zAll-Student
All Active Staff/Faculty/MPP Employees	zAll-Employee	zAll-Employee

3.5.2. NNNNN is the 5-digit PeopleSoft department ID. In PCO, the field name is “Dept ID”.

3.5.3. CSUN will create the access levels.

3.5.4. PERSONA Interface will add access levels to cardholders.

3.5.4.1. If exists zNNNNN-Employee: Add if SOLAR_DATA.dbo.hrnprd_export: The if ‘Union Code’ is one of C99, M80, M98, R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, and the DeptID matches NNNNN. (The employee export contains some non-staff employees, so limit it by union code.).

3.5.4.2. If exist zNNNNN-StudentEmployee: Add if the Union Code is R11, R12, R13, R14, or the job code is one of these values: 1868, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1880, 1881, 1883.

- 3.5.4.3. zAll-MPP: Add if the 'Union Code' is equal to M80 or M98 (This is a subset of zAll-Employee.)
 - 3.5.4.4. zAll-Student: Add all records in SOLAR_DATA.dbo.sanprd_export. (A cardholder will be in both zAll-Student and another group if they are also an employee.)
 - 3.5.4.5. zAll-Employee: Add if SOLAR_DATA.dbo.hrnprd_export: The 'Union Code' is one of one of C99, M80, M98, R01, R02, R03, R04, R05, R06, R07, R08, R09, R10.
 - 3.5.4.6. PCO Interface will remove access levels if the record is not in the source (SOLAR_DATA) tables.
 - 3.5.5. Uses of these access levels may include granting access to perimeter doors to buildings.
 - 3.5.6. By design, special consultants, helper/aid, casual workers, summer aid, childhood teachers, research fellows, instructional faculty non-credit extension, police cadets, and other positions in union code E99 are excluded from the above employee groups.
- 4. Student and Guest Access Policy
 - 4.1. Students are expected to use their MataCard issued by Enrollment Services. Departments may purchase a PPM-issued credential for a student or student employee at PPM's chargeback rates.
 - 4.2. A user may not share an access credential or a CSUN login with any other person. If PPM becomes aware that a credential or CSUN login is being shared, the affected credential may be revoked without notice, and/or the shared login may be disabled.
 - 4.3. For unaffiliated users (guests, contractors, vendors, etc), the sponsoring department must submit a request to PPM IT Services to create a cardholder record. Non-state and enterprise entities will be required to reimburse PPM per PPM's normal financial reimbursement process.
 - 5. Access Scheduling & Delegation
 - 5.1. To request creation of a Partition for a department or College, see the Lock & Key pricing menu website for information.
 - 5.2. Schedules and access levels reside in the System Partition by default.
 - 5.3. Department-specific schedules and access levels can be moved to the departmental partitions to reduce confusion and dependency on the Lock Shop.
 - 5.4. Only doors shared with department partitions can be managed in that partition.

REFERENCES

[MataCard](#)
[Smartsheet Unaffiliated Cardholder Request](#)
 PPM SOP 25-2019 Key Request
 Pricing Menu: <https://www.csun.edu/facilities/lock-key>

APPROVED



Jason R. Wang, Senior Director

05/27/2025

Date

APPENDIX

REVISION HISTORY

DATE	NAME	EVENT	NOTES
04/21/2025	E Garcia	Created	
04/28/2025	E Garcia	Final	
05/23/2025	E Garcia	Updated	Reference to Key Request SOP 25-2018 to 25-2019