1 Card Access and Security Clearance

Version 1 (Current Version)

Print

Policy	REG07.45.01
Title	1 Card Access and Security Clearance
Category	Finance, Operations and Auxiliary Services
Sub-category	One Card
Authority	Chancellor
History	Approved September 17, 2024
Contact	ECU 1 Card Director - (252) 328-2673; Office locations: G-521 Old Cafeteria Complex and 224 Health Sciences Student Center
Related Policies	
Additional References	1 Card security information & forms web site (https://1card.ecu.edu/security/)

1. Introduction

1.1. ECU 1 Card – Security Access

The ECU 1 Card office manages the security access system for East Carolina University for various buildings/ areas located on Main campus, the Health Sciences campus, and off-campus facilities. This involves controlling the locking and unlocking of buildings and facilities that are equipped with 1 Card readers across campus, and the configuration of individual cardholders' physical access via the ECU 1 Card upon authorized approval. The ECU Police Department monitors this system 24 hours a day, 7 days a week.

1.2. Definitions

1.2.1. "General Access" – Access to a building that has been unlocked by the 1 Card Office on a pre-determined schedule or for an event by request through 25Live or email.

1.2.2. "Patron" – A record of an individual in the 1 Card system and/or application.

1.2.3. "After Hours Access" – Any access granted to a facility, outside of the pre-determined schedule or general access assigned to valid patrons.

1.2.4. "Authorized Approver" – An ECU employee designated by the department or unit head to approve requests for access to a specific building, room, or facility based on a cardholder's business purpose.

1.2.5. "Authorized Scheduler" – An ECU employee designated by the department or unit head to set and modify building time schedules or access schedules for building access.

1.2.6. “Valid Card Holder” – ECU 1 Card holders who have been verified by 1 Card staff as being an active patron by virtue of their role as an employee, student, contractor, and/or specific business purpose that warrants the individual be issued an identification card.

1.2.7. “Visitor” – Individual that is not a current student, staff, or faculty member, but has legitimate reason to conduct business on campus or participates in university activities and is approved by an authorized approver.

1.2.8. “25Live” – The ECU application used by the Central Reservations Office for scheduling events, classes, meetings, etc. for the university.

2. Security Access

2.1. Building Access

2.1.1. Campus Community Access

2.1.1.1. General Access. There are two types of general access to buildings; access to unlocked buildings and access to locked buildings by ECU 1 Card. Both are associated with a pre-determined time schedule.

2.1.1.1.1. Access to buildings by unlock schedule. Certain university buildings are unlocked per a pre-determined schedule for public access. Time-specific unsecure entry is based on a standard schedule, e.g., regular business hours.

2.1.1.1.2. Access to locked buildings by ECU 1 Card. Certain university buildings remain locked at all times and require valid ECU 1 Card to gain entry and/or access. All valid ECU 1 Card holders are authorized access based on their current status; however, time-specific clearance for entry can be limited to a pre-determined schedule, i.e., regular business hours.

2.1.1.2. After Hours Access. A designated authorized approver can approve non-standard entry access to an individual by submitting an approved security access form request. An authorized approver may not approve his/her own security access form request. For business purpose only, a security access form request can be completed and approved for general building access during non-standard hours, and access to restricted doors or areas of a building, such as clinics, research areas, or warehouses.

2.1.2. Campus Wide Closures and Unique Events.

2.1.2.1. Holidays. The ECU 1 Card office will schedule and configure building closures based on the holidays identified by the university. This will deactivate normal unlock schedules for 1 Card controlled buildings and permit access only to those cardholders with pre-approved access including holiday access. The designated authorized approvers or schedulers may request additional changes as it relates to the operations of their building or area for the specified holiday.

2.1.2.2. Adverse Weather. The ECU 1 Card Office has the ability to secure university doors/facilities during regularly-scheduled hours due to campus emergencies or university closures, such as closures due to weather. The ECU Police Department, Chancellor, Vice Chancellor of Administration and Finance, and Associate Vice Chancellor of Campus Safety & Auxiliary Services level designees have the authority to direct these security measures. The ECU 1 Card office will respond based on the condition level declared for campus: Condition 1, 2 or 3.

2.1.2.2.1. Condition 1 (Reduced Operations). The ECU 1 Card will take no action to normal unlock schedules for 1 Card controlled buildings and access unless otherwise requested by the designated authorized approver or scheduler for 1 Card controlled buildings.

2.1.2.2.2. Condition 2 (Suspended Operations) or Condition 3 (Closure). The ECU 1 Card will schedule and configure building closures for all 1 Card controlled buildings and permit access only to those

cardholders with pre-approved adverse weather access only unless otherwise requested by the designated authorized approver or scheduler.

2.1.2.3. Emergency Event. Events requiring campus-wide closure with restricted access to mandatory employees the ECU 1 Card office will follow outlined procedures for buildings closures and access as identified:

2.1.2.3.1. Building closures for all 1 Card controlled buildings and areas. In the event of a potential threat to campus, ECU 1 Card administrators may deem it necessary to secure campus buildings/departments until ECU Campus Police, Chancellor, Vice Chancellor, and Associate Vice Chancellor of Campus Safety & Auxilary Services notifies and/or confirms ECU 1 Card administrators the campus is “all clear” from the potential threat. The Chancellor, Vice Chancellor of Administration and Finance, or Associate Vice Chancellor of Campus Safety and Auxiliary Services may permit opening of some buildings based on the buildings services or operations.

2.1.2.3.2. Permit access by ECU 1 Card for mandatory and emergency management employees only. Access for non-mandatory cardholders will be retained but will not be active during the emergency event. Pre-determined access specified for each mandatory and emergency management will be activated. Access will be pre-determined and assigned with the mandatory and emergency management employees regular access but will not be active until the emergency event is activated.

2.1.2.4. Campus Lockdown. Events requiring campus-wide closure with restricted access to emergency personnel only due to campus threat or security issue the ECU 1 Card office will follow outlined procedures for buildings closures and access as identified:

2.1.2.4.1. Building closures for all 1 Card controlled buildings and areas. The ECU Police will be the only authorized personnel to request opening of any 1 Card controlled building.

2.1.2.4.2. Permit access by ECU 1 Card for emergency personnel only. Pre-determined access filter levels have been identified in the 1 Card system to restrict access needed by the ECU Police. These access filter levels will be activated as authorized by the ECU Police. The highest access level will be active upon activation of the campus lockdown event permtting access for emergency personnel only. The ECU Police will be the only authorized personnel who may request a change to the access filter level. Access for cardholders will be retained but will not be active during the campus lockdown event.

2.2. Obtaining Access to Secure Areas

2.2.1.1. One-time Access Request. An individual or department administrator can request access to a building/area by submitting an approved security access request form to the ECU 1 Card office. The security access request will consist of an approval of the building/area’s designated authorized approver and identify the business purpose for the requested access.

2.2.1.2. Recurring Access Request. A designated authorized approver for a building/area can request access for groups that may be cross referenced in Banner. These groups may be defined by the parameters including but not limited to the following: course, section, major, class, lab, etc. Access on such recurring access requests will be assigned with an end of semester/year expiration date that shall not exceed one year. Student access is only granted to valid students unless otherwise approved for a specific business purpose.

2.2.1.3. Scheduling Events Requests. A 25Live Scheduler may request a building/department to be unlocked for an event by attaching the “Early Opening/Late Closing” resource to their event within 25Live and specifying the area/time in the special instructions. Buildings/departments not included in 25Live may be requested to be unlocked for an event by the authorized approver and/or authorized scheduler only, by sending requests to the 1 Card Office via email, electronic request form, or other formal request mechanism as directed by the 1 Card Office.

2.3. Configuring Security Access (by 1 Card personnel)

2.3.1. Approved Security Access Forms. Formal written requests that have been approved by the designated authorized approver will be reviewed and access will be configured by the 1 Card Office, provided that the request meets the following criteria:

2.3.1.1. Cardholder's Department. The cardholder's department listed on the approved access request corresponds with cardholder's department in Banner and it is within the approver's area to approve.

2.3.1.2. Cardholder's Type. The cardholder's type listed on the approved access request corresponds with the cardholder's affiliation to the university and the business purpose of the request.

2.3.1.3. Access Requested. The access requested on the approved access request corresponds with business purpose and limits the physical access to include specific access points and time frames.

2.3.1.4. Justification. The justification on the approved access request corresponds with the stated business purpose for the request.

2.3.1.5. Authorized Approval. The authorized approver has successfully approved the access request by including his/her signature in the form of writing, digital, or electronic email approval (depending on the request method that is in place and available at the time).

2.3.2. Expiring Access Request. When in receipt of expiring access requests, the 1 Card office will assign access using a designated expiration date on the access. This will ensure access is automatically deactivated and removed in a timely manner.

2.3.3. Recurring Access Request. All recurring access requests will be assigned with an expiration date to ensure access is deactivated at the appropriate time, such as the end of the semester, year, etc.

2.3.4. Department Access Request. In certain unique circumstances with a justifiable business need, a department may request a card(s) to be assigned to the department (department card) with designated access authority. The department card may be checked out/in to visitors upon arrival to their department/ area, when approved. These requests must be approved by the 1 Card Director or the Associate Vice Chancellor for Campus Safety & Auxiliary Services, or designee, on a case by case basis and will only be approved where unique circumstances justify the need for a departmental card are demonstrated by the requesting unit.All department cards must be kept secured within the department and a corresponding records log must be maintained for each card. Logs are subject to audit by 1 Card Office and/or Internal Audit. Failure to properly maintain logs will result in the confiscation/deactivation of department card(s).

2.4. Removing Security Access

2.4.1. Employment Termination. As part of the exit process resulting from an individual's separation from employment with the university, security clearances for the ECU 1 Card must also be removed. The cardholder's supervisor or unit head is responsible for notifying the ECU 1 Card office in advance, when notice is available or immediately upon notice of separation, in order for access to be removed at the time of the individual's departure. The ECU 1 Card should be collected from the cardholder and promptly returned to the 1 Card office as it is considered university property. Supervisors may consult with the Department of Human Resources, Employee Relations, for questions related to employee separation.

2.4.2. Employment Transfers. As part of the transfer process resulting from an individual transferring to another department within the university, security clearances for the ECU 1 Card must be removed. The cardholder's supervisor or unit head is responsible for notifying the ECU 1 Card office in advance, when notice is available or immediately upon notice of the transfer, in order for access to be removed at the time of the individual's departure. The ECU 1 Card office will notify the cardholder if the transfer of deparmtents requires the reissuance of a new ECU 1 Card. Otherwise, the individuals ECU 1 Card may be retained and used accordingly in the individual's new department. If security access to the new department is needed, a

new security access request form must be completed by the new department.

2.4.3. Temporary Suspension of Access. A supervisor or authorized approver may request access to be suspended from a cardholder for a time frame in which the cardholder no longer has a business purpose for access, to include but not limited to FMLA leave, change in job duties, etc. Supervisors or authorized approvers should contact the Department of Human Resources, Employee Relations, for assistance with such requests. Reinstatement of access will require an updated approver security access form.

2.4.4. Student Deactivation. Student access to facilities is managed through cross-referencing Banner. Student access is only granted to currently registered students unless otherwise approved for a specific business purpose. At any time, student access may be terminated by contacting the 1 Card office. Although an automated report is processed identifying students withdrawn or valid, the 1 Card office should be notified by the department/authorized approver as well.

2.4.5. Visitor Deactivation. Visitor access to facilities will be reviewed routinely by appropriate Authorized Approvers and the 1 Card Office. The 1 Card office will notify and confirm the status of visitors and their need for continued physical access with the sponsoring department contact.

2.4.6. Access Deactivation in receipt of Granted Physical Access Review. The 1 Card office will deactivate access according to confirmation of reviews completed by authorized approvers.

2.4.7. Inactivity Access Removal. The 1 Card office will run and remove access on a routine basis for cardholders that have been granted access to secure areas meeting the inactivity period. Inactivity periods will be determined and set by the 1 Card office.

2.4.8. Miscellaneous Access Removal. The department of People Operations, Success, and Opportunity, Dean of Students, or ECU Police may request access removal of a cardholder when retaining access presents a safety or security concern. These request must be provided in writing via email and copy the ECU Police Chief and Deputy Chief. Due to the nature of this request, the ECU 1 Card office is required to report this information to the ECU Police Chief and Deputy Chief.

2.5. Monitoring Physical Access

2.5.1. Security System vs. Banner Review. The 1 Card office will perform a comparison between cardholders granted access to secure areas and active individuals (students, employees) in Banner on a routine basis in order to confirm cardholders in the security system are currently active in Banner.

2.5.2. Granted Physical Access Reports. The 1 Card office will create and provide granted physical access reports to authorized approvers on a routine basis of individuals who are currently assigned access to their areas. This report will contain all cardholders who have access to a designated building/area and a summary of clearance groups assigned others to complete their job duties (ex. Police, ITCS, Facilities, etc.).

2.5.3. Journal Physical Access Reports. The 1 Card office will create and provide journal physical access reports to authorized approvers on a routine basis of individuals access to high risk areas within their building and/or department. This report will contain door activity transaction history for the assigned secured areas in the building/department to include access granted, rejects, forced/held alarms, and manual actions.

2.5.4. Inactivity Access Reports. The 1 Card office will run and remove access on a routine basis for cardholders that have been granted access to secure areas meeting the inactivity period. Inactivity periods will be determined and set by the 1 Card office.

2.5.5. Authorized Approver and Scheduler Review. The 1 Card office will routinely verify and confirm authorized approvers and schedulers.

2.5.6. Visitor Tracking. The 1 Card office will review system journals to ensure visitor and department cards are being checked in and out daily via routine request of logs and/or reports.

3. Roles & Responsibilities

3.1. Department or Unit Heads

3.1.1. Department/Unit heads are responsible for ensuring that appropriate physical security controls are in place for their units so that personnel and resources are appropriately protected. This includes ensuring that the 1 Card Office is notified timely of any required changes to access, removal of access that is no longer required, or other access or security needs.

3.2. 1 Card Office

3.2.1. The 1 Card Office is responsible for providing reports referenced in this Regulation and tools to Department/Unit heads and their designees (i.e., the Authorized Approvers and Schedulers)

3.2.2. The 1 Card Office shall timely respond to requests from Department/Unit heads, Authorized Approvers, and Schedulers to grant and remove access for individual users.

3.2.3. The 1 Card Office shall monitor other reports and information to detect situations to make best efforts to ensure individual user access is timely removed or updated.

3.3. Authorized Approvers shall perform the following tasks:

3.3.1. Review and approve security access forms to ensure they meet the following criteria before being submitted to the 1 Card Office:

3.3.1.1. Verify Department. The cardholder’s department corresponds the cardholder requesting access and is within the approver’s scope to approve.

3.3.1.2. Verify Cardholder Type. The cardholder’s type corresponds with the business purpose. If a cardholder hold more than one affiliation with the university, select the type that meets the business purpose.

3.3.1.3. Verify Business Purpose. All request must contain a business purpose for the request and justify the need for the request.

3.3.1.4. Verify Access Requested. The access requested must include all areas required and time frame must meet business purpose.

3.3.2. Review reports as specified below and respond in a timely manner to requests for information by 1 Card Office personnel.

3.3.2.1. Granted Physical Access Report. Authorized approvers will review the granted physical access report to verify all cardholders still have a true business purpose to retain access. The Approver will confirm the accuracy of report to 1 Card personnel and/or request removal of access for specified cardholders.

3.3.2.2. Assigned Door Associations Report. Authorized approvers will review the assigned door associations report to verify all groups in which doors are assigned are still accurate and group still has a true business purpose to retain access.

3.3.2.3. Physical Access Report. Authorized approvers will review and use this report to monitor cardholders admits/rejects, door forced/held alarms, scheduled unlocks, etc. for suspicious activity to high risk areas. No response or confirmation is required to 1 Card personnel.

3.3.2.4. Renew Agreement. Authorized approvers will annually renew their agreement with the 1 Card office to ensure the understanding of their role and responsibilities.

3.4. Authorized Schedulers shall perform the following tasks:

3.4.1. Modify Schedules. Authorized schedulers can modify/update schedules for buildings and clearances.

These changes may be permanent operational changes or temporary changes made for events and/or holidays. Schedulers may request these changes through the appropriate scheduling resources (e.g., 25Live, Outlook).

3.4.2. Manage Authorized Personnel. Authorized schedulers will assist the 1 Card office in managing/reviewing the designated authorized approvers and schedulers for their building/department.

3.4.3. Renew Agreement. Authorized schedulers will annually renew their agreement with the 1 Card office to ensure the understanding of their role and responsibilities.