



# Department of Administration

## Office of Information Security

### Operations Standard

Control No.	Rev.	Title	Effective Date	Page
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	1 of 7

#### 1.0 PURPOSE

To establish a standard for the data entry and personnel database management of the Nevada Card Access System (NCAS) physical security management application.

#### 2.0 SCOPE

This standard applies to all state agencies using NCAS to maintain and control physical security access to their offices and facilities.

#### 3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Security Officer (CISO).

#### 4.0 RESPONSIBILITIES

The OIS NCAS Administrator and agency NCAS security administrator(s) have the responsibility to ensure compliance with this standard. The NCAS security administrators are responsible for disseminating this standard and implementation within their units.

#### 5.0 RELATED DOCUMENTS

EITS Security Standard 101, Personnel Security Standard  
EITS Security Standard 109, Physical Access Control and PIV Clearance Standard  
EITS Security Form 111, PIV Card and Access Request Form  
Software House training and user manuals  
EITS NCAS user manuals

#### 6.0 STANDARDS

##### 6.1 GENERAL PROGRAMMING AND ADMINISTRATION

- A. The Office of Information Security (OIS) is responsible for the creation and administration of all partitions operated by EITS OIS.
- B. Participating agencies are responsible to assign a primary and back up administrator to administrate their partition. The back-up administrator should have privileges equal to the primary administrator to perform all functions within NCAS. In the absence of an assigned primary and back up administrator, OIS can provide assistance.
- C. Partitions not administered by EITS OIS are the responsibility of the participating agency. Upon request, OIS will provide assistance with the creation of security objects.
- D. Upon request, OIS will provide NCAS programming and On the Job Training (OJT) for all agencies.



# Department of Administration

## Office of Information Security

### Operations Standard

Control No.	Rev.	Title	Effective Date	Page
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	2 of 7

- E. Programming privileges are assigned based on delegated authority and the principle of least privilege.
- F. Security administrators have delegated authority to administrate all partitions.
- G. Partition administrators are assigned to agencies, to administrate security objects and personnel within their home partition.
- H. Selected partition administrators are assigned to agencies with more than one partition. Selected partition administrators have the same delegated authority as a partition administrator in multiple partitions. Selected partition administrators administrate all security objects and personnel within the selected partitions they are assigned.
- I. Partition coordinators are assigned by selected partitions administrators and partition administrators to manage personnel records and PIV card issuance. Partition coordinators cannot administrate security objects, only personnel records and card issuance.
- J. Partitioned security objects in the NCAS application are security objects that can be viewed, edited, or deleted by selected partition administrators, or partition administrators within their home partition. Please see appendix "A" for list of partitioned security objects.
- K. Non-partitioned security objects are objects that can be viewed, edited, or deleted by all partition security administrators system wide. Please see appendix "B" for a list of non-partitioned security objects.
- L. Partition administrators shall not view, edit, or delete shared partitioned security objects outside of their home partition(s) without permission from the primary partition administrator responsible for the security objects.

#### 6.2 PROGRAMMING STANDARDIZATION AND DATA INTEGRITY

- A. Partition administrators programming the NCAS application are required to standardize all entries to maintain business continuity and data integrity.
- B. Partition administrators shall identify all security objects within their agency partition through the use of a unique abbreviated identifier of their agency name.
- C. Examples of acceptable abbreviated agency names:
  - 1) Department of Public Safety = DPS
  - 2) Enterprise IT Services = EITS
  - 3) Secretary of State = SOS
- D. Programming entries into NCAS that are unique to an agency and a specific division within that agency are required to be identified by an abbreviated agency name,



# Department of Administration

## Office of Information Security

### Operations Standard

Control No.	Rev.	Title	Effective Date	Page
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	3 of 7

abbreviated Division name, and an abbreviated city/region name (if applicable), where the security object exists. Each sub category requires a hyphen separating the Department, Division, and city/region.

E. Example of an acceptable naming convention:

- 1) Department of Public Safety = DPS
- 2) Division of Records and Technology = RT
- 3) Carson City = CC

F. Please see appendix for security objects that require abbreviated names to include Division, and city/region (if applicable).

#### 6.3 PERSONNEL DATA ENTRY

- A. Partition administrators are responsible for the input and auditing of all personnel records within their partition(s).
- B. Each personnel record shall be assigned to an individual to maintain integrity and accountability of each personnel record. This best practice allows the State of Nevada to provide accurate auditing capabilities while protecting State buildings, property, and assets and assists in facilitating a safe environment for all building occupants.
- C. All personnel records must contain the first name, last name, and person type. If a Personal Id agency Verification card (PIV card) is issued the card must have an activation and expiration date. PIV cards should not be issued for a period of time greater than four years or the anticipated retirement date of an employee. Contractor PIV Cards should not be issued greater than the negotiated contract expiration date.
- D. All personnel records must contain the minimum in the user defined fields; Department Name, Job Title, and Division Name. These entries must be verified thru the Division of Human Resource Management ([http://hr.nv.gov/Resources/Class\\_Specifications/](http://hr.nv.gov/Resources/Class_Specifications/)) prior to the NCAS administrator entering them into the drop down window for selection.
- E. Physical access should be granted on the principle of least privilege. This best practice minimizes the unauthorized access to State buildings, property and assets.
- F. The NCAS administrator is prohibited to grant access to any facility, property, or leased buildings without the written consent of the building partition administrator or agency head.
- G. If an employee transfers to another department outside of your partition(s), and remains in state service contact the NCAS administrator and inform the administrator of the transfer. The NCAS administrator will transfer the employee to the appropriate agency and contact the partition administrator of the receiving agency.



# Department of Administration

## Office of Information Security

### Operations Standard

Control No.	Rev.	Title	Effective Date	Page
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	4 of 7

#### 6.4 NCAS CHANGE CONTROL

- A. Participating agencies shall inform EITS OIS of any changes to the Partition Administrator roles and responsibility within NCAS. Upon notice the NCAS administrator will add, edit, or delete partition administrator's privilege(s) as requested by the agency head.
- B. NCAS administration is performed through the use of the NCAS administration and monitoring client applications. The clients connect to the NCAS server through agencies' local LAN and SilverNet. The NCAS server is a shared resource for authorized agencies. This shared resource requires system maintenance and changes based on user requests and system/application updates. Planned outages shall be performed during a service window from 5:00AM-7:00AM daily. During this service window all administration and monitoring client applications should be closed.
- C. Personnel record formats (i.e. drop down browser, tabs, and enumerated fields) requiring modification must be requested in writing (email acceptable) by the partition administrator. Modifications to personnel record formats can only be performed by a NCAS administrator. Modifications to personnel record formats require all administration client applications closed and exited from the NCAS server. Changes will be requested through the EITS helpdesk and be performed during the next available business day.

#### 6.5 PARTITION ADMINISTRATORS

- A. Each agency should have two partition administrators with equal administration privileges appointed by the agency head.
- B. An IntegraScan and finger print FBI background check must be performed on all personnel performing the duties of a partition administrator or selected partition administrator.
- C. Partition administrators are responsible for the data administration and standardization of all security objects and personnel records.
- D. Partition administrators are responsible for assigning NCAS administration and monitoring users within their partition(s).
- E. Partition administrators are responsible for delegating authority to partition coordinators for the data input and issuance of PIV cards.
- F. Partition administrators are responsible for all network connections, TCPIP connections, and agency hardware between NCAS equipment and SilverNet.
- G. Partition administrators are responsible for the installation and updating of all NCAS desktop applications within their partitions.



# Department of Administration

## Office of Information Security

### Operations Standard

Control No.	Rev.	Title	Effective Date	Page
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	5 of 7

#### 7.0 DEFINITIONS/BACKGROUND

**PERSONAL ID AGENCY VERIFICATION CARD** – PIV Card is an identification card with technology encoded or embedded into the cards design through the use of a micro chip, magnetic strip or proximity technology that is used to verify an individual's identification and access on multiple systems. A PIV card can be used as an identification card, physical access control card, and fuel card on state fueling sites and in the future used as a credential to log into IT systems and applications.

**SECURITY ADMINISTRATOR** – This level of administration allows users full access to all windows, menus, and tabs including default templates and allows the security administrators to edit user passwords. If the NCAS application is upgraded in the future, security administrator privilege will have full access to new windows automatically.

**HOME PARTITION** – A home partition is identified by the partition the personnel record is assigned to. All personnel are assigned to one partition and that is considered their "Home Partition".

**PARTITION ADMINISTRATOR** – This level of administration allows users to configure and maintain the common data in the NCAS database to include create, edit, delete, or view data in their home partition.

**SELECTED PARTITION ADMINISTRATOR** – This level of administration allows users to configure and maintain the common data in the NCAS database to include create, edit, delete, or view data in their selected partitions.

**PARTITION COORDINATOR** – This level of coordination allows users to selected windows and menus associated with personnel records and PIV card issuance.

**SECURITY OBJECT** – A security object is an object in the system other than a report or personnel record. Several examples of security objects include doors, inputs, clearances, and areas.

**PARTITION** –A partition in the NCAS System is a segment of the database that is divided into separate groups of security objects and personnel. Partition Administrators/Coordinators are typically assigned one partition known as their "home partition" where they can create and edit data. Security Administrators and Selected Partition administrators are assigned in one partition, but can administrate more than one partition.

#### 8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).



# Department of Administration

## Office of Information Security

### Operations Standard

Control No.	Rev.	Title	Effective Date	Page
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	6 of 7

#### APPENDICES

##### APPENDIX A

- 1) Personnel and personnel groups
- 2) Clearances
- 3) Time Specifications
- 4) Doors and door groups
- 5) Elevators and elevator groups
- 6) Nodes (includes activity printers)

Note: All other security objects are shared with all partition/selected partition administrators. Partition/selected partition administrators have delegated authority to change any non-partitioned security objects outside of their home partition. This administration privilege is a default delegated authority within the CCURE•9000 application by the manufacturer and cannot be changed.

##### APPENDIX B

- |                              |  |
|------------------------------|--|
| a. Areas                     | 10) All group except personnel/door groups |
| b. Badge layouts             | 11) Time Zones (view only)                 |
| c. Events                    | 12) Advanced Process controls              |
| d. Guard Tour                | 13) Communication Ports                    |
| e. Holidays (view only)      | 14) iSTAR Controllers                      |
| f. Holiday lists (view only) | 15) Host modems                            |
| g. Keypad Commands           | 16) NetVue (video tour & video view)       |
| h. Maps                      | 17) RM LCD messages                        |
| i. Recipients                | 18) Reader Status Messages                 |

##### APPENDIX C

- |                         |                            |
|-------------------------|----------------------------|
| a. Configurable Reports | 13) Nodes                  |
| b. Areas                | 14) Page Messages          |
| c. Badge Layouts        | 15) Time Specifications    |
| d. Clearances           | 16) Group                  |
| e. Doors                | 17) APC's                  |
| f. Events               | 18) Communication Ports    |
| g. Guard Tours          | 19) Host Modem             |
| h. Intrusion zones      | 20) iSTAR Cluster          |
| i. Keypad Command       | 21) NetVue                 |
| 10) Maps                | 22) Input                  |
| 11) Output              | 23) RM LCD Messages        |
| 12) Reader              | 24) Reader Status Messages |



**Department of Administration**  
Office of *Information Security*

**Operations Standard**

<b>Control No.</b>	<b>Rev.</b>	<b>Title</b>	<b>Effective Date</b>	<b>Page</b>
146	B	Nevada Card Access System (NCAS) Administration	3/27/2019	7 of 7

<b>Approved By</b>		
<b>Title</b>	<b>Signature</b>	<b>Date</b>
State Chief Information Security Officer (CISO)	Signature on File	3/27/2019
<b>Document History</b>		
<b>Revision</b>	<b>Date</b>	<b>Change</b>
A	05/01/16	Initial Release – Formerly EITS Standard 112
B	03/27/2019	Review and update format and terminology.