AD ASTRA PER ASPERA

Kansas

Office of the Governor

Office of Information Technology Services

POLICY AND PROCEDURE MEMORANDUM
9207.00

Effective Date
06/12/2013

Review Date
06/2014

1.0 SUBJECT: ID Badges/Electronic Card Key Management

2.0 DISTRIBUTION: OITS

3.0 FROM: ____
Anthony Schlinsog, Chief Information Technology Officer

4.0 PURPOSE: The purpose of this document is to provide guidance for issuance of Electronic Card Keys for access to OITS Central Office controlled areas.

5.0 BACKGROUND: The State of Kansas requires the use of access controls to restrict physical access to facilities that house information systems. Without physical access control the potential exists that information systems could be illegitimately accessed and the information within compromised.

Unaccompanied access to these controlled areas will be limited to authorized personnel only and that authorization shall be demonstrated through the use of authorization credentials (badges, identity cards, etc.) that have been issued by the State.

6.0 PROCEDURE:

6.1 ID Badge/Electronic Card Key

6.1.1 ID badges shall be issued by Administrative Services.

6.1.2 Three types of ID badges shall be available:

6.1.2.1 State Employee ID Badge: This badge is issued by the Kansas Highway Patrol and is only issued to State employees. Access to areas using this badge will be determined by the employee's supervisor. Access provided by the badge may be changed as duties change.

6.1.2.2 Visitor ID Badge: Visitor ID badges are used only for identifying visitors; they shall not provide access to any area.

6.1.2.3 Consultant ID: Badge. Managed by Administrative Services this badge is issued by the Kansas Highway Patrol and shall only open office area doors. This badge shall only be issued to authorized consultants, contractors, or vendors. As a standing exception, this badge may also be temporarily issued to an employee that has lost or forgotten their State Employee ID Badge.

6.1.3 ID Badges and Electronic Card Keys: Except for State Employee ID badges, and for the purpose of this Policy and Procedures Memorandum (PPM), all other ID badges and electronic card keys shall be used to identify electronic keys that provide access to controlled areas. These electronic keys shall be used and treated as an ordinary key and managed by local key control procedures.

7.0 Visitors

7.1 Must sign in and out at the reception desk; visitors must have a sponsor; the sponsor will be responsible for ensuring the visitor logs in and out.

7.2 All visitors shall be issued a visitors badge which must be worn at all times.

7.3 No visitor shall have unaccompanied access to any area.

7.4 For further information on visitors refer to the visitor's policy.

8.0 Consultants, Contractors and Vendors

8.1 Consultant ID badges may be requested for consultants performing services that require more than four consecutive hours to complete. Consultant ID badges only open doors to office areas and no others (datacenters, storage areas, frame rooms, etc.)

8.2 For consultants, contractors and vendors that do not maintain a clearance with administrative services, escorts are required for access to any controlled area such as datacenters, storage areas, frame rooms, etc.

8.3 For unaccompanied access to controlled areas the following applies:

8.3.1 Must be working on behalf of a local active where access to a controlled area is required.

8.3.2 Must possess an equivalent OITS security clearance that has been verified by the Office of the CISO, and proof of this clearance is on file with Administrative Services.

8.3.3 Must be on the unaccompanied access roster maintained by Administrative Services

8.4 Non-state employees that have been authorized unaccompanied access to controlled areas shall sign for (card) keys to specific areas from the appropriate key control custodians such as the Network Operations Center (NOC).

9.0 Employees

9.1 Employees shall not share use of their State Employee ID badge.

9.2 For employees that forget their State Employee ID badge, they may temporally sign for a Consultant ID Badge from Administrative services

10.0 Facilities Maintenance Personnel.

10.1 State personnel performing maintenance in controlled areas are also required to possess a security clearance for unaccompanied access. This clearance must be maintained on file with Administrative Services.

11.0 Administrative Services

11.1 Shall be responsible for requesting all badges and card keys.

11.2 Shall be responsible for issuing Consultant ID badges. The following are requirements before a Consultant ID badge is issued.

11.2.1 Issuing a consultant badge to employees requires that employment is verified, and the employee has either lost or forgotten their State issued ID badge.

11.2.2 Issuing a Consultant ID badge to non-state employees requires that an office head has approved a request, for an individual whose services require more than four consecutive hours.

11.3 Shall be responsible for issuing electronic card keys to controlled areas to the NOC.

11.4 Shall be responsible for conducting monthly reconciliation reviews of those authorized unaccompanied access to controlled areas. Records of these reviews shall be maintained on file for six years.

11.5 Shall be responsible for providing the NOC with an “access roster” of those authorized unaccompanied access that may be issued keys to controlled areas.

11.6 Shall conduct quarterly inventories of all electronic card keys issued. Records of these audits shall be maintained for six years.

11.7 Shall be responsible for discontinuing access of any electronic card key or ID badge if lost, missing or stolen.

12.0 Network Operations Center (NOC)

12.1 Shall manage electronic card keys in accordance with local key control policy .

12.2 Shall be responsible for issuing electronic card keys to all controlled areas.

12.3 Shall only issue electronic card keys to authorized persons whose names are present on the access roster provided by Administrative Services.

13.0 HISTORY: This is a new PPM.

14.0 CONTACT PERSON: Public Service Administrator
Office of Information Technology Services
785-296-5501