Policy 8.4	Building Access and Control		
Effective Date: 2/28/12 *Last Amended Date:*	*Applicable Law/Statute:* None	*Source Doc/Dept.:* None/OEM	*Authorizing I.C. Sec:* None

BUILDING ACCESS AND CONTROL 8.4

POLICY

The following policy outlines security measures specifically designed to govern access control to the DuPage County Government Complex. This policy applies compliance and established protocol to minimize the risk associated with intentional or unintentional acts or breaches of access against DuPage County.

ELIGIBILITY

- All employees under County Board jurisdiction including temporary personnel as defined within the policy.

GUIDELINES

A. Control Procedures

In order to effectively manage Access Control to DuPage County Government and to protect the safety of all employees and the visiting public, the following procedures shall be adhered to:

1. All personnel shall be issued an ID card upon hire. An ID card shall consist of a photo ID for identification, and an access card for approved access to the facility.

2. Employees, Vendors and other ID Card Holding personnel must display their ID Cards on their outer-most garment of clothing at all times.

3. It is not permitted to share ID cards, or to “piggy back” into a building or secured area.

4. The Access Control System should contain programming information to limit access areas and timings, as designated by the employees manager.

5. The issued ID card shall contain sufficient information to identify the individual (ie: name, photograph)

6. Security shall be notified of all separations or terminations of employees of temporary workers to deactivate the card. The employee/temporary employee's manager is responsible for collecting the ID card upon separation and returning it to Security.

B. Access Card Issuance

Requests for new ID cards must be accompanied by an "Access Application Form" available from Security.

All requests for the production of a new access card or modification of an existing card shall be provided by:

1. Human Resources or the Employees Manager for new employees,

2. Employees Manager for transferred employees or for current employees requiring access modification

3. Relationship Manager for vendor/contractors

It is the responsibility of Security Services to enter the new employee data into the access control system following the guidelines of the system and this policy.

C. Temporary Personnel/Volunteers

1. In some scenarios, temporary personnel, vendors or volunteers (referred to as temporary employees) may be required to support County operations. Temporary personnel that frequent the Campus or are assigned to the Complex shall be eligible to receive ID cards.

2. The Background color of temporary personnel ID cards shall be different in color than the background of employee cards to easily distinguish them.

3. The manager responsible for the relationship shall complete an Access Application form and authorize the required access. This form shall be provided to Security Services.

4. All temporary cards shall have a maximum length of 90 days prior to automatically expiring. This will ensure limited exposure to temporary personnel who are no longer servicing DuPage County where security has not been notified. In all separations or terminations, Security should be notified.

5. The length of expiry on any temporary card may be extended upon the relationship manager's written approval (ie: e-mail). This extension request will then be filed with the temporary employees original access application form by Security.

6. To simplify the expiration process, all temporary cards shall be set to expire on the last day of the quarter (ie: March 31, June 30, September 30, December 31). Relationship managers will be able to easily identify the first day of each quarter as the date by which authorization extensions are due in to Security.

D. Key Issuance

1. Security shall maintain a listing of issued keys and share this listing with HR on a frequent basis. Facilities Management manages key issuance in some buildings, and their system of tracking and maintaining keys should be identical to Security's.

2. Procedures for issuing keys should mirror that of access control cards, in that an application form for keys should be completed by the employee's manager. The issuance of physical keys should be limited and highly scrutinized, as the management of lost, stolen or unreturned keys is a difficult process.

3. Keys that control the perimeter of any building shall not be issued unless required specifically for an individual's job function, or as approved by the Director of their department. Issuance of such keys will be to departments only – not to an individual, unless approved by the Chief Security Officer. Perimeter keys, when issued, should remain in a departmental lock box or other secure area, and should not be taken home by personnel.

4. Temporary employees, contract employees and/or volunteers shall not be issued keys on a permanent basis. Should physical key use be required to fulfill a job function, keys should be managed within the department and signed in/out to the temporary employee on an as-needed basis.

E. Resignations and Terminations

1. Security shall be notified in writing, where possible, of a termination or separation slated to take place. As this is a sensitive area for HR, Management and the Employee, caution should be used in the handling and timing of the deactivation of terminated employees ID card.

2. Once a termination has taken place, the ID card shall be collected by HR/Management. The ID card shall be returned to Security, and all access to the ID card removed, and the card destroyed.

3. If the terminated employee did not have his/her ID card on their person, HR/Management shall ask that the ID card be mailed back to Security. Security shall be notified, and will remove all access associated with the card.

4. If HR/Management was unable to retrieve the card for any other reason, Security shall be immediately notified, and the above steps shall be followed.

5. Terminated employees should not be allowed back into the workspace following the termination for any reason.

F. Lost or Stolen ID Cards/Badges

1. Access ID cards act as keys, and should be treated as such if lost or stolen.

2. Lost or Stolen badges must be reported to Security immediately. Lost or stolen badges shall have access removed from the card. The “tracking” feature shall be enabled on any lost/stolen card in hopes that any unauthorized use can be discovered by Security personnel and/or CCTV.

3. There shall not be any fee associated with lost or stolen badge/ID cards or keys.

4. If ID card that was lost is later found, it should be turned into security to be destroyed. Employees may not possess more than one ID card.

G. Exceptions

1. Exceptions to policy are not possible, unless approved in writing by the Chief Security Officer.