

**Polk County Government
PHYSICAL SAFEGUARDS
Facility Access Controls
Facilities Security Policy and Procedures**

Policy 603.I

Effective Date: May 17, 2005

Revision Date:

I. Policy

The purpose of this policy is to set forth those procedures and practices necessary to ensure the physical security of plant, property and sensitive information located within Polk County offices, workspaces and grounds.

II. Definitions

Secure space: Work area not open to public access

Public Space: Area where uncontrolled movement of public is authorized

Visitor: Member of the public who is not an employee of the County

Sensitive Information: Medical, financial or other information whose dissemination to the public would be harmful to the County or otherwise protected by state or federal laws (i.e. HIPPA Act of 1996, etc.)

Need-to-Know: Access to sensitive material or knowledge necessary for one's job

III. Visitor Control

While many areas of County buildings are open to the public, care must be taken to safeguard those areas that are not. Any work areas where access is controlled will be labeled as such. Departments requiring signage will contact Buildings and Parks department for assistance.

Employees within County workspaces are required to wear their identification badges at all times, in accordance with County Badge policy 506. Any employee who sees a visitor, an individual they do not recognize, or someone who is not wearing a badge within a secure space will offer assistance to that individual, and determine the reason for their presence. If unauthorized, they are to be escorted back to a public space.

Non-employees are not authorized or permitted within Polk County workspaces after normal working hours.

Specific security procedures more stringent than those set forth in this policy (i.e. Corrections, Sheriff's Department, Child Support, etc.) will be at department discretion.

IV. Access Control

Access control and specific "need-to-know" shall be the responsibility of the department heads and division managers, with coordination through Information Technology Department for computer access and Building and Parks for badge access. All access will be terminated upon change in employment status per County Employee Discipline Policy 716.

V. Office Security

Offices and workspaces, especially secure spaces where sensitive data or valuables are located, must be safeguarded. All spaces will have functional locks, and all spaces are to be secured (locked) when not occupied, even for short periods of time.

Employees should consider security when arranging office furniture; material on desks and work surfaces should not be visible to casual viewers, and care should be taken regarding proximity of work surfaces to outside windows.

Valuables or sensitive material should be stowed in appropriate containers when not actually in use. They should never be left unattended on desktops or in unlocked containers. Sensitive paperwork should be covered with a labeled cover sheet when on workspaces where visitors or others without a valid need-to-know could view them.

Per County Computer Policy 901, computer monitors will not face the public, and employees will have the appropriate screen savers set for the required inactivity intervals.

File cabinets, storage containers, vaults and/or safes holding sensitive or valuable material shall be locked unless actually in use. All locking containers will be locked at the close of business. Office windows will be secured at the close of business.

VI. After-hours

Most employees will require access to work spaces during normal business hours; those whose jobs require flexible hours or who are on call will use the badge-activated entrances as prescribed per Polk County Badge Policy 506. After-hours access to County buildings will be monitored and recorded by Buildings and Parks Department.

Network logon access will be restricted outside of regular business hours by IT Department and individual departments; Department Heads will be responsible for authorizing after-hours access to their workforce who require it, and supplying the authorization list to the Information Technology Department. Any changes to the authorization list must be documented and forwarded to the Information Technology Department.

As previously stated, visitors will not be authorized entry to County spaces outside of normal working hours.

All outside doors will be properly secured after hours. Under no circumstances are doors to be blocked open or left ajar, whether employee or public entrances.

VII. Emergency Procedures

Some “emergency” situations allow for more time than others. Response (i.e. evacuation) to a building fire would likely be more time critical than response to a tornado watch. Safety of the individual is always paramount, but we are still responsible for the security of our workspaces.

In the event of an emergency, attempt to secure your work space as much as practical during departure. At a minimum, lock the door as you exit. If time permits, stow any sensitive information or valuables in

the appropriate containers and ensure that nothing is left out prior to departing the area. Log off and shut down your computer systems.

Please refer to County General County Emergency Plan Policy 501.A for responsibilities and procedures regarding specific emergencies.

Restoration of physical access to County buildings following an emergency or disaster situation will be coordinated by, but not limited to Parks personnel, Information Technology Department, and Law Enforcement. Law Enforcement personnel may be contacted for perimeter security until the situation is resolved.

Building and Parks Department will ensure that emergency systems (i.e. back-up generators, ventilation, water controls, fire alarms, temperature/humidity controls, etc.) remain in good working order, and that any and all maintenance performed on them is recorded and retained, six years within the County, and in accordance with contractor policy, where applicable.

VIII. Sensitive Material Destruction Procedures

All paper waste in Polk County shall be disposed of in accordance with Wisconsin Adm Code NR 544.

Offices or workspaces in which sensitive or protected information is used shall ensure that disposal of that material will be by shredding. Under no circumstances will sensitive material be discarded in the regular recycling waste bins. Individual departments who shred their own material will implement procedures to ensure proper destruction. Those departments using centralized shredding via Building and Parks will use the appropriate shredding containers.

Individual departments desiring to conduct their own shredding should ensure that the shredders they purchase are of the crosscut type, and that they meet or exceed the requirements of any governing laws or regulations.

Some material, such as protected health information (PHI) may require written record of destruction; these records will be the responsibility of the individual departments, and records and retention will be in accordance with the applicable law or regulation. Refer to County Policy 602.T, Disposal Policy and Procedures.

Destruction or disposal of County property other than sensitive data as previously detailed in this destruction shall be in accordance with County Purchasing Policy 912.

IX. Exterior Security

Security measures exterior to County buildings will include alarm systems, lighting, surveillance cameras and motion sensors, as appropriate.

All exterior doors and windows, excepting Law Enforcement's main door, will be locked after hours. Doors not in regular use shall remain secure during working hours, and shall be appropriately posted.

Buildings and Parks Department will make periodic checks of exterior areas to ensure adherence to this policy, both during and after hours.