Policy on Privacy Regarding Information
From Electronic Access Systems for University Facilities

Effective: 8/5/2014
Updated: By Order of Division of Public Safety In Coordination with Business Services Division & Office of Audit, Compliance & Privacy

I. Purpose

The purpose of this policy is to regulate the use, disclosure and handling of information derived from Penn's electronic access systems for University Facilities.

II. Scope

This policy applies to all personnel, schools and centers of the University in the use of electronic door and facilities access systems managed by the Division of Public Safety and Business Services Division. Specifically, the policy covers appropriate use and disclosure of individually identifiable card use (examples: swipe cards, contactless cards) information.

III. General Principles

1. Penn is committed to utilizing technology in facilities access systems in a manner that enhances the safety and security and quality of life of the University community, operating as efficiently as possible, and consistent with the reasonable privacy interests of the Penn community.
2. Penn personnel authorized to use, disclose and handle information obtained from electronic facilities access systems shall do so in a professional, ethical and legal manner.
3. The use, disclosure and handling of information obtained from electronic facilities access systems shall be conducted in a manner consistent with all existing University policies, including the Non-Discrimination Policy, Confidentiality of Student Records, HIPAA-related policies, Open Expression Guidelines and other relevant policies.
4. All personnel with access to individually identifiable information in electronic facilities access services will be appropriately trained and supervised in the responsible use of this technology and information.
5. Violations of this policy may result in disciplinary action up to and including termination, consistent with the rules and regulations governing employees of the University.

IV. General Requirements

1. System Owners
   - A. The Division of Public Safety and the Business Services Division are "owners" of electronic facilities access systems and are responsible for ensuring compliance with this policy. For example:
     - i. The Division of Public Safety is the owner of its electronic facilities access system covering exterior doors to facilities and interior restricted access areas.
     - ii. Business Services- Housing and Conference Services office is the owner of its electronic facilities access system covering access within student residences.
   - B. System Owners have an obligation to ensure, through training programs and other reasonable measures, that individually identifiable information in electronic access systems is used only by authorized individuals or offices for authorized purposes, as described in this policy.
2. Primary Purposes for Use of Electronic Facilities Access Information

It is the expectation that the uses of individually identifiable information from electronic facilities access systems will ordinarily be for the purposes of protecting safety and security of individuals and for the administration of access to housing and other facilities.

3. Safety and Security-Related Purposes

The Division of Public Safety (“DPS”) is charged with protecting the safety and security of Penn’s campus. Accordingly, all electronic access systems must be managed by and/or available to the DPS and under the following conditions:

A. The Vice President for Public Safety is responsible for authorizing the access, use and disclosure of information from electronic facilities access systems, including ensuring the following:
    i. Except as otherwise provided by this policy, DPS may only use information in electronic access systems for safety and security purposes, such as criminal investigations (thefts, etc.), missing person’s reports and safety related issues such as but not limited to remote lockdown or immediate termination of access privileges for named individuals.
    ii. Except as otherwise provided by this policy, DPS will only share such information with authorized offices charged with protecting the safety and security of a member or members of the Penn community, such as the Director of Student Intervention Services.
    iii. Within DPS, access to information will be limited to systems administrators and DPS personnel as necessary for their job function as authorized by the Vice President for Public Safety.

4. Ordinary Administration of Housing and other Facilities Access Services

System Owners may allow authorized individuals to access and use information from electronic facilities access systems for the ordinary administration of their University sanctioned services, consistent with the reasonable privacy interests of individuals whose information is obtained.

For example:

A. The Division of Business Services may use such information as reasonably necessary to detect safety-related issues, administration of room assignments and operational needs, related residential assignments and changes services, to detect abuse of housing services and to audit for no-shows and failures to depart.
B. The Division of Public Safety may share information with designated individuals in the Office of Fraternity and Sorority LIFE (OFSL) for administration of housing assignments under OFSL’s jurisdiction.

5. Protecting the Institution

System Owners may allow individuals and offices charged with protecting the University in claims and related matters – and authorized individuals working with such offices on these matters -- to receive and use information from electronic facilities access systems pertinent to such claims.

For example, System Owners may share information with the Office of Risk Management and/or the Office of General Counsel in connection with claims or other matters related to protecting the institution or its members.

6. University Infraction Investigations

Consistent with Penn’s Policy on Privacy in the Electronic Environment, information from electronic facilities access systems may be used to investigate a suspected violation of law, or a suspected serious infraction of University policy (for example one that threatens the safety and security of an individual of individuals, or alleged misappropriation of University assets), as follows:

A. In the case of an investigation pertaining to faculty misconduct, such use must be approved by the University office charged with the investigation, in consultation with the Office of the Provost or the office of the relevant Dean.
B. In the case of investigating staff, such use must be in connection with an official human resources investigation and/or outcome and approved by the Office of Human Resources or the relevant School Human Resources leadership.

C. In the case of students, such use must be in connection with a sanctioned student conduct investigation and approved by the Office of the Provost or the office of the relevant Dean.[1]

D. In cases where there is a lack of certainty regarding the appropriate approvals individuals should consult the Office of General Counsel or the Office of Audit, Compliance and Privacy.

7. Legal Process. Information from electronic facilities access systems may be used as necessary to comply with legal requirements or process.
8. System Administration. Information from electronic facilities access systems may be used as necessary for maintaining the function and integrity of University computing systems and for ensuring that the system is operating as designed.
9. Consent. In addition, and notwithstanding the above, System Owners may use and share information from electronic facilities access systems consistent with the written, voluntary consent of the individual whose information is at issue.
10. Security of Information. System Owners must ensure that reasonable administrative, physical and technical safeguards are in place to protect information from electronic facilities access systems from unauthorized access, use and disclosure.

V. Questions or Comments

Questions or comments should be directed to the Division of Public Safety, the Division of Business Services, the Office of General Counsel, or the Office of Audit, Compliance and Privacy.

[1] Please see College Houses and Academic Services (CHAS) policy on electronic access requests, available from the Office of the Executive Director.