



Electronic Door Lock Systems Data Policy

Policy Title:

Electronic Door Lock Systems Data Policy

Policy Section:

Responsible Executive(s):

Treby Williams, Executive Vice President

Responsible Office(s):

The Department of Public Safety

Contact(s):

Paul L. Ominsky, Executive Director, Department of Public Safety
pominsky@princeton.edu, (609) 258-6688

Effective Date:

April 16, 2013

Last Updates:

December 12, 2018

.....
I. Policy Statement

This policy defines how data produced by Electronic Door Lock systems is restricted in accordance with the University's Information Security Policy and respect for individual privacy as defined in Rights, Rules, and Responsibilities.

II. Who Is Affected By This Policy

All members of the University community



III. Definitions

“Electronic Door Lock Systems” – Systems that records the time(s) and date(s) that a card has been used to enter, and in some instances to leave, certain buildings and/or facilities on campus.

“Data” – information produced through the routine operation of the Electronic Door Lock Systems. This information may include time and date of entry; a unique identifier that identifies the owner of the card; location of entry.

IV. Policy

Electronic Door Lock systems store **“Data”** on University Servers. Access to the Data shall be restricted in accordance with the University’s Information Security Policy and respect for individual privacy. University personnel who manage Electronic Door Lock systems shall have access to the Data only as necessary to administer and evaluate the Electronic Door Lock systems and to fulfill requests approved by the Executive Director of Public Safety. University personnel authorized to access Data for these purposes are required to secure such Data appropriately and may not disclose the Data except as instructed by the Executive Director of Public Safety.

Use of Data in a way that targets one or more identifiable individuals shall be permitted only for the following purposes:

- To investigate breaches of building security, serious violations of University policy, and crimes and for related external or internal proceedings.
- To respond to security alerts and to address other emergencies.
- To monitor access, audit and/or manage internally secured spaces, inventory and other resources, as required for internal control, governmental regulations, or other legitimate business purpose.

University personnel authorized to use Data for any of the above purposes should submit their request to the Executive Director of the Department of Public Safety, who exercises discretion to approve/modify requests, in consultation with the Office of the General Counsel and/or the appropriate Information Guardian as defined under the Information Security Policy.

In the event the University is served with a properly issued subpoena or court order compelling the disclosure of personally identifiable data, the University will make reasonable efforts to give advance notice to the relevant individual, provided that such notice is practicable and permitted under the law. This Policy does not indicate that the



University considers these records to be education records, but focuses on securing the records, rather than defining privacy practices.

V. Procedures

VI. Related Documents and Forms

VII. Roles and Responsibilities

<i>Executive Director Department of Public Safety</i>	<i>In consultation with the Office of General Counsel, exercise discretion to approve/modify requests for door access Data that identifies individuals</i>
<i>Staff administering Access Systems</i>	<i>Maintain Data from Electronic Lock Systems and secure the Data appropriately; produce specific Data for legitimate requests approved by Executive Director of Public Safety</i>
<i>University personnel</i>	<i>Submit requests for Data to Executive Director, Department of Public Safety</i>

VIII. Related Policies

Princeton University Information Security Policy

<http://www.princeton.edu/oit/it-policies/it-security-policy/>

Princeton University Rights, Rules, Responsibilities

<https://rrr.princeton.edu/>

IX. Update Log

April 16, 2013 - CACS Privacy Policy updated to Electronic Door Lock Systems Data Policy

December 12, 2018 - Roles and responsibilities