Institutional Data Council

Issue Decision Summary Report:
AggieAccess Data Access

May 2022

Introduction

The AggieAccess system handles electronic access control to campus facilities in a platform used across the UC Davis campus, with central management at the Police Department and Admin IT in FOA.

The IDC initially was asked to consider three governance questions related to AggieAccess data usage:

1. Access Report: Can AggieAccess provide a report listing who has access to campus facilities to those who are responsible for managing access?
2. Automated Reporting (API Usage): Can the access list be maintained programmatically using the vendor provided API?
3. Logging Data: How can AggieAccess logging data be used (i.e., standalone or in combination with other data sources)?

Summary of Findings

1. The AggieAccess system contains highly sensitive (P4-level) data so it was carefully designed for data security and approved by the campus Information Security Office (ISO).
2. AggieAccess uses badges (ID cards) to look up access permissions to campus buildings.
3. IET manages the campus's Identity & Access Management system, and those IDs are linked to badge IDs, with ISO approval, so that badges are individually identifiable for faculty, staff and students.
4. Badge holder access control data, primarily building entry and exit transactions, are governed by PPM policy 360-50, IV.B.
5. Key card and electronic access control is covered by PPM policy Section 360-50, III.D.2 and 4, which states that departments or organizations assigned space in a building are responsible for enabling and disabling electronic access to their assigned spaces.
6. The UCD Police Department, as the AggieAccess system owner, anticipates questions regarding appropriate use of system data beyond its primary purpose of controlling building access. This includes long-standing uses, electronically replicating what UC Davis did in the past with physical keys, and novel uses enabled by electronic records of building entry and exit transactions linked to individuals.
7. The issue raised was whether building owners are allowed access to AggieAccess data that was previously provided for physical key data, particularly data regarding who is currently authorized for access to their building.

Decisions

1. Reporting Who Has Access – initial Use Case: The IDC and ISO recommend that AggieAccess provide the building owner with a daily report of active ID card numbers for their constituents: students, faculty and staff. Data will include who is currently authorized to access their facilities (IMID, BadgeID, IssueCode, BadgeStatus, ActivateDate, DeactivateDate, LastPrinted), securely transferred by Admin IT to the requesting unit to load into local systems. This access will be approved by the UCPD Chief, the AVC Admin IT, and the campus CISO (security oversight).
2. Future Reporting Use Cases: The IDC recommends blanket approval for similar requests in the future, to only require review and approval by the three roles identified above: UCPD Chief, AVC Admin IT, and CISO.
3. Use of the AggieAccess Vendor API: The IDC recommends limited use of the AggieAccess Application Programming Interface (API) to automate the use case described in the first recommendation. Specifically, campus units who are responsible for managing access may implement an API interface to AggieAccess subject to the following constraints:
    a. The access is approved by the UCPD Chief, the AVC for Admin IT, and the campus CISO
    b. AggieAccess API usage is limited to the purpose of reporting who has access and updating access by the responsible campus units
    c. The AggieAccess API is approved by the UC Davis Information Security Office (ISO) as a secure implementation and means for accessing sensitive information
    d. Campus units will review their specific programmatic interface with their UISL as well as the identified data stewards and the ISO
4. Potential Future Use Cases Involving Integrating Logging Data: The Institutional Data Council, in consultation with the original requestor, have agreed to address new use cases for AggieAccess as they arise rather than in advance. Standard use cases can follow the existing process for requesting approval from the Data Proprietors identified in the first recommendation. The Data Proprietors may opt to engage the IDC in the future for unique or complex use cases, especially those involving integrating data sources with AggieAccess logging data.