ASD INTERNAL AUDIT REPORT

2020-03

Building Access Controls

Anchorage School District

November 12, 2020

MUNICIPALITY OF ANCHORAGE
Internal Audit Department
632 W 6th Avenue, Suite 710
P.O. Box 196650
Anchorage, Alaska 99519-6650
www.muni.org/departments/internal_audit

INTERNAL AUDIT DEPARTMENT
Michael Chadwick, CIA, CICA
Director
Phone: (907) 343-4438

E-Mail: michael.chadwick@anchorageak.gov

Municipality of Anchorage

Austin Quinn-Davidson
Acting Mayor

Internal Audit Department

November 12, 2020

Anchorage School District Superintendent and Members of the School Board:

I am pleased to present for your review **ASD Internal Audit Report 2020-03; Building Access Controls; Anchorage School District**. A brief summary of the report is presented below.

We have completed an audit of Building Access Controls at the Anchorage School District. The objective of this audit was to determine if there were adequate controls over building access. To accomplish our objective, we reviewed policies and procedures related to building access to determine if the policies and procedures were being enforced. In addition, we reviewed records of keys and fobs issued to employees and contractors.

Our audit revealed that controls over building access can be improved. Specifically, we found three different versions of the Key Control Procedure being used by schools and departments and the Anchorage School District's Key Distribution Plan was not always followed. Moreover, the key database maintained by the Maintenance Department was inconsistent, outdated, incomplete, and inaccurate. Furthermore, lost or stolen keys were not always reported to the Security and Emergency Preparedness Department; information regarding investigations of lost and stolen keys was not readily available; and the Maintenance Department reissued lost or stolen keys without coordinating with the Director of the Security and Emergency Preparedness Department to ensure that a lost/stolen key investigation report had been completed. In addition, assigned employee access privileges did not always match the requirements found in the Fob Control Procedure; building access was not always removed for terminated employees having fobs; and the Security and Emergency Preparedness and Maintenance Departments did not have accurate records of fobs issued to employees. Finally, lost and stolen fobs were not always reported by Anchorage School District staff to the Security and Emergency Preparedness Department.

There were ten findings in connection with this audit. Management was responsive to the findings and recommendations.

Michael Chadwick, CIA, CICA
Director, Internal Audit

Municipality of Anchorage

Austin Quinn-Davidson
Acting Mayor

Internal Audit Department

November 12, 2020

ASD Internal Audit Report 2020-03
Building Access Controls
Anchorage School District

Introduction. The Anchorage School District's (District) Maintenance Department (Maintenance) provides a wide variety of services to support the District's mission of educating students. Among the many services provided are maintaining lock and key systems to control access to the District's more than 100 buildings. There are two types of access controls employed by the District: traditional key and lock systems and electronic fob devices that are used in place of a traditional key to unlock a door. Traditional locks are installed, and keys are cut and issued by Maintenance staff for most buildings. Some buildings have electronic fob systems where a device reader is installed, and a fob is used for building access. Schools and departments are issued a stock of keys and fobs from Maintenance. As new employees are hired, the schools and departments issue stock keys and/or fobs to employees. When fobs are issued, employee information is sent to Maintenance so that the fob can be activated with the appropriate building access. In addition, keys and fobs are issued to contractors performing building repairs and maintenance. Keys and fobs for the contractors are requested by Capital Planning and Construction Department staff and should be returned when the jobs are complete.

According to District staff, building access can be deactivated quickly with fobs, in cases of loss or theft, and upon employment termination. However, when keys are lost or stolen, a risk assessment must be performed to decide if building locks need to be rekeyed since rekeying buildings is a time consuming and costly process. The Security and Emergency Preparedness Department (Security and Emergency Preparedness) provides oversight and approval for the issuance of keys and fobs after loss and theft. In addition to other duties, Security and Emergency Preparedness is the "proponent" for the key control and fob control procedures.

Objective and Scope. The objective of this audit was to determine if there were adequate controls over building access. Specifically, we reviewed policies and procedures related to building access to determine if the policies and procedures were being enforced. In addition, we reviewed records of keys and fobs issued to employees and contractors.

The audit was conducted in accordance with generally accepted government auditing standards, except for the requirement of an external quality control review, and accordingly, included tests of accounting records and such other auditing procedures as we considered necessary in the circumstances. The audit was performed during the period of December 2019 through March 2020, however completing the report was hindered by the COVID-19 pandemic. The audit was requested by Anchorage School Board Finance Committee.

Overall Evaluation. Controls over building access can be improved. Specifically, we found three different versions of the Key Control Procedure being used by schools and departments and the District's Key Distribution Plan was not always followed. Moreover, the key database maintained by Maintenance was inconsistent, outdated, incomplete, and inaccurate. Furthermore, lost or stolen keys were not always reported to Security and Emergency Preparedness; information regarding investigations of lost and stolen keys was not readily available; and Maintenance reissued lost or stolen keys without coordinating with the Director of Security and Emergency Preparedness to ensure that a lost/stolen key investigation report had been completed. In addition, assigned employee access privileges did not always match the requirements found in the Fob Control Procedure; building access was not always removed for terminated employees having fobs; and Security and Emergency Preparedness and Maintenance did not have accurate records of fobs issued to employees. Finally, lost and stolen fobs were not always reported by District staff to Security and Emergency Preparedness.

FINDINGS AND RECOMMENDATIONS

1. Inconsistent Key Control Procedures.

a. **Finding.** We found three different versions of the Key Control Procedure being used by schools and departments. The latest version was updated effective August 15, 2019, and was distributed to principals and front office staff. However, some staff we interviewed stated that they had not received the most current version while others stated they had received it, but chose not to use it. Reasons stated for not following the procedure were that the process was repetitive, requiring the same information on three different forms, too time consuming, and since there was no oversight or enforcement, they didn't see it as a good use of their time. A Key Control Procedure cannot be effective if a uniform version is not formally approved, fully distributed, and enforced.

b. **Recommendation.** The Director of Security and Emergency Preparedness should:

1) Review the Key Control Procedure and make any needed updates.
2) Ensure that the Key Control Procedure is distributed to all appropriate staff.
3) Consider conducting periodic audits to ensure compliance.

c. **Management Comments.** Management concurred and stated,

"1) Key and Fob Control Procedures will be updated after completion of the Audit with changes made due to our newest Access Control selection which was officially selected October 2020.

"2) Will work with Education Directors for distribution to ensure proper dissemination and compliance.

"3) Will provide guidance to front office staff during Clerical Advance."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

2. Key Distribution Plan Not Followed.

a. **Finding.** The District's Key Distribution Plan was not always followed. The Key Distribution Plan outlines the type and number of keys to be issued. Although the Key Distribution Plan limited elementary schools to only 10 front door keys, one elementary school we visited had been issued 43 front door keys and another elementary school had been issued 35 front door keys. In the summer of 2019, Security and Emergency Preparedness, working with Maintenance, tried to reduce the number of keys issued to schools based on the Key Distribution Plan. However, this reduction in keys met with resistance from some District staff.

b. **Recommendation.** The Director of Security and Emergency Preparedness should ensure compliance with the Key Distribution Plan and may want to consider revising the Key Distribution Plan in consultation with stakeholders.

c. **Management Comments.** Management concurred and stated,

"1) The Key Distribution Plan will be updated to reflect keys provided based on positions opposed to a number per school.

"2) Transition to fobs will mitigate the need for key distribution at schools."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

3. Inaccurate Key Database.

a. **Finding.** The key database maintained by Maintenance was inconsistent, outdated, incomplete, and inaccurate. For example, sometimes the database indicated the individual who received the key. However, in other cases the database showed the Principal as having all the keys for the school. For instance, the database indicated one high school principal having 1,282 keys, with some of the keys being issued before the

principal started working for the District. In another case, the database revealed one elementary school with 201 keys, but records at the school only accounted for 35 keys. In another instance, one employee terminated employment with the District in 2014, but the database showed the employee as having a key. According to the former employee, the key had been returned years ago. When we asked for a copy of the key database, we discovered that it contained over 40,300 lines of data, yet the District only has about 8,000 part-time and full-time employees.

Part of the reason the key database is inaccurate is because there is no process to notify Maintenance when keys are assigned, reassigned, lost, or stolen. For example, when employees received keys, they should have signed a Key/Fob Agreement. The Key/Fob Agreement states that the completed forms are sent to Security and Emergency Preparedness. However, nothing directs Security and Emergency Preparedness to provide this form to Maintenance to update the database. As a result, there was no accurate record of keys currently in circulation that belong to District buildings.

b. **Recommendation.** The Maintenance Director should:

1) Clarify the process of notifying Maintenance when keys are assigned, reassigned, lost, or stolen.

2) Annually provide to each school or department a list of keys to reconcile to school/department records to help ensure the accuracy of the key database.

c. **Management Comments.** Management concurred and stated,

"1) Transition to fobs will allow an opportunity to rekey exterior doors, which will effectively cancel out all current front door access keys, and provide overall better management of key distribution, collection, and inventory."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

4. Lost or Stolen Keys Not Always Reported.

a. **Finding.** Lost or stolen keys were not always reported to Security and Emergency Preparedness. Security and Emergency Preparedness' web page has a form link to report lost or stolen keys. However, Security and Emergency Preparedness staff was not able to provide a list of stolen or lost keys. Instead of using the form, we were told by some school staff that they send an email to Risk Management and/or Security and Emergency Preparedness regarding the lost or stolen key or sometimes they do not report the lost/stolen key at all. Sometimes these emails are forwarded to Maintenance. Maintenance staff estimated 15 keys are reported lost or stolen each year.

b. **Recommendation.** The Director of Security and Emergency Preparedness should remind District staff of the importance of timely reporting lost and stolen keys.

c. **Management Comments.** Management concurred and stated,

"1) Process for lost keys will be reviewed, updated, and distributed to schools appropriately.

"2) Transition to fobs will alleviate the high number of lost keys per year."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

5. Investigation Information Not Readily Available.

a. **Finding.** Information regarding investigations of lost and stolen keys was not readily available. According to the Key Control Procedure, the Director of Security and Emergency Preparedness maintains copies of completed investigations and reissues keys based upon investigation outcomes. However, when we requested copies of the investigations, Security and Emergency Preparedness staff stated that recently completed investigations were not readily available and prior year investigations had

been destroyed. When we asked who should conduct the investigation, we were told by Security and Emergency Preparedness staff that principals and department leads are responsible for completing investigations.

b. **Recommendation.** The Director of Security and Emergency Preparedness should maintain copies of completed investigations according to its Key Control Procedures.

c. **Management Comments.** Management concurred and stated,

"1) This was a new process established after the key audit in 2019. Security & Emergency Preparedness only investigates lost or stolen front door or master keys. All Security & Emergency Preparedness investigates is whether or not to reissue a key; the investigation of how or when the key was lost is done at the school level."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

6. **Keys Reissued Without Verification of Lost/Stolen Report.**

a. **Finding.** Maintenance reissued lost or stolen keys without coordinating with the Director of Security and Emergency Preparedness to ensure that a lost/stolen key investigation report had been completed. Supervisors can request replacement keys by submitting a work order or emailing Maintenance directly. Currently, no review or approval is obtained from Security and Emergency Preparedness, so keys may be issued whenever requested. The Key Control Procedure states that the Director of Security and Emergency Preparedness makes the final determination on lost and stolen keys and authorizes them to be reissued based on the outcome of the investigations.

b. **Recommendation.** The Maintenance Director should obtain authorization from the Director of Security and Emergency Preparedness prior to reissuing lost/stolen keys as required in the Key Control Procedure.

c. **Management Comments.** Management concurred and stated,

"1) This process is in place as of August, 2019 and has been functioning appropriately."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

7. Fob Access Privileges Sometimes Inconsistent.

a. **Finding.** Assigned employee access privileges did not always match the requirements found in the Fob Control Procedure. It was unclear why these access privileges did not match the Fob Control Procedure. For example, did principals or staff ask for different access privileges or were older fobs provided to employees without being updated? The Fob Control Procedure provides the days and hours that various positions can access District facilities. The following table contains some examples where employee access privileges did not match the Fob Control Procedure.

Employee	Position	Fob Access That Was Granted	Fob Access That Should Have Been Granted
Employee 1	Elementary Noon Duty	M-Sun 3 p.m. – 10 p.m.	6:30 a.m. - 8:30 p.m.[1]
Employee 2	Secondary Noon Duty	M-F 6:30 a.m. – 10 p.m. and Sat-Sun 8:00 a.m. – 4 p.m.	M-F 6:30 a.m. – 10 p.m. and Sat 8 a.m. - 4 p.m.
Employee 3	Teacher	6 a.m. - 9 p.m. 7 days	6:30 a.m. – 8:30 p.m.[1]
Employee 4	Counselor	6 a.m. - 9 p.m. 7 days	M-F 6:30 a.m. - 10 p.m. and Sat 8 a.m. - 4 p.m.
Employee 5	Secretary	6 a.m. - 9 p.m. 7 days	6:30 a.m. - 8:30 p.m.[1]
Employee 6	Secretary	7 Days a Week 24 Hours a Day	6:30 a.m. - 8:30 p.m.[1]

[1]The Fob Distribution Plan only provided the hours of access, but no days of access for elementary schools.

Source: Auditor Analysis of fob data provided by the Maintenance and Information Technology Departments.

b. **Recommendation.** The Director of Security and Emergency Preparedness should coordinate with the Information Technology Department to conduct periodic audits to ensure that fob access privileges match the privileges in the Fob Control Procedure.

c. **Management Comments.** Management concurred and stated,

"1) The most recent access control vendor selected will fix this issue. All access times are tied to job titles based on HR systems. They will not be able to be changed manually. New vendor, Openpath, was selected October 2020 and will be in 7 schools by December 2020 and priority is to transition schools and buildings on old access control systems prior to installing in non-fobbed schools."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

8. Fobs Not Always Deactivated.

a. **Finding.** Building access was not always removed for terminated employees having fobs. We found over 900 terminated employees whose fobs were still active, and we were not able to verify if the fobs were returned. If the fobs were not returned to the school/department when employment ended, these individuals can still enter buildings. There was no process to deactivate fobs upon employment termination, such as a termination checklist, and there was no guidance in the Fob Control Procedure to ensure that fobs for terminated employees were deactivated.

In addition, employees hired using a Special Activity Agreement, such as coaches and extra class help, may receive fobs for school access. The Special Activity Agreements specified employment dates and were valid for the school year. However, the Special Activity Agreement termination date was not used when assigning school access with a fob. For example, we found one such employee with an active fob, but the agreement ended two years ago.

b. **Recommendation.** The Director of Security and Emergency Preparedness should update the Fob Control Procedure and Fob Distribution Plan to address the deactivation of fobs. In addition, for employees hired using a Special Activity Agreement, since the dates of employment are known when entering into the agreements, they should be used when assigning and programming fobs.

c. **Management Comments.** Management concurred and stated,

"1) The most recent access control vendor selected will fix this issue. As soon as an employee is removed from the HR system, the fob will be deactivated immediately.

"2) Special Activity Agreement fobs will have start and end dates and will shut off automatically after the end date."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

9. Inaccurate Fob Inventory.

a. **Finding.** Security and Emergency Preparedness and Maintenance did not have accurate records of fobs issued to employees. Stocks of fobs were given to schools and departments to issue to employees. When an employee received a fob he/she should have completed and signed a Key/Fob Agreement form and a Key/Fob Control Registry which were then sent to Security and Emergency Preparedness. However, Security and Emergency Preparedness did not always receive these forms. Instead, Maintenance may have been notified by email.

In addition, when an employee terminated and returned a fob, it may have been issued to another employee without being reprogrammed with new access privileges. The information regarding the fob transfer to another employee may or may not have been sent to Security and Emergency Preparedness to update their records. For example, there was an active fob listed for an elementary school employee who terminated in May 2018, but the fob was recorded being used in March 2020. We confirmed with the school that the fob had been provided to another employee. In another case, 14 fobs were not deactivated at one elementary school when employees were terminated, but were reissued to other staff without letting Maintenance know of the changes. The Fob Control Procedure does not provide any guidance regarding what happens to a fob when an employee transfers or terminates employment with the District.

b. **Recommendation.** The Director of Security and Emergency Preparedness should:

1) Ensure that the Key/Fob Agreement and Key/Fob Control Registry forms are used as required by the Fob Control Procedure.

2) Consider revising the forms to eliminate duplicate information.

c. **Management Comments.** Management concurred and stated,

"1) Security & Emergency Preparedness took over the fob process Summer 2019. Schools on existing systems were operating under no overall program guidance and were managing at their own levels. This will be fixed once all schools are transitioned over to the new selected vendor, Openpath. Transition is currently ongoing."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

10. Lost and Stolen Fobs Not Always Reported.

a. **Finding.** Lost and stolen fobs were not always reported by District staff to Security and Emergency Preparedness. Specifically, when we compared the list of active fobs to school and department records, we found that some District employees had lost their fobs and had them replaced at the school level. According to the Fob Control Procedure the Director of Security and Emergency Preparedness reissues fobs based on the outcome of investigations. However, Security and Emergency Preparedness staff were unable to provide any completed investigations.

b. **Recommendation.** The Director of Security and Emergency Preparedness should:

1) Remind staff of the importance of reporting lost and stolen fobs.

2) Ensure that investigations are completed for each incident.

3) Periodically monitor active fobs to identify multiple fobs issued to employees and follow up to understand why they have multiple fobs.

c. **Management Comments.** Management concurred and stated,

"1) We will be able to pull these reports with the new selected access control vendor.

"2) Will work with Education Directors for proper dissemination of Fob Procedures to include process for lost fobs."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

Discussion With Responsible Officials. The results of this audit were discussed with appropriate District officials on June 24, July 8, and September 9, 2020.

Audit Staff:
Dawn Brown