Audit of Badge Access (DPW-Controlled)

City of Milwaukee

Internal Audit Division

September 2021

Agenda

- Scope
- Objectives
- Procedures
- Conclusion
- Findings
- Next Steps

Audit Scope

The scope of this audit includes DPW-controlled badge access. Specifically included in the scope are:

- All individuals with current access* to DPW-controlled spaces.
- Transferred employees between departments within the period HRMS data is available.

Specific exclusions from scope are:

- MPD, MFD, ERS, and Library-controlled badge access.
- Transferred employees between departments prior to the period of HRMS data availability.
- Access within departments.

* As of April 19, 2021 audit kickoff

Audit Objectives

- Determine if terminated employees and other individuals who should not have badge access do not have badge access.
- Determine if transferred employees between departments within the period HRMS data is available have had badge access to their former departments removed.
- Assess the root cause of process deficiencies for departments with significant badge access issues identified.

Audit Procedures

Audit activities consisted of:

- Process walkthroughs
- Observations
- Review of policies and procedures
- Testing of controls

Audit Conclusions

Opportunities exist to reduce inappropriate and unnecessary badge access to DPW-controlled spaces. Personnel responsible for badge access management are relatively new to their roles and have made demonstrable progress. However, there remain significant opportunities for a more understood, thorough, systematic, and sustainable process.

Audit Finding #1: Department Head Access Reviews

- Finding: The access of former employees is not always terminated timely. Additionally, employee ID numbers are not consistently entered and employee departments are often outdated in the badge access system.

- Risk: Individuals could gain access to a space to which they should not have access. *Risk Rating: High*

- Recommendation: Send badge access lists to department heads at least annually and require the department heads confirm whether the employee is an active employee within their department and enter any incomplete information. Utilize updated lists for more efficient termination audits.

Audit Finding #2: Departmental Manager Guidance

- Finding: There is no comprehensive document to provide to departmental managers under the DPW badge access umbrella with guidance on their role in badge access creation, access changes, information changes (e.g., name changes), reactivation, and return.

- Risk: Inconsistent execution of creation, access changes, information changes (e.g., name changes), reactivation, and return of badges due to lack of understanding of the process by management of the departments under the DPW badge access umbrella. *Risk Rating: Medium*

- Recommendation: Create and distribute comprehensive guidance to provide to managers under the DPW badge access umbrella regarding their responsibilities for creation, access changes, information changes (e.g., name changes), reactivation, and return of badges. The guidance should be reviewed by DPW badge access management at least annually.

Audit Finding #3: Policies and Procedures

- Finding: Internal (i.e., DPW badge access group) policies and procedures do not exist for badge processes.

- Risk: Lack of policies and procedures could result in inconsistent execution of responsibilities. *Risk Rating: Low*

- Recommendation: Document internal policies and procedures for badge creation, access changes, information changes (e.g., name changes), deactivation, reactivation, retrieval, redeployment, and disposal. Policies and procedures should be reviewed annually and signed as evidence of review.

Audit Finding #4: Clearance Space Access Reviews

- Finding: Badge clearances do not have owners identified or descriptions of what they are protecting.

- Risk: Access to clearance spaces may be inappropriate. *Risk Rating: Low*

- Recommendation: Identify owners for each clearance group and have the owners review the access list for appropriateness at least annually. Fill in the badge system with notes about what the clearance is protecting.

Audit Finding #5: Inactivity Deactivation Setup

- Finding: Inactivity deactivations are not consistently set up in the badge access system.

- Risk: Unused cards can be found and used by unauthorized people. *Risk Rating: Low*

- Recommendation: Inactivity deactivations should be consistently set up in the badge access system.

Next Steps

Phase 1

- Auditee will execute audit finding remediation action plans

Phase 2

- Internal Audit will solicit audit finding remediation progress updates at least annually

Phase 3

- Internal Audit will report remediation status to the F&P committee annually until fully executed

Thank You.

Charles Roedel CPA, CIA
Charles.Roedel@Milwaukee.gov

Brenda Koehler CISA, CISM
Brenda.Koehler@Milwaukee.gov

Nuducha Yang
Nuducha.Yang@Milwaukee.gov