WaterISAC Physical Security and Resilience Advisory Committee Fact Sheet

KEYS & LOCKS: THE OVER-LOOKED SECURITY RISK

Robust key and lock systems are essential for mitigating physical security threats at water and wastewater utilities, where unauthorized access to sensitive assets can pose serious risks to public safety and operational integrity. Keys and locks form the foundation of physical security, yet they are often overlooked in favor of electronic solutions. Understanding how your key system is structured—whether it uses restricted keyways, master key hierarchies, or standard locks—is critical to reducing vulnerabilities.

Poor key control can lead to unauthorized duplication, lost keys, and uncontrolled access, creating significant security gaps that can lead to service disruption, equipment damage, contamination, or intentional sabotage. This is especially important for geographically dispersed assets like remote pump stations, which may be vulnerable due to limited on-site staffing or perimeter security barriers.

Strong, well-managed locking systems serve as a primary barrier against malicious actors by ensuring that only authorized personnel can access sensitive areas. When combined with clear key access control policies these systems reduce the risk of insider threats and prevent lost or stolen keys from being exploited. A well-managed key program, supported by strict issuance policies, secure storage, and regular audits, ensures accountability and strengthens an organization's overall security posture.

To assist water and wastewater utilities in improving their keys & locks management strategies, WaterISAC's Physical Security and Resilience Advisory Committee has developed the following best practices.

Key Management Best Practices

1. Identify Your Key System

- ☑ **Standard Lock-and-Key –** Each lock has its own unique key. Simple but hard to manage at scale—requires multiple keys for multiple doors.
- ☑ **Master Key System –** One key (master) opens multiple locks while individual keys open specific doors. Convenient but risky if a master key is lost.
- ☑ **Restricted Keyway System –** Patented key designs that cannot be duplicated without authorization. Strong control over key copies.
- ☑ **High-Security Key System –** Combines restricted keyways with advanced mechanisms resistant to picking, drilling, and bumping. Often UL 437 or ANSI/BHMA Grade 1 certified.

2. Implement a Formal Key Control Policy

- ☑ **Define who can approve key issuance –** Designate specific roles (e.g., Utility Director, Operations Manager, Security Manager) authorized to approve key issuance, clearly document approval authority levels, and prohibit informal or verbal approvals. Approvals must come from designated authorities only.
- ☑ **Require written or electronic approval for every key request –** Mandate that all key requests be submitted through a standardized form or electronic system.
- ☑ **Limit access based on job role and operational need –** Apply the principle of least privilege—employees receive only the keys necessary to perform their job duties. Restrict master key access to a minimal number of trusted personnel and implement temporary or time-limited access for contractors.

3. Maintain a Key Issuance Log

- ☑ **Track all keys issued, returned, and approved –** Maintain a centralized key issuance log, either electronic or hard copy, managed by a designated key control authority.

>>>

4. Duplication Restrictions

- **Prohibit unauthorized duplication –** Require key holders to acknowledge duplication restrictions in writing as part of a key custody or access agreement.
- **Use restricted key systems requiring manufacturer authorization –** Implement restricted or patented key systems where feasible and periodically review restricted key system status to ensure patents remain valid and duplication controls are still enforced.
- **Emerging Risk: 3D-printed keys—avoid sharing key images –** Prohibit sharing, posting, or transmitting key images and educate employees on the risks associated with digital key replication.

5. Lost or Stolen Key Protocol

- **Immediate reporting requirement –** Require employees and contractors to report lost or stolen keys immediately upon discovery, regardless of time or day.
- **Documented steps for re-keying affected locks –** Establish predefined criteria for determining when re-keying is required and update key issuance logs and access records immediately following re-keying.
- **File incident reports for accountability –** Require a formal incident report for every lost or stolen key and review incidents to identify systemic issues.

6. Secure Storage

- **Store spare and master keys in locked cabinets or electronic key management systems –** Prohibit storing keys in unsecured locations such as desks, drawers, or vehicles and label keys using unique identifiers rather than facility names or door descriptions to reduce risk if accessed improperly.
- **Limit access to authorized personnel only –** Restrict access to key storage cabinets or electronic systems to a minimal number of authorized personnel based on job role and operational need. Document authorized individuals in a formal access list approved by management. Immediately revoke access when an employee separates, changes roles, or no longer requires key control responsibilities.

7. Auditing and Compliance

- **Conduct regular audits of key logs and physical keys –** Perform scheduled audits of key issuance logs, storage records, and authorization documents at defined intervals. Verify that all issued keys are accurately recorded in the key log; approval documentation exists for each issued key; and key returns are properly documented.
- **Reconcile issued keys against active employees and contractors –** Compare key issuance records against current employee rosters, contractor and vendor access lists, as well as temporary or seasonal staff assignments. Require immediate recovery of unnecessary keys or initiate lost key procedures if keys cannot be retrieved.

8. Training and Awareness

- **Train staff on key control importance and reporting procedures –** Provide mandatory key control training to all employees and contractors who are issued keys or have access to secure areas and incorporate training into new employee orientation. Training should cover the role of key control in protecting water and wastewater infrastructure; risks associated with lost, stolen, or duplicated keys; procedures for requesting, using, storing, and returning keys; immediate reporting requirements for lost or stolen keys; and consequences of noncompliance with key control policies.

>>>

- **Reinforce that keys are security assets, not personal property –** Clearly communicate that all keys issued remain the property of the utility at all times. Emphasize that misuse or loss of keys can directly impact utility operations and public health and safety. Encourage a culture of accountability where staff feel responsible for reporting issues promptly.

9. Emerging Threats

Physical security risks are evolving with technology and human factors. Key threats include:

- **3D-Printed Keys**
  - **Threat:** Keys can be duplicated from a photo or scan.
  - **Mitigation:** Use restricted keyways, educate staff, and choose complex profiles.
- **Lock Bumping**
  - **Threat:** Bump keys and tutorials are widely available.
  - **Mitigation:** Install high-security locks, inspect for tampering, and use anti-bump pins.
- **Insider Threats**
  - **Threat:** Employees may misuse or duplicate keys.
  - **Mitigation:** Limit master keys, enforce strict issuance policies, and audit regularly.

10. Integration with Electronic Systems

How Keys and Card Readers Complement Each Other

- **Keys as the Foundation:** Reliable first barrier, works during outages.
- **Card Readers for Enhanced Control:** Audit trails, rapid revocation, and role-based access.
- **Layered Security:** Combine both for redundancy; use dual authentication for critical areas.

When to Consider Hybrid Solutions

- **High-risk areas (control rooms, chemical storage).**
- **Transition periods during system upgrades.**
- **Facilities with power/network reliability concerns.**
- **Compliance requirements for sensitive infrastructure.**

11. Emergency Protocols

- **Lock Failure Response:** Secure the area with temporary measures and notify security immediately.
- **Urgent Re-Keying:** Trigger emergency re-keying for lost or stolen keys or compromised master keys.
- **Backup Plans:**
  - Store spare keys in secure cabinets.
  - Maintain emergency locksmith contacts.
  - Document fail-safe procedures for critical access points.

>>>

Bottom Line

Manual keys and locks remain the foundation of physical security—they are reliable, cost-effective, and essential for any facility. Before moving away from traditional keys, ask yourself: Do you truly understand your current key system and its risks? Many organizations overlook key control, which can lead to serious vulnerabilities.

If you are exploring other solutions like electronic keys or card readers, do your due diligence. These systems offer benefits such as audit trails and rapid credential revocation, but they also introduce new risks—such as cyber vulnerabilities, power outages, and system failures.

The best approach may not be replacing one system with another, but creating a layered defense:

- Keep manual keys for reliability and emergency access.
- Add card readers or electronic keys for enhanced control and monitoring.

A hybrid solution combines the simplicity and resilience of mechanical locks with the intelligence and flexibility of electronic systems—providing stronger security than either method alone.

Additional Resources:

- 11 Design Rules for More Secure Locks
- The Essentials of Access Control
- Guidelines for the Physical Security of Water Utilities
- AWWA J100-21 Risk and Resilience Management of Water and Wastewater Systems

---

About the Physical Security and Resilience Advisory Committee

WaterISAC's Physical Security and Resilience Advisory Committee (PSARC) provides strategic guidance and subject matter expertise on issues related to physical security, natural disasters, and operational resilience for the water and wastewater sector.

The PSARC is composed of 12 water and wastewater utility security professionals, along with WaterISAC staff. PSARC members have over 100 years of combined experience in physical security, emergency management, and risk and resilience planning roles. Given its role, the PSARC is essential to WaterISAC's mission of increasing the physical security and resilience of the water and wastewater sector.