Lost Key Replacement Guide

CONSIDERATIONS AROUND LOST KEYS

1. Assessing risks around lost and unaccounted for keys:
   - Amount and type of spaces compromised by key. Do the spaces in question house:
     - Intellectual property / sensitive research?
     - Legally protected data?
     - Represent a theft risk, cash, or credit card information?
     - Medical Records?
     - Are they any State or Federal Government mandates?
     - Living space?
     - Critical maintenance?
     - IT infrastructure?
     - Restricted access space (roofs/tunnels)?
   - How many keys with the same or similar access are known to be lost or unaccounted for?
   - How was the key lost? What are the unknowns? If an employee dropped his keys on vacation in Hawaii is vastly different situation than an unaccounted-for key in the possession of a recently terminated, disgruntled employee.

2. Assessing mitigation options:
   - Are secondary security measures in place or available to staff?
     - Is data protected by passwords, two factor authentications?
     - Are spaces alarmed and monitored?
     - Human and animal life protection?

3. Complexity of mitigating risk:
   - If master or sub-master lost can unique high-risk spaces be separated out of the key series?
   - Should the entire series be rekeyed with considerations for how space is used currently?
   - Review and evaluate conversion to electronic access solution.
   - Can exterior doors or suite entrances be changed to limit building/space access?

NOTE:
- Current governance (decision policy points) remain in place but will be updated as new policy is developed.
- Decisions should align with the Information Risk Framework.
- The decision to rekey space(s) is at the discretion of the individual units.
- Individual departments are responsible for the costs of rekeying for keys they have lost or cannot account for.