Office Security Policy

ACME Evil Anvil Corporation

March 2019 Contents

1. Purpose and Scope
2. Policy

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.4

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

1. This policy establishes the rules governing controls, monitoring, and removal of physical access to company's facilities.
2. This policy applies to all staff, contractors, or third parties who require access to any physical location owned, operated, or otherwise occupied by the company. A separate policy exists for governing access to the company data center.

2 Policy

1. Management responsibilities
    1. Management shall ensure:
        1. appropriate entry controls are in place for secure areas
        2. security personnel, identification badges, or electronic key cards should be used to validate employee access to facilities
        3. confirm visitor & guest access procedure has been followed by host staff
        4. management periodically reviews list of individuals with physical access to facilities
        5. card access records and visitor logs are kept for a minimum of 90 days and are periodically reviewed for unusual activity
2. Key access & card systems
    1. The following policies are applied to all facility access cards/keys:
        1. Access cards/keys shall not be shared or loaned to others
        2. Access cards/keys shall not have identifying information other than a return mail address
        3. Access cards/keys shall be returned to Human Resources when they are no longer needed
        4. Lost or stolen access cards/keys shall be reported immediately
        5. If an employee changes to a role that no longer requires physical access or leaves

the company, their access cards/keys will be suspended
   6. Human Resources will regularly review physical security privileges and review access logs
3. Staff & contractor access procedure
   1. Access to physical locations is granted to employees and contractors based on individual job function and will be granted by Human Resources.
   2. Any individual granted access to physical spaces will be issued a physical key or access key card. Key and card issuance is tracked by Human Resources and will be periodically reviewed.
   3. In the case of termination, Human Resources should ensure immediate revocation of access (i.e. collection of keys, access cards, and any other asset used to enter facilities) through the offboarding procedure.
4. Visitor & guest access procedure
   1. The following policies are applied to identification & authorization of visitors and guests:
      1. All visitors must request and receive written onsite authorization from a staff member.
      2. Visitor access shall be tracked with a sign in/out log. The log shall contain:visitor's name, firm represented, purpose of visit, and onsite personnel authorizing access
      3. The log shall be retained for a minimum of 90 days
      4. Visitors shall be given a badge or other identification that visibly distinguishes visitors from onsite personnel
      5. Visitor badges shall be surrendered before leaving the facility
5. Audit controls & management
   1. Documented procedures and evidence of practice should be in place for this policy. Acceptable controls and procedures include:
      1. visitor logs
      2. access control procedures
      3. operational key-card access systems
      4. video surveillance systems (with retrievable data)
      5. ledgers if issuing physical keys
6. Enforcement
   1. Employees, contractors, or third parties found in violation of this policy (whether intentional or accidental) may be subject to disciplinary action, including:
      1. reprimand
      2. loss of access to premises
      3. termination

From:
https://wiki.cloud.dlzpgroup.com/ -

Permanent link:
https://wiki.cloud.dlzpgroup.com/doku.php?id=security:soc:osp

Last update: **2019/04/13 19:25**