Michael Scott Paper Company

Data Center Policy

Revised January 2024

Purpose

Michael Scott Paper Company's Data Center Policy aims to establish guidelines and procedures for controlling physical access to the data center facility. This policy aims to ensure the security, integrity, and confidentiality of the data center infrastructure and the information contained within.

Scope

The scope of this Data Center Policy extends to all employees, contractors, and third-party vendors who require access to the data center facility. It encompasses all physical access points, including entry and exit points, as well as any areas containing sensitive information or critical infrastructure.

Responsibilities

Management: Management is responsible for establishing and enforcing this access policy, allocating resources for its implementation, and ensuring that personnel are trained on access procedures and security measures.

Employees and Contractors: All employees and contractors are responsible for familiarizing themselves with this policy, complying with access procedures, and reporting any security concerns or incidents promptly.

Access Control

Authorized Personnel: Only authorized personnel with a legitimate business need shall be granted access to the data center facility. Access privileges will be granted based on job role and responsibilities.

Access Approval Process: Access to the data center facility must be requested through the appropriate channels, such as the IT department or facility management. All access requests must be approved by the designated authority before access is granted.

Access Levels: Access privileges will be granted based on the principle of least privilege. Personnel will only be provided with the level of access necessary to perform their job duties effectively.

Visitor Access: Visitors to the data center facility must be pre-authorized and accompanied by an authorized employee or contractor at all times. Visitors must sign in and out, providing appropriate identification, and adhere to all data center access policies.

Doubt!!! phyical access logs ?

Sanctions

Failure to comply with the Data Center Policy may result in disciplinary action, which will be administered in accordance with the corporation's Human Resources procedures. This can range from formal warnings and mandatory cybersecurity training to temporary suspension of access privileges and, in severe cases, termination of employment or contractual relationship. Additionally, individuals may be subject to prosecution for any illegal activities under applicable local, state, national, or international laws. This is to underscore the critical nature of cybersecurity and everyone's role in maintaining the safety and integrity of our corporate digital assets. Sanctions will be enforced impartially and consistently to all parties covered by the policy, with severity proportional to the extent of the policy violation.