**DocuSign**

# Physical Safety and Security Brief

The physical safety and security of our employees, our company, our customers, and the information and assets within our offices are a matter of critical importance for DocuSign. To this end, we apply comprehensive, industry-standard measures to maintain strict control and awareness of access to all of our corporate and computing facilities.

In the following pages, we provide an overview of DocuSign physical safety and security policies, including building access, data center access and physical security operations.

# DocuSign physical safety and security policies apply to all individuals or groups with physical or logical access to DocuSign information assets including employees, contractors, consultants and contingent workers.

## Building Access Control

**Access to all DocuSign sites is controlled through policies to protect the workforce and safeguard information assets.**

– No one is admitted to any access-controlled area of the building unless they use an authorized access control card or sign a log and present identification credentials

– Visitors are escorted by a DocuSign employee at all times while in our offices

– Card access records and visitor logs are kept for a limited time for review by physical security or human resource departments if needed for investigation purposes

– Visitors are not permitted to remove equipment, computer hardware, software, information, or any other information asset from a DocuSign site without prior authorization– Any unusual access is investigated fully

## Data center access control

**The data centers housing DocuSign technology and information assets meet strict standards for cybersecurity and physical safety, and undergo regular reviews.**

– DocuSign supporting utilities are commercial grade and provided through a professional data center facility

– Common areas such as building lobbies and loading zones are isolated from secure areas

– The physical security environment of every DocuSign data center is reviewed annually

– All critical systems including, but not limited to, servers, firewalls and storage systems are physically located within a secured room or data center

– All new DocuSign computer or communications centers are located in sites hardened against natural disasters, serious accidents, riots and related problems

– All DocuSign production computer centers are equipped with fire, water and physical intrusion alarm systems

– Access to DocuSign areas in third-party data centers is strictly limited to authorized DocuSign IT personnel

## Physical security operations

**Physical security operations are addressed as an essential function of the DocuSign security monitoring center (SMC)**

– Physical security plans are documented for each DocuSign site

– Risk assessments are performed for all DocuSign sites on a regular risk-based schedule

– Environmental risk assessments are performed periodically on DocuSign security equipment, with safeguards implemented to mitigate any identified risks

– Physical security plans are updated following each risk assessment

– DocuSign access control and monitoring systems meet the highest level of modern standards for physical security

– Access to all DocuSign offices globally is monitored 24x7x365

– News events in proximity to DocuSign offices, data centers and employees around the world are monitored for potential impact

## Additional resources

[DocuSign Trust Center](#)

**DocuSign®**