DOORDECK

Security Information Document

VER 3.0 - JUNE 18

1. Mission Statement

At Doordeck, security is of course our main priority.
The Doordeck platform was built from the ground up using the core principles of information security, also known as the CIA triad:

Confidentiality

Prevent the disclosure of information to unauthorized individuals or systems.

Integrity

Maintain and assure the accuracy and consistency of data over its entire lifecycle.

Availability

Ensure the information is available when needed.

Doordeck is committed to achieving and maintaining these principles and the trust of our customers. Integral to this is providing a robust security and privacy program that carefully considers data protection matters across our suite of services where applicable.

**User sensitive data is encrypted with AES256.
All data in transmitted using HTTPS with TLS.**

2. Architecture

Doordeck hardware is hosted at third-party facilities (“data centres”).

This facility is an Amazon Web Services (AWS) facility.

Prior to selection, the facility was subjected to a stringent assessment for the presence, implementation, and ongoing administration of physical security controls.

Each facility is fully protected 24x7x365 by security guards, high-security fencing, and video cameras.

Facilities have an annual audit by industry-leading firms for ISO 27001 and/or SSAE 16 Type II compliance in addition to many other certification as seen on the following diagram below.

HIPAA
CJIS
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
FedRAMP
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports
PCI Security Standards Council
PARTICIPATING ORGANIZATION
CYBER ESSENTIALS PLUS
DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA
FIPS 140-2
CRYPTOGRAPHY
TÜV AUSTRIA
ITAR
International Traffic in Arms Regulations Compliant
CSA cloud security alliance
FDA
GOV.UK
irap
NIST

3. Doordeck Employee Access, Controls, and Policies

Employee access to production infrastructure is permitted only via VPN which uses encrypted private keys.

Access to any data centre server is further protected by the mandatory use of SSH public key infrastructure (PKI) technology.

Doordeck staff cannot see any sensitive-user data without being granted permission by the customer through the native access control system.

Access is based on the information security principle of "least privilege" with access strictly limited to a select number of skilled individuals.

All access is monitored and logged.

All employees are subject to background checks prior to employment.

All employees are trained on documented information security and privacy procedures.

All employees are required to sign "Customer Data Confidentiality Agreements."

All employees in the Engineering, Quality Assurance, Technical Operations, and Security teams receive additional security training.

All access is immediately revoked on termination of employment.

4. Security Team

Doordeck has full-time employees focused on governance, risk, audit, and compliance in the areas of security and privacy.

Each team member has years of industry experience and one or more well-known industry certifications, including:

CISSP

CISM

CISA

CEGIT CISSP

BSI27001 LI

MBCS

In addition to the certifications held by our service provider, we are also looking to obtain 27001 certification by the end of Q1 2019

5. Vulnerability and Malware Management

Malware and Viruses

Doordeck will never introduce any virus or malware to a customer's systems. Scans are performed for viruses and malware that could be included in attachments or other customer data uploaded into Doordeck by a customer.

Vulnerability Management

The Doordeck application is subjected to a regular web application scanning (WAS) process carried out a using market-leading security and compliance provider.

6. Security Procedures, Policies, and Logging

All services are monitored both internally and from an external system. Doordeck is operated in accordance with the following procedures to enhance security:

Security Logs

All systems (for example, firewalls, routers, network switches, and operating systems) used in the provision of Doordeck will log information to their respective system log facility and to a centralized syslog server.

- All data access by customer and staff is monitored & logged.
- All data changes by customer and staff are monitored & logged.
- Logging will be kept for a minimum of 365 days.
- Logging will be kept in a secure area to prevent tampering.

System Maintenance

Maintenance is carried out during non-business hours, typically weekdays 7pm onwards or weekends and bank holidays. Maintenance is most commonly used for new version release, typically every 2-4 weeks.

Change Management

Doordeck follows fully documented change management procedures for all tiers of the service covering application, operating system, server, and network layers. All configuration changes are tracked and managed through a written ticketing system.

6. Security Procedures, Policies, and Logging

Deletion of Customer Data

Upon contract termination, customer data submitted to Doordeck is retained in inactive status within Doordeck for 30 days and a transition period of up to an additional 30 days, after which it is overwritten or deleted. Doordeck reserves the right to reduce the number of days it retains such data after contract termination. This process is subject to applicable legal and/or contract requirements.

Event Management

Doordeck maintains event management policies and procedures as shown in this Information Security Event Management Escalation Workflow.

Doordeck security procedures

- All of Doordeck's cloud infrastructure is hosted in Amazon Web Services (AWS).
- Access to cloud infrastructure is restricted to senior developers.
- Cloud management is done via audited bastian server, protected with a VPN.

Is Doordeck behind a firewall?

- Yes, our backend lives in a virtual private cloud
- Our EC2 instances are separated into different security groups with restricted policies
- Instances do not have direct internet access rather access is done by elastic load balancer

Hardware & Software Security Information

1. Cloud, AWS

Cloud

- All changes are code reviewed.
- Software is signed with digital signatures.
- Access to code repository is controlled via ACL (Access Control List).
- Unit testing.
- Changes are deployed to staging first.
- Done with automation tools.
- Tested internally.
- When it’s ready, code is promoted to production.
- All access is via TLS & strong encryption.

AWS

Please refer to aws.amazon.com/security

2. Communication, How Doordeck Works

Communication

- Each user has a private key.
- Private keys are stored encrypted on the cloud using AES 256 with a key derived from the users password.
- Passwords hashes are stored in the cloud using PBKDF2 tuned to take 100 millisecond per computation to prevent brute forcing.
- Password hashes are generated using a salt and pepper.
- Requests to interact with the controllers are digitally signed using the user's private key and verified on the cloud and on the controller.

How Doordeck Works

- A user generates a request using their key.
- Request is sent to the cloud.
- The cloud verifies the request.
- Cloud forwards request to the controller.
- Controller verifies request again.
- 2 step verification process means that if the cloud server was ever compromised, an attacker cannot unlock your door