DonorDock Application Security Overview

DOCUMENT REF	AppSecOverview
VERSION	1.4
DATED	08 December 2023
DOCUMENT AUTHOR	Mathew Bitzegaio
DOCUMENT OWNER	Mathew Bitzegaio

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	11/9/2020	Mathew Bitzegaio	Initial Version of Document
1.1	8/12/2021	Mathew Bitzegaio	Added information on TDE
1.2	7/26/2023	Andrew Lutgen	Updated Vulnerability Scanning, People Security
1.3	7/26/2023	Andrew Lutgen	Added SOC 2 Type I and 2FA information
1.4	12/8/2023	Andrew Lutgen	Updated SOC 2 information to reflect Type 2 compliance

DonorDock Application Overview

To avoid loss of Company property, DONORDOCK has IT and security procedures, which include maintaining control of entrances, exits, restricted areas, document control, record keeping, and use of Company property and IS resources. Due to the risks for our Team Members, our customers and our company, all Team Members are expected to abide by all DONORDOCK security procedures.

Compliance

DonorDock has achieved SOC 2 Type 2 compliance and was independently audited by Laika (Thoropass) Compliance, LLC. SOC 2 is a security framework that defines requirements for security, availability, processing integrity, confidentiality, and privacy. A copy of the SOC 2 Type 2 report is available on request.

Infrastructure

Azure

All hosting for the DonorDock SaaS application is through Microsoft Azure. Microsoft Azure is a leading, enterprise-grade cloud platform. Microsoft maintains all necessary compliance and certifications for Azure cloud services.

All compliance reports for Microsoft services can be found here:

https://servicetrust.microsoft.com/Documents/ComplianceReports

Azure Dev Ops

All ALM for the DonorDock SaaS application is managed through Microsoft's Azure Dev Ops. Azure DevOps Services is a cloud-hosted application for your development projects, from planning through deployment. Based on the capabilities of Team Foundation Server, with additional cloud services, Azure DevOps manages your source code, work items, builds, tests, and much more. It uses Azure's Platform as a Service infrastructure and many of Azure's services, including Azure SQL databases, to deliver a reliable, globally available service for DonorDock's development processes.

More information on Azure Dev Ops security can be found here:

https://docs.microsoft.com/en-us/azure/devops/organizations/security/data-protection?view=azure-devops

Application Security Overview

Encryption

- User access to DonorDock's hosted applications is done so securely via HTTPS protocol using a TLS 1.2 sublayer
- HTTP to HTTPS redirection is enabled

Database encryption

Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. TDE is enabled on all DonorDock SQL Azure databases. Each DonorDock customer has a discreet database, and no customer data is stored in shared databases.

Authentication & Authorization

- DonorDock applications require authentication to access
- Authentication is provided by Oauth2
    - Clients use an authorization code-based flow
- Two-factor (2FA) Authentication
    - 2FA authentication can be enabled and is verified by email
    - Request for 2FA authentication can be set to every login, every 14 days, 30 days, 45 days, or 90 days
- Session expiration
    - Identity and Access token lifetime is set at 8 hours
- Guarded resource access
    - Assigned roles are used to ensure data access and updates are restricted to authenticated and approved users

Vendor Relationships

Microsoft

All cloud hosting and code management is done through Microsoft Azure. All compliance reports for Microsoft services can be found here:

https://servicetrust.microsoft.com/Documents/ComplianceReports

SendGrid

DonorDock uses SendGrid to send transactional emails from the DonorDock application to users. For more information on SendGrid and their security policies, please see:

https://sendgrid.com/policies/security/

Stripe

DonorDock uses Stripe as a payment process for online giving. For more information on Stripe and their security policies, please see:

https://stripe.com/docs/security/stripe

PayPal

DonorDock uses PayPal as a payment process for online giving. For more information on PayPal and their security policies, please see:

https://www.paypal.com/re/webapps/mpp/paypal-safety-and-security

Application Continuity

DonorDock leverages Microsoft Azure for all hosting and code repositories. No code is stored on-premise and all code and databases are subject to weekly full backups and daily differential backups. Cloud services are also set up for redundancy and automatic failover. More information can be found here:

Databases:

https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?tabs=single-database

App Services:

https://docs.microsoft.com/en-us/azure/app-service/manage-backup

Git Repositories:

https://docs.microsoft.com/en-us/azure/devops/organizations/security/data-protection?view=azure-devops

People Security

DonorDock uses an approved background check vendor to perform background checks on individuals prior to employment. All employees must undergo security awareness training after hiring and annually thereafter. Employee access to systems and data uses the principle of least privilege and is audited regularly.

Employee devices with access to company data are equipped with a device management solution to ensure compliance. Managed devices can remotely lock or wipe company data access from the device. Employees are to use strong passwords, stay up to date with device updates, are not allowed to download illegal content, and lock all devices when not in use.

Vulnerability Testing

DonorDock tests for vulnerabilities using Detectify surface and application scanning. Vulnerability scanning helps identify any areas of weakness to production systems. Azure resources utilize Microsoft Defender for Cloud for threat detection, misconfigurations, and intrusion detection. Any discovered vulnerabilities are tracked for remediation.

Any Critical impact issues are remediated immediately to within 7 days from identification. High issues are remediated within 14 days of identification. Medium and Low impact vulnerabilities will be triaged and managed in the ALM cycle.

Overall App Architecture (SOA)

- DonorDock applications consist of two primary client applications with the following architecture
    - Angular Single Page Application (SPA)
    - .NET Web API 2 (REST APIs)
    - MS SQL (see Microsoft Azure section)
- Authorization to client applications is facilitated by an identity application with the following architecture:
    - .NET Framework
    - ASP.NET Identity
    - MS SQL (see Microsoft Azure section)

DonorDock Application Diagram