FORVIS™

FORVIS Security Overview

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

Table of Contents

1.0 Introduction 4

1.1 What Is FORVIS Client Sites? 4

1.2 Site Creation 4

1.3 Client Authentication & Access 4

2.0 Security Design 4

2.1 Confidentiality 4

2.1.1 Least Privilege & Role-Based Security 4

2.1.2 TLS Authentication & Communication 5

2.1.3 Access Controls in Client Sites 5

2.1.4 Network Segmentation 5

2.1.5 Separate Authentication Mechanisms 5

2.1.6 Encryption 5

2.1.7 Content Retention 5

2.2 Integrity 6

2.2.1 Audit Trails 6

2.2.2 Document Control 6

2.3 Availability 6

2.3.1 Segregated Environments 6

2.3.2 Redundant Systems 6

2.3.3 Load Balancers 6

2.3.4 Backups 6

3.0 Security Operations 7

3.1 Physical Security 7

3.2 Personnel & Processes 7

3.3 Additional Security Controls 7

4.0 MyDHG Review 8

Approver's Name and Title	Approver's Signature	Date/Time
Andrew Thayil, Chief Information Security Officer	Andrew Thayil Digitally signed by Andrew Thayil Date: 2023.06.10 11:25:18 -04'00'	June 2023

Revision History

Effective Date	Version Number	Author(s)	Description
5/15/2023	2.0	MyFORVIS Product Team	Combined LBKD & LDHG Security Review

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

1.0 Introduction

1.1 What Is Client Sites?

Client Sites is an online application hosted by FORVIS, LLP. With Client Sites, FORVIS hosts client data, provides site management, and enables client collaboration through the life of a site.

Client Sites allows clients to easily submit documentation, oversee their site, provide updates, and collaborate with other client users and FORVIS staff.

FORVIS recognizes that with the increased efficiency and communication of online applications, there are also increased security concerns and risk. This document describes the controls implemented by FORVIS specific to Client Sites for the purpose of clients to determine if Client Sites is suitable for their business.

1.2 Site Creation

A new site can only be created by FORVIS professionals who are responsible for the administration and management of Client Sites. FORVIS professionals are responsible for adding Site Sharing Approvers and Site Administrators to each client's site.

1.3 Client Authentication & Access

Upon creation of the site, FORVIS professionals will add a Site Sharing Approver. This account is used by the client to approve the Site Administrator. The Site Administrator then adds Client Users and selects their level of access to the site.

As the Site Administrator adds to or edits the Client User list, each individual user is systematically added to or removed from specific permission groups based on the selections made by the Site Administrator. When individual users are added to the Client Users list, system-generated invitations are sent requesting registration. Upon successful registration, the user will be granted access to the site. When individual users are removed from all Client Users lists, all permissions to the sites are systematically removed.

More information about setting up Client Users can be found on the Client Sites Help Center page.

Each site is created by internal FORVIS professionals for a specific client and only accessible to the Client Users assigned to that site. FORVIS professionals are assigned to a site by an authorized FORVIS professional, while client users are assigned by the Site Administrator.

2.0 Security Design

2.1 Confidentiality

Confidentiality ensures that client data is only accessible by authorized entities. FORVIS provides confidentiality in the following ways:

2.1.1 Least Privilege & Role-Based Security

The principle of least privilege is widely accepted as a best practice, and as such, FORVIS has implemented role-based security within and around Client Sites. With this security model, the client has the ability to assign specific access permissions to their staff. FORVIS recommends all clients make use of this security feature whenever possible.

The following roles are available within Client Sites:

- Infrastructure Team – Internal FORVIS IT users responsible for the hardware and operating system of the application. This team is responsible for system stability and maintenance and does not have access to the Client Sites application or data.

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

1217000 6.08.23

- System Administrator – Internal FORVIS IT users responsible for the Client Sites application and underlying databases. These users are responsible for patching and maintaining the stability of the application.
- FORVIS Users – Internal FORVIS users responsible for managing client engagements and the client's site. A FORVIS user creates the Site Administrator account, adds a Site Sharing Approver, and assigns FORVIS staff as FORVIS users.
- Site Sharing Approver – Client executive responsible for the authorization of site sharing for client users. Only one per site. This user is maintained by a FORVIS User. No enrollment into Client Sites is required. Approvals are managed through email.
- Site Administrator – Used by the client to assign Client users from client staff. In addition, this account can set access permissions for the accounts they create.
- Client Users – Client staff assigned to the site. This account is maintained by the Site Administrator. Client users are granted one of two types of access – Full Client Site access, which includes all existing and future engagements, or Engagement Specific access, which allows the Site Administrator to pick which engagements the user can access.

2.1.2 TLS Authentication & Communication

All communications, including the registration and authentication processes, are protected with TLS encryption.

2.1.3 Access Controls in Client Sites

Access controls have been implemented within the Client Sites application. Each site is restricted and only accessible by the accounts assigned specifically to that site. This prevents an account from one client site being used to gain access to other client sites.

2.1.4 Network Segmentation

Network segmentation creates a collection of isolated networks within a larger network. Each network then becomes its own separate broadcast domain. This segmentation severely hinders a would-be attacker since each one is essentially a standalone network, with no ability to access another network. Virtual local area networks (VLANs) provide this capability and are used to segregate Client Sites systems from their respective databases.

2.1.5 Separate Authentication Mechanisms

Separate user management and authentication systems are used for FORVIS users and client users. This design ensures that FORVIS users cannot create "client accounts" and clients cannot create "FORVIS accounts," which prevents attempts to circumvent security controls and gain unauthorized access to data.

This segregation also allows each client to implement role-based security for their users that matches their own internally designated roles.

2.1.6 Encryption

Data is encrypted both "at rest" and "in motion" with Client Sites. This is accomplished using encrypted databases and TLS, respectively.

All communication and data encryption is compliant with the FIPS 140-2 standards.

2.1.7 Content Retention

Data is stored in Client Sites throughout the life of the engagement for which the client site was created. At the completion of the engagement, data is available to be rolled forward to future engagements or downloaded but otherwise cannot be modified.

The completed engagement will show in the client list of engagements for three years.

All unfiled data and task documents stored on Client Sites are purged 18 months after engagement completion.

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

2.2 Integrity

Integrity refers to the trustworthiness of information. This means that data has not been changed inappropriately, either accidentally or intentionally. FORVIS provides integrity through:

2.2.1 Audit Trails

Client Sites is configured to generate detailed audit logs. These logs record actions such as who accessed data, when they accessed the data, what pages were visited, and what they did within Client Sites with the data they accessed.

These logs are retained within a discrete database and are accessible only by a System Administrator.

2.2.2 Document Control

To modify a document, it must be downloaded from the site, edited locally, and then uploaded back to the site. No documents can be edited directly in the application. FORVIS users are notified daily when new documents have been added to their engagements. Multiple documents can be downloaded if they are all on the same page or section. There is no ability to download an entire client site at once.

2.3 Availability

Availability refers to the ability to access and use data resources when needed and to protect against unplanned failures in service. FORVIS provides availability by:

2.3.1 Segregated Environments

Client Sites uses a development environment for creating new code and changes to the Client Sites system. These changes are then moved to a Quality Assurance instance where they are thoroughly assessed and reviewed. Once all testing has been performed and the new or changed code is approved, it is moved into the production instance during a maintenance cycle.

This process ensures that unstable or malicious code does not go into production. This is a standard best practice of a systems development life cycle (SDLC).

2.3.2 Redundant Systems

FORVIS uses best-in-class systems and network devices as part of the Client Sites infrastructure. This includes redundant Internet connections, routers, firewalls, and servers. FORVIS has removed all single points of failure through a layered approach, ensuring maximum availability and security for the Client Sites platform.

2.3.3 Load Balancers

FORVIS uses enterprise-class load balancers to ensure that high volumes of traffic do not limit service or reduce functionality.

2.3.4 Backups

All Client Sites servers and databases are backed up using FORVIS' enterprise backup solution. Backups are performed hourly. These backups are replicated off site to a secure location.

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

1217000 6.08.23

3.0 Security Operations

While not necessarily specific to Client Sites, many security controls within FORVIS contribute to the overall security of the Client Sites system.

3.1 Physical Security

FORVIS uses best-in-class data centers to house systems. These facilities provide protection from all but the most severe natural disasters.

Each facility is staffed around the clock and provides physical access restrictions through a dead-man room, electronic access controls, and remote monitoring via cameras. In addition, each data center includes the environmental controls necessary for a continuous computing environment (redundant power, HVAC, fire suppression, etc.).

3.2 Personnel & Processes

FORVIS not only uses best-in-class systems but enterprise-class personnel. With dedicated and trained IT personnel, FORVIS ensures stable and secure system operations through the use of best practice processes such as change control, patch management, SDLC, and other techniques.

3.3 Additional Security Controls

Dedicated IT Security – FORVIS has a dedicated IT security team responsible for overseeing and ensuring the confidentiality, integrity, and availability of FORVIS systems and data.

- Information Security Program – FORVIS has a formalized Information Security Program that consists of formalized policies and procedures, incident response, and IT continuity and recovery plans.
- Penetration Testing – FORVIS performs routine vulnerability assessments against internal and external systems. In addition, FORVIS has penetration testing performed annually.
- Application Testing –Client Sites has undergone an independent application test by an industry- recognized application testing company.
- Intrusion Detection – FORVIS uses an enterprise-class intrusion detection system with 24/7 monitoring and alerting services.
- Antivirus Protection – FORVIS uses enterprise-class antivirus software at both the operating system and application level to protect against malicious software.

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

4.0 MyDHG Review

MyDHG (legacy DHG application) is a customized digital experience that supports seamless collaboration and sharing of essential information between our clients and FORVIS professionals.

- Intuitive platform for the execution of engagement tasks and the exchange of documents
- Centralized functionality for effective and documented communication
- Transparency into the progress of engagements
- Ability to restrict access to requests and documents
- Safe, secure, and efficient transmission of documents and information between FORVIS and external parties (clients, potential clients, vendors)
- Leverages Microsoft B2C Authentication Mechanism
- MFA Enforced
- Can support Client Side SSO and Federation (SAML 2.0 + OAuth 2.0)
- Encryption in transit via HTTPS/TLS 1.2 and Encryption at rest via AES-256
- The application has been tested for the prevention of cross site scripting attacks, parameter manipulation, SQL injection, buffer overflow, truncation, hidden web paths, cookie manipulation, and other known web application vulnerabilities
- Model of least privileged access followed
- 90-day retention for internally uploaded files, one-year retention for client/external user uploaded files

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

1217000 6.08.23