DFIN

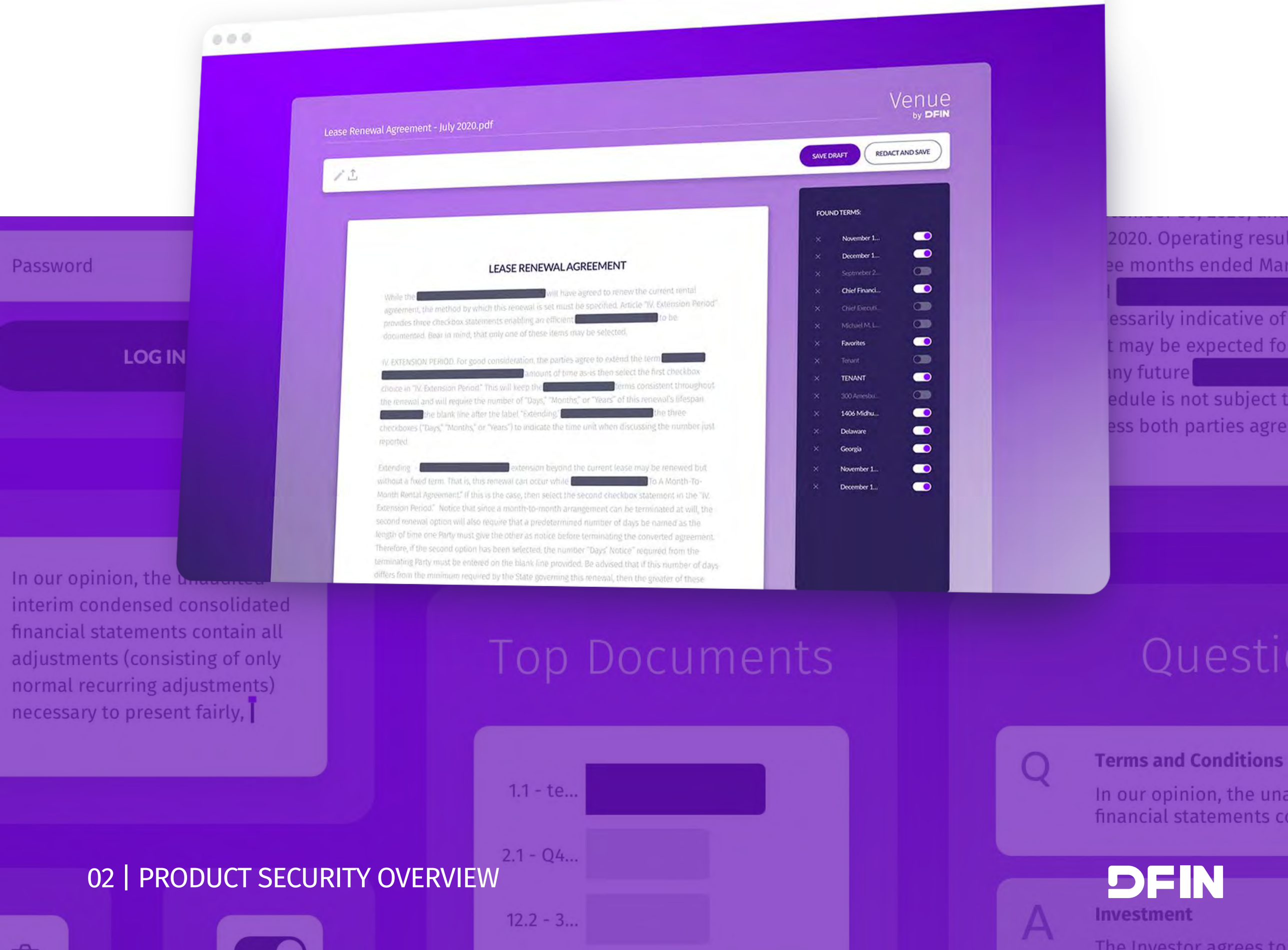
Venue

by DFIN

Product Security Overview

Venue virtual data rooms help clients to accelerate their deal process securely. They are reinforced by DFIN regional experts and continually optimized for security, productivity, and usability. Venue is trusted globally by Fortune 1000 companies, Silicon Valley startups, PE firms, investment banks, and government agencies.

Donnelley Financial Solutions (DFIN) is a leader in risk and compliance solutions, providing insightful technology, industry expertise and data insights to clients across the globe.



DFIN'S CYBERSECURITY OVERVIEW

The **DFIN Information Security Program** is designed to ensure data protection, enterprise cybersecurity, and supply chain security throughout the environment. The program is based on business requirements derived from:

Assessing

security risks to the organization.

Complying

with the legal, statutory, regulatory, and contractual requirements that DFIN and its business partners, contractors, and service providers must satisfy.

Delineating

the principles and objectives for operational information processing.

Information Security for Venue is achieved by implementing a set of controls, which consist of policies, processes, procedures, organizational structures, and software functions.

Controls have been established to minimize risk and protect information assets required to meet the operational, financial, and regulatory requirements to safeguard client data and privacy. Information security is characterized as the preservation of:

SECURITY

to protect assets from external and internal threats

AVAILABILITY

to prevent disruption of service and productivity

CONFIDENTIALITY

to prevent unauthorized disclosure of sensitive information

Venue by DFIN

CONTROLS APPLIED TO OUR PRODUCTS

Organizational Controls

DFIN's robust organizational controls ensure that security is addressed as a part of all software development at DFIN by integrating security practices and generating security and compliance artifacts throughout the process. The **advantages** in doing so are:

- Reduction in vulnerabilities, malicious code, and other security issues.
- Mitigation of potential impacts of vulnerability exploitation throughout the product's lifecycle.
- Evaluation of root causes for vulnerabilities to avoid future occurrences.

DFIN leverages SOC2 Type II auditing and reporting, ISO/IEC 27001:2013 certification, an expert-staffed Security Operations Center (SOC), and a security awareness program with training for DFIN staff to ensure application and data security.

Secure Software Development Life Cycle (S-SDLC), Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), secure software release management, and vulnerability management help to ensure Venue application security.

From an accountability perspective, security awareness, data privacy, ethics, and code of conduct are instilled into DFIN team members.

Security by Design

DFIN applies the principle of "security by design" and has applied multiple security standards including but not limited to:

Information Rights Management (IRM) protection encrypts documents to prevent unauthorized users from viewing or sharing content.

Application Programming Interface (API) automates the retrieval of security-related data including audit logs, user activity, and document uploads/downloads.

Encryption at rest and in transit using TLS1.2 and strong encryption algorithms like AES-256.

Annual penetration tests by an authorized independent third party.

Single Sign-On (SSO), Multifactor Authentication (MFA), and robust role-based access control (RBAC) ensure the least privileged access to assets and resources.

Comprehensive network and infrastructure security controls including firewalls, Intrusion Prevention System (IPS), and Intrusion Detection System (IDS).

Commitment to Security

Venue virtual data rooms ensure the integrity of client data and access through industry standards and best-in-class security provisioning. The chart below highlights security considerations for virtual data rooms.

Security	Venue	Description
SOC2 Type II Audits	YES	Performed by a third party with annual reports for observed security effectiveness
ISO/IEC 27001:2013 Certification	YES	Comprehensive Information Security Management System (ISMS) that ensures adherence to applicable ISO 27001 clauses and relevant controls
Document encryption at rest	YES	Uses AES-256bit encryption for data at rest
Information encryption in transit	YES	Uses TLS 1.2
Access encryption	YES	HTTPS (Hypertext Transfer Protocol Secure)
Encryption Keys Per Room	YES	Unique keys for each virtual data room protect against data leakage across rooms
Client Managed Encryption Keys	YES	Clients can expire and rotate keys on their schedule
Identity Access Management – Multi-Factor Authentication	YES	Supported
Identity Access Management – Single Sign-On (SSO)	YES	Supported
Penetration Testing	YES	Methodic and exhaustive annual test with priority remediation of any security vulnerability issues
User Session Time Out	YES	Configurable from 15 to 60 minutes

Venue
by DFIN

In Summary

Venue virtual data rooms safeguard clients with the highest levels of infrastructure security yet make it easy to quickly self-launch one or multiple deals.

DFIN understands the importance of maintaining a comprehensive and robust Information Security Program that spans network, system, application, and data security singularly focused on safeguarding our products and our client's data. DFIN aims to be a trusted partner to our clients.

CONTACT US

venue@dfinsolutions.com
+1 800 823 5304

DFIN