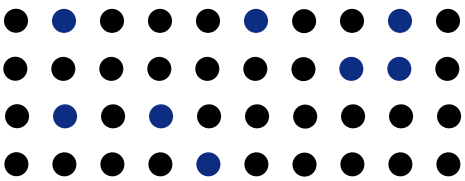
SecuriKey

eDOC INNOVATIONS

idocVAULT

Core Image Processing

VERSION
June 2021



LEGAL DISCLAIMER

The information contained in this document does not constitute legal advice. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers nor eDOC Innovations, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Quick Reference Summary of Controls

HTTPS

The problem with the regular HTTP protocol is that the information that flows from server to browser is not encrypted, which means it can be easily stolen. HTTPS protocols remedy this by using an SSL (secure sockets layer) certificate, which helps create a secure encrypted connection between the server and the browser.

ENCRYPTION

Documents are encrypted in storage as well as in transit.

SESSIONS

Communication channels are secured via sessions. If the IP address changes during a session, the session is terminated.

PASSWORD COMPLEXITY

idocVAULT enforces complex passwords.

ACCESS RESTRICTIONS

idocVAULT provides for time, IP, and multifactor authentication access restrictions.

SecuriKey

Credit unions may be asked by examiners or auditors to provide an idocVAULT risk assessment, documenting idocVAULT's safeguarding of non-public personally identifiable information. This document provides a description of the controls used to protect information and verify identity.

eDOC innovations is aware that in this modern world security is more important than ever. It is one of the fastest-growing industries in the world today and something we should all pay close attention to.

Overview of idocVAULT Security Features

eDOC takes security seriously. eDOC regularly educates its employees of security risks and advise them on ways to ensure client data is safe and secure. eDOC cultivates a cybersecurity culture centered around our commitment to keeping data protected.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS protocols remedy the risk of stolen information in transmission by using an SSL (secure sockets layer) certificate, which helps create a secure encrypted connection between the server and the browser. HTTPS protects potentially sensitive information from being stolen as it is transferred between the server and the browser.

ENCRYPTION

eDOC files are encrypted by default on the idocVAULT. This helps protect data no matter how documents are transferred. Encryption ensures documents stay secure both during transit as well as when housed in the idocVAULT.

SESSIONS

Communication channels are secured via sessions. eDOC uses this session approach to protect against session hijacking. If the IP address changes during a session, the session is terminated.

FIREWALLS

Additional security layers for Intel-based managed hosting devices include border and gateway devices secured to industry best-practices, dual redundant gateway firewalls, network and host based intrusion detection systems, layered network firewalls in some segments, hosts secured to industry best-practices and kept up to date with critical security fixes, regular log file reviews, centrally managed enterprise-wide anti-virus software updated hourly, centralized critical event log file aggregation systems, centralized device performance and response monitoring and alerting, and regular internal host configuration security audits.

PASSWORD COMPLEXITY

eDOC offers settings to ensure your staff creates passwords that are not easily cracked. In-House credit unions can maintain these settings and also have the option of integration with active directory.

Hosted solutions have the following minimum requirements;you can request more complex requirements.

Minimum password length
Required is 8 characters

Minimum number of lower-case characters
Required is 1 lower-case character

Minimum number of upper-case characters
Required is 1 upper-case character

Minimum number of numeric characters
Required is 1 numeric character

Select the number of days for each password to expire
Required is a minimum of 45

Set lockout time
Required is a minimum of 15 minutes

Set a password history length
Required is a minimum of 6

Grace period
Set grace period for expired passwords and password resets

ACCESS RESTRICTIONS

IP Restriction
IP restrictions allows credit unions to limit access to the idocVAULT to a predefined list of IP addresses.

Time Restriction
Time restrictions allow self-hosting and hosted credit unions to control when staff can access the system.

MFA (Multi-Factor Authentication)
eDOC Supports Google Authenticator, which is widely available for free in the Google and Apple stores. Setting up MFA at a self-hosting or hosted credit union provides an additional layer of protection.

CU*SPY Ransomware Responses

CU*Answers is occasionally asked about controls regarding ransomware and backups. Some questions are related to our hosted Imaging System (CU*SPY). CU*Answers and our credit union clients are on entirely separate, segregated networks, and therefore it is highly unlikely if one business is victimized by ransomware that both entities would be affected. The CU*SPY discussion does not apply to clients that have their own in-house imaging solution.

CU*SPY is part of the daily backup system. Encrypted system snapshots are made to a local, high speed network attached storage (NAS) device. Incremental backups are compressed and transferred to an offsite via high-speed encrypted connection. The system offers restore capabilities for multiple file versions. The backup system is monitored 24x7 and a ticket is automatically generated for missed backup or any issue with the backup system. The local and remote NAS devices also offer backup virtualization capabilities, facilitating a business continuity strategy for critical hardware or environmental failures at the primary site. Data backup integrity, recovery and virtualization are tested on the backup appliances on a quarterly basis. Storage media is available to clients who wish to purchase.

(a) Procedures are in place to prevent backups from being affected by ransomware.

- Encrypted backups are made to NAS devices
- Backup system is monitored 24x7

(b) Access to backups use authentication methods that differ from the network method of authentication.

- Backup system requires separate credentials

(c) At least daily full system (vs incremental) backups are made.

- Daily backups are made to the NAS system

(d) At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.) and they are stored separately.

- Backups are virtualized for speedy recovery, credit unions may purchase media, or may download all their reports and documents to their own in-house devices

(e) At least one backup is offline, also known as air gapped or immutable.

- Credit unions can elect to purchase storage media of their data

(f) A regular backup testing process is used at least annually that ensures the institution can recover from ransomware using an unaffected backup.

- The backup process is tested quarterly

Version Control

VERSION	DATE	CHANGE	TEAM
1.0	June 1, 2018	First published	Internal Audit

Learn More

eDOC INNOVATIONS
Core Image Processing — When Strategy Matters

Contact eDOC Innovations support team at 800-425-7766 to learn more.