

Item 8.A.

Document Scanning



MEMORANDUM

TO: City of Delray Beach General Employees' Retirement Plan
Retirement Committee

FROM: Lisa Castronovo, Pension Administrator

SUBJECT: Document Scanning

DATE: August 13, 2026

ISSUE:

Document scanning

EXPLANATION:

Over the last two years, Elizabeth scanned all active retirees' and beneficiaries' old paper files. We now can access these files as needed digitally. Once we verify that each file was completely and accurately scanned, the paper files will be removed from our office and securely stored in a secure City facility.

We now would like to hire an outside company to scan the remaining files in our office - 16 bankers boxes of non-sensitive documents and about 11 boxes of sensitive documents (deceased retiree files that contain Social Security numbers). The cost for the scanning would be shared evenly by the three pension plans. We received three quotes - Access: \$10,125 (\$375/box; \$3,375/plan), ARC: \$8,100 (\$300/box; \$2,700/plan), and Docufree: \$7,800 (\$290/box; \$2,600/plan).

RECOMMENDATION:

Motion to approve Access, ARC, or Docufree to scan approximately 27 bankers boxes.

ACCESS

Castronovo, Lisa

From: Samuel Vehorn <Samuel.Vehorn@accesscorp.com>
Sent: Tuesday, July 28, 2026 10:31 AM
To: Castronovo, Lisa
Subject: Access Scanning

Follow Up Flag: Follow up
Flag Status: Flagged

You don't often get email from samuel.vehorn@accesscorp.com. [Learn why this is important](#)

Hi Lisa,

Good news — I've got pricing put together for your pension file project. For the 30 banker boxes, we're looking at around \$375ish per box, the project would come out to \$11,500 for the full project. That covers color scanning, digital indexing by folder, and pickup and return of your boxes.

Since there's no deadline on your end, we can schedule whenever works best for you — just say the word and we'll get it on the calendar. Happy to walk through any of it.

Best,
Sam



Samuel Vehorn
Inside Sales Representative
904-495-3853
8AM – 5PM EST, M-F



Custom Records Management & Information Governance Solutions Tailored to Your Industry

Information governance, records management, and regulatory compliance are complex subjects, and best practices vary greatly between industries.

With over 20 years of experience in the document storage and records management business, we assist clients in a wide variety of industry verticals, creating custom document management and storage solutions tailored to your needs.

- [Healthcare](#)
- [Legal](#)
- [Finance](#)
- [Insurance](#)
- [Energy](#)
- [Manufacturing](#)
- [Government](#)
- [Education](#)
- [Automotive](#)
- [Retail & Hospitality](#)

Healthcare

Our enterprise-scale records management services are fully HIPAA compliant, with complete security and local regulatory compliance for all your sensitive patient files and health records. Our digital transformation solutions can also help your practice go paperless and securely manage all electronic health records.

We will help create a comprehensive health information management program that provides guidance for which files to keep and which to safely destroy. Our secure destruction services ensure that medical records are disposed of securely and with full regulatory compliance.

Legal

We provide custom document management solutions for the rigorous needs of the legal industry. We can securely store and manage a wide variety of legal documents including:

- Paper documents, including contracts and agreements
- Electronic media and digital documents
- Tape rolls, microfilm, and other sensitive media

Our [secure chain of custody process](#) allows you to quickly retrieve important case documents and submit and process subpoena requests. And all stored documents are digitally accessible 24/7 with our records management software.

Finance & Banking

Our information governance and records management solutions can be tailored to a wide variety of uses within the finance and banking industry. We can help store and manage your client's private documents and transaction statements in accordance with all federal rules and regulations including FACTA, SOX, GLBA, and more.

Our off-site storage and digital backups can help mitigate the loss of records in the event of a natural disaster, security breach, or other black swan events. Our document imaging and scanning services can also help your institution make the transition to paperless, saving you time and money in the long term.

Insurance

Our document management solutions are perfectly tailored to fit with the complex requirements of the insurance industry. We provide document storage, scanning, and records management software that can be customized to match the complexity of your own retention schedules, user permission groups, and internal file organization system.

Our underground vaults make it easy to create secure backups of your most important files, while the [Access Classic | Services Portal](#) makes it easy to access those files anywhere, any time. We'll also help manage your stored document retention schedules and securely destroy any documents once they are no longer needed.

Energy

Whether your records are digital or physical, you want reliable and easy access so your team can focus on the project, not the process. Reduce legal risk with best-in-class processes that sets and governs standards. Free your staff to work on higher value activities while enjoying economies of scale with bundled records management solutions. Our team is experienced with the unique requirements of:

- Land files
- Surface, mineral, easement, contract and joint venture files
- Well files and logs
- Pipeline files
- Environmental files
- Special media and oversized documents

Manufacturing

Your company should be focused on building and designing things, not worrying about document management and record retention schedules. We can help streamline your industrial and manufacturing records including:

- Inventory and production records
- Sales, invoices, purchase orders, and tax documentation
- HR and employment documentation
- Compliance and safety forms

Furthermore, offsite storage provides critical backups of your key documents in the event of a fire, natural disaster or other emergency events at your facility.

Government

Government agencies are subject to rigorous federal, state, and local regulations specifying how and for how long documents and records must be stored. Our government-focused records management services are built to help your agency comply with all local regulations, freeing up your team to focus on more important work.

Given the volume of paper documents that must be retained and managed for many government agencies, offsite records management solutions can greatly reduce the need for on-site storage space, which ultimately saves costs in high-rent areas. Additionally, countless man hours can be saved by switching to a digital document management solution.

Education

Schools and educational agencies are often subject to similar document storage and regulatory compliance rules as government agencies. Between document privacy regulations, retention schedules, and ensuring backups in the event of a natural disaster, managing records for your school, college, or university can be a time-consuming and expensive process.

Our records management services for schools and educational organizations securely handle all student information in accordance with all relevant regulatory frameworks (HIPAA, FERPA, IDEA, and more). We also offer decentralized digital transformation solutions that can help your team quickly access digitized documents, perfect for schools with multiple facilities or distributed campuses.

Automotive

Your showroom should be focused on cars, not document storage. We help automotive dealers and manufacturers reduce the need for keeping physical records on-site, while providing the tools to manage and protect those important records digitally.

We can help store and manage all dealership-specific records such as:

- Department of transportation vehicle records
- EPA waste and emission records
- Buyer records and credit applications for the FTC and Truth in Lending/Leasing Acts
- Employee, payroll, and sales records

Retail & Hospitality

Managing a service-focused business is complicated enough without having to think about regulatory compliance, retention schedules, and other common records management problems. We help retail businesses, hotels, restaurants, and stores of all sizes manage their daily business records so they can get back to focusing on what matters most: client satisfaction and efficiently running the business.

We can help manage everything from decluttering locations by going paperless, and providing guidance on compliance and retention schedules, to scanning and digitizing documents so you can access them 24/7.

ARC



Scan-by-Box Service Agreement

This service agreement is designed to outline the processes which ARC will implement, to complete a successful capture and conversion of targeted hard copy documents into electronic form, for City of Delray Beach; hereinafter referred to as "Customer". In addition, this agreement will indicated team responsibilities and expectations as the documents are being processed.

City of Delray Beach

100 Northwest 1st Avenue
Delray Beach, Florida 33444

Lisa Castronovo

castronovol@mydelraybeach.com
+15612437289

Reference: 20260813-162741630
Quote created: August 13, 2026
Quote expires: September 12, 2026

ARC Document Solutions, LLC

1000 Clint Moore
Suite 107
Boca Raton, FL 33487

Prepared by: Kristen Seal

Document Solutions Consultant
kristen.seal@e-arc.com
+17865849924

PRODUCTS & SERVICES	QUANTITY	UNIT PRICE	PRICE
Standard Service (per Box)	31	\$279.00	\$8,649.00

PRODUCTS & SERVICES	QUANTITY	UNIT PRICE	PRICE
HIPAA Compliant Service (per Box)	4	\$20.00	\$80.00
Certified Document Shredding (per Box)	31	\$10.50	\$325.50
Document Transport and Loading	1	\$300.00	\$300.00

Total	\$9,354.50
-------	------------

Comments to buyer:

To: The City of Delray Beach, in care of Lisa Castronovo:

Thank you for the opportunity to quote your scanning project. The confidentiality of your documents is our highest priority. Ensuring the privacy and security of healthcare records is essential for any organization handling sensitive patient information. HIPAA-compliant scanning services offer a secure and efficient way to transition from physical records to digital workflows. These services not only protect patient data but also streamline accessibility, making healthcare operations more efficient and effective.

Professional document scanning services ensure that all patient records are managed in secure environments. Strict protocols prevent unauthorized access, safeguarding the confidentiality of protected health information (PHI). From document collection to digitization, every step aligns with HIPAA requirements to maintain trust and data security.

Advanced scanning technology ensures every detail of medical records, billing information, and other sensitive documents is captured accurately. With high-resolution imaging and Optical Character Recognition (OCR) capabilities, digitized files become searchable and easy to manage. This precise approach improves accessibility while maintaining data integrity.

The enclosed quote provides pricing per box sized 15" Long x 12" Wide x 10" High - a per unit cost. The Boxes will be picked up from your location listed below. Any boxes marked as HIPAA will be securely taped with tamperproof seal. All boxes will receive a barcode label and counted.

The City of Delray Beach HR Office 80 Depot Avenue, Suite 1 Delray Beach, FL 33444

They will be brought to our secure scanning center where the boxes will be counted again and checked. They will be prepped by removing staples, binding, prongs and clips. Barcodes will be inserted to ensure all page counts match.

Files will then be scanned as a multipage pdf per file folder and labelled according to the name on the folder as follows: Last name, Firstname. Files will then be processed for Optical Character Recognition (OCR) that provides word searchability.

A secure digital link containing the files will be sent to the email address provided. Per our discussion, I've provided the option to shred your files upon completion.

Indexing will be as follows:

Index Value #1: Box Name

Found where?: On Box

Parent Folder

Index Value #1: Last name, First name or whatever is listed on the tab

Found where?: File Folder Tab

File Folder

Please let me know if you have any questions or if you'd like to view any testimonials from our previously completed work.

Thank you!

Kristen Seal

Standard Service Included:

- At Customer request, empty boxes will be provided to customer
- When boxes are ready for pick-up, and at the request of Customer, ARC will make arrangements for boxes to be transported to ARC location for processing
- Additional costs will apply to any boxes picked up over 25 miles from ARC Service Centers or when box count is less than 5 boxes
- Once received at ARC service center, documents will be prepared by removing and discarding all document binding materials, post-it notes and flags. Binding materials will not be re-applied to hard copy when completed
 - *For the purposes of this agreement, one document will be defined as all papers contained within: a file folder, a binder, and/or a bound book, with a limit of 50 documents per box*
- Prepared documents will be scanned at a pixel density of 300 DPI, using a programmatic Auto-color mode, where documents containing a moderate amount or color will be imaged in color, and all others will be imaged as Black & White
- Documents will be indexed (up to 25 characters per field) as determined in the "Index Values Definition" Section below
- The Index Values (up to 3) must be easily identifiable on the tab of the folder, cover of book, or on the first page of the document
- Scanned documents will be processed to generate one multi-page, searchable image (OCR) PDF file for each document
- Output PDF files will be named, and foldered as defined in the Index Values Definition section below
- A .CSV file will be generated for each batch of PDF files, where the .CSV file will contain all indexed values for each document, and the digital path to where the PDF file is placed
- The resultant files will be compressed into one zipped file and transmitted to customer via a download link sent within an e-mail message
- ARC will make arrangements for boxes to be returned to customer

ARC Document Scanning Optional Services (Circle Options that apply):

- Additional Index Fields (per field, per Box) ... \$7.50
- Certified Document Shredding (per Box) ... \$10.50
- HIPAA Compliant Service (per Box) ... \$20.00
- Thumb Drive Deliverable (per Drive) ... \$25.00
- Create Custom Batch Load File (Quoted Separately)
- Document Transport beyond 25 mile mileage limit (Quoted Separately)

TERMS AND CONDITIONS

1. General:

- A. ARC's pricing for scanning services is based on a per box basis, where the box contains paper-based business documents, in relatively good condition, and where box measures 10"x12"x15", is reasonably full, not overstuffed.
- B. Boxed documents requiring low to medium levels of preparation (such as having not more than an average of 1 staple for every 20 pages), will qualify for this service. Boxed documents requiring high levels of preparation (such as having an average of more than 1 staple for every 20 pages), will be subject to additional charges. Customer will be notified by ARC, and a Change Order will be offered to Customer for approval, which will cover costs for additional work effort.
- C. ARC reserves the option to apply additional costs if the box contents does not meet the criteria defined in this Service Agreement, and/or if the Customer requirements exceed the specifications defined herein.
- D. A paper document storage option is not contemplated or included in services provided under this Agreement. Should Customer delay providing the approval for document shredding (or delay the authorization of the return of hard copy original documents upon project completion) beyond 30 days of completion, Customer will incur and be responsible for payment of document storage fees.
- E. If document shredding services are elected with this service agreement, ARC will destroy all hard copies of the Customer documents provided to ARC, and Customer shall indemnify and hold harmless ARC from any claim or liability arising from such destruction.

2. Pick-up & Delivery of Hard Copy Originals

- A. Pick-up and return delivery (if required) of originals is included if the point of pick-up is within 25 miles of an ARC service center with a 5 box minimum
- B. If the point of pick-up is outside the 25-mile limit, ARC will utilize the most efficient means for transport of the originals to the ARC service center, at which costs will be added to the Price Schedule above

3. Timeline:

- A. ARC will exercise its best efforts to complete services and deliver files within the following timeframes:
 - 1 to 5 boxes, within 10 Business Days
 - 5 to 10 boxes, within 15 Business days
 - 11 to 20 boxes, within 20 Business Days
 - Over 20 boxes, (Quote)
- B. If an alternate timeframe is required, ARC will be open to discuss with Customer to determine best way to meet the requirement

4. Change Orders:

1. Specific technical details relative to various processes are addressed in this Service Agreement and are open to change, pending Customer needs. Once agreed upon, and signed below, any future change requests must be made in writing, submitted to ARC, and a change order form will be completed so as to document the change. If the Change is significant enough to affect the costs and/or timeline for the project, then the change order form will be submitted to the Customer, indicating the affects, where the change order would be confirmed by the Customer via authorized signature.

A. Customer:

Customer represents and warrants that (i) Customer owns or has sufficient legal right to the intellectual property rights in the Customer documents, and (ii) the Customer documents, including any use thereof by ARC in performing these services, does not violate applicable law or the rights of any third party.

Services to be performed on materials received from Customer that fall outside the scope of the material outlined in this Service Agreement will be identified.

Customer will be notified so that ARC may receive additional instruction and provide Customer with pricing (if appropriate) for the handling of those extraordinary materials outside the scope of Services contemplated under this Agreement. ARC expects the documents to be of reasonably good quality which will not require extraordinary preparation prior to scanning. Should the condition of the documents require extraordinary document preparation, ARC will provide the Service for these types of documents at our published rates via a change order that will identify pricing and timeline.

B. ARC:

ARC will be responsible for executing the production requirements as defined herein, maintaining the level of accuracy, and providing the image reproduction as defined in this agreement. In the event that any unforeseen issues arise, which might jeopardize the outcome of the project (quality, accuracy, timeline and/or costs); ARC will notify the Customer who will work together to resolve such issues in a mutually beneficial manner.

5. Service Warranty:

All work produced will be covered for a 30-day warranty period from the deliverable date. Once delivered, Customer will have 30 days to review any or all documents scanned to verify the contents, completeness, and accuracy of the service provided.

At any time, Customer can request to designate a time for document review, and ARC will make the hard copy documents, and the resultant images available for review. It is encouraged that Customer randomly select a series of documents; from which Customer will run a "page-by-page" review of the hard copy documents comparing to the resultant image file, for completeness, quality and accuracy.

This document review must be completed within 30 days after delivery. Therefore, any warranty claims must be made within this 30-day period, and before authorization of destruction of the source documents.

The warranty period will end either at the close of the 30th calendar day, or upon receipt of authorization for destruction, whichever comes first.

6. Limitation of Liability:

IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY CAUSE RELATED TO OR ARISING OUT OF THIS AGREEMENT, WHETHER IN AN ACTION BASED ON A CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR ANY OTHER LEGAL THEORY, HOWEVER ARISING, FOR ANY DAMAGES BASED ON USE OR ACCESS, INTERRUPTION, DELAY OR INABILITY TO USE THE SERVICE, LOST REVENUES OR PROFITS, DELAYS, INTERRUPTION OR LOSS OF SERVICES, BUSINESS OR GOODWILL, LOSS OR CORRUPTION OF DATA, LOSS RESULTING FROM SYSTEM OR SYSTEM SERVICE FAILURE, MALFUNCTION OR SHUTDOWN, FAILURE TO ACCURATELY TRANSFER, READ OR TRANSMIT INFORMATION, FAILURE TO UPDATE OR PROVIDE CORRECT INFORMATION, SYSTEM INCOMPATIBILITY OR PROVISION OF INCORRECT COMPATIBILITY INFORMATION OR BREACHES IN SYSTEM SECURITY OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEABLE OR A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY, ARC'S maximum liability shall not exceed the aggregate amounts paid or payable to ARC pursuant to this Agreement. NOTWITHSTANDING THE FOREGOING, THIS SECTION SHALL NOT APPLY WITH RESPECT TO DAMAGES FOR BODILY INJURY (INCLUDING DEATH) AND DAMAGE TO REAL PROPERTY AND TANGIBLE PERSONAL PROPERTY.

Signature

Before you sign this quote, an email must be sent to you to verify your identity. Find your profile below to request a verification email.

Lisa Castronovo

castronovol@mydelraybeach.com

Verify to sign

Porschea McConnehey

porschea.mcconnehey@e-arc.com

Verify to sign

DOCUFREE

Castronovo, Lisa

From: Patrick Dooling <Patrick.Dooling@docufree.com>
Sent: Tuesday, July 28, 2026 12:32 PM
To: Castronovo, Lisa
Cc: Pension
Subject: Re: Document Scanning Project for City of Delray Beach

Follow Up Flag: Follow up
Flag Status: Flagged

You don't often get email from patrick.dooling@docufree.com. [Learn why this is important](#)

Hi Lisa,

Thank you for the additional information.

Based on the scope you've described, a preliminary budgetary estimate would be approximately \$260 per box, which includes:

- One-way shipping to Docufree
- Scanning to one searchable PDF per folder
- Folder name indexing
- Secure destruction of the records following scanning

Since you mentioned you would like the folders returned, the cost would be approximately **\$290 per box** to cover return shipping and handling.

Please note that this budgetary estimate is based on approximately 30 boxes with an estimated 2,500 pages per box and the project requirements outlined below. Any significant changes to the volume of records or project scope may affect final pricing.

If you'd like to move forward, I'd be happy to provide a formal proposal. If you'd prefer to discuss the project first, I'm also available for a brief call.

Best regards,

Patrick Dooling, CIP
Product Line Manager



Docufree

Exceeding Industry Standards for Compliance



INFORMATION MANAGEMENT SOLUTIONS FOR A VARIETY OF INDUSTRIES

Industries We Serve

Docufree provides services and solutions targeted to meet your specific requirements. We allow organizations to enhance productivity and improve workflow while increasing security and ensuring regulatory compliance. Docufree has developed secure document automation and information management solutions that address the specific needs of various industry verticals.

CORPORATE

Corporate files range from confidential contracts to private HR files and beyond. These documents are a corporation's vital records. They must be safely stored, secure, easy to access instantly, and searchable.

[how we work with corporate](#)

HEALTHCARE

Patient records and billing info are extremely sensitive, confidential, and paper-intensive records. Holding on to these records in your office or in storage introduces the risk of natural disasters, fire hazards, lost documents, and human error.

[how we work with healthcare](#)

LEGAL

Legal documents require the upmost confidentiality, care, and security. Your firm has high standards. Don't let your operations get bogged down in the messy world of paper. Your file management should give you an edge...better client service, instant document search ability, and the state-of-the-art security.

[how we work with legal](#)

FINANCIAL, INSURANCE AND REAL ESTATE

An industry full of paper. Not only are Financial, Insurance and Real Estate processes inherently document intensive, they are also riddled with security and regulatory compliance requirements. Document storage is an inefficient use of your budget, and finding old paperwork is a time consuming hassle.

[financial, insurance, and real estate](#)

EDUCATIONAL

Docufree works with many leading educational and research institutions on the local, state and national levels. We help these institutions achieve increased productivity and efficiency with corresponding decreases in paper volumes, storage and staffing costs.

[how we work with education](#)

GOVERNMENT

Docufree assists many government organizations at the local, state and federal levels. Our solutions eliminate the government's massive paper records and their storage costs.

[how we work with government](#)

ENERGY & UTILITIES

Organizations in the Energy industry face document challenges in a broad range of functions. Exploration, production, refining, support services, contract management and marketing all add up to rooms full of paper.

[how we work with energy & utilities](#)

Security by Design

A strong foundation of security and privacy is at the core of everything we do. Docufree is very proud of our security record and our staff works diligently to maintain the greatest levels of security and privacy possible. We are the only SaaS vendor to accept total accountability for the chain of custody from time a document enters the mail room until your staff or systems accesses it programmatically. We have over a decade of experience protecting and processing sensitive information. From a security perspective, our data centers have stringent regulations and we design and test Docufree® with security and privacy as top priorities.



Docufree frequently performs security assessments drawing on software vulnerability categories from (National Institute of Standards and Technology (NIST), Common Weakness Enumeration (CWE), and OWASP to provide a thorough risk assessment. Some of the areas of the application that are tested for that various vulnerability attack scenarios include:

- Access Control
- Administration Interface
- Application Server Configuration
- Authentication
- Caching
- Code Quality
- Cross-site Scripting
- Cryptography
- Denial of Service
- Error Handling
- External Communications
- Input Validation
- Interpreter Injection
- Logging
- Malware
- Privacy and Compliance
- Session Management
- SQL Injection
- Thread Safety

Docufree® Document Cloud

Docufree has been architected, developed and deployed in compliance with OWASP (Open Web Application Security Protocol) Top Ten best practices. These are the same security practices used by the U.S. Defense Information System Agency and required for DOD Information Technology Security Certification and Accreditation Process to secure their Web applications. Global companies like IBM Global Services, Price Waterhouse Coopers and Swiss Federal Institute of Technology also follow these same security practices.

Access Controls

Docufree employs an advanced access control framework built into the core solution that enables secure authentication, records logs of user activity and allows administrators to control which users have access to highly sensitive documents. Users can view the detailed audit trail which shows which users have viewed and acted on any given file.

Testing & Assessments

The Docufree development lifecycle includes steps for performing vulnerability testing and applying any necessary remediation to ensure that the application is secure at the source. In addition, Docufree sub-contracts with security experts who specialize in identifying flaws in source code that expose business-critical applications to potential attack through rigid vulnerability assessments to ensure we are continually identifying security vulnerabilities and producing actionable results to take appropriate action to reduce risk to business operations.

Encryption

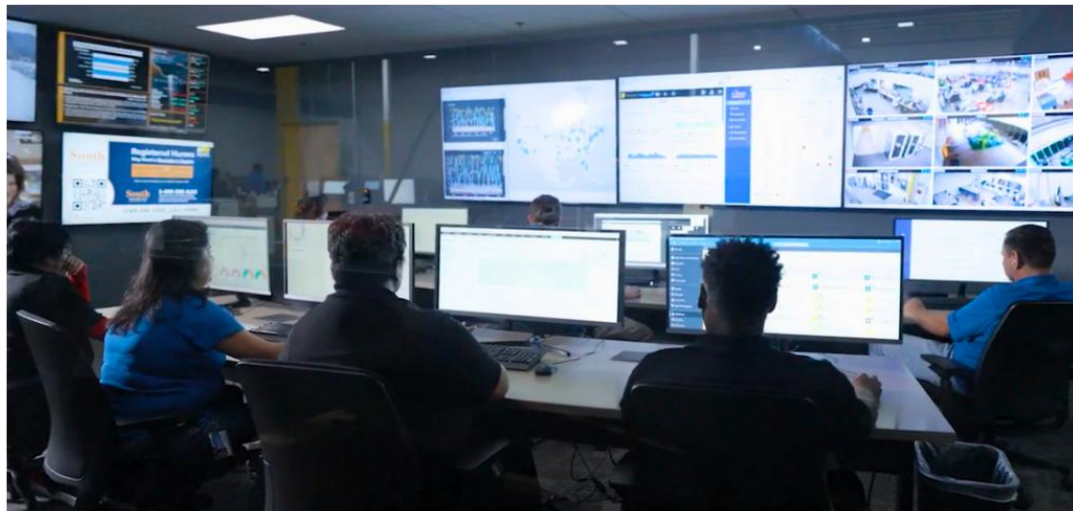
Docufree stores documents with 256-bit encryption, the highest level of encryption available. Data is securely transmitted using industry standard TLS 1.3 encryption to manage the security of message transmissions on the internet. Docufree utilizes multiple, strong cryptographic encryption keys, which are created using a random generator and AES 256-bit encryption, to meet the stringent Payment Card Industry (PCI) compliance standards, ensuring proper access. AES stands for Advanced Encryption Standards which provides strong encryption to protect electronic data. Docufree maintains Universal Threat Management (UTM) appliances for intrusion detection and prevention when transmitting data. And, Docufree grants access to users based on a strict set of permissions for controlled access.



Docufree® Physical Environment

Docufree corporate facilities control every aspect of physical access, data integrity, network speed, safety, and power management to make sure that your data is safer with us than it would be in your own facility. Our Docufree staffed network operations center (NOC) continuously monitors for intrusion detection every hour of every day throughout the year, and we provide a redundancy to ensure that your data will always be available.

Access to our facilities is strictly controlled through the use of biometric sensors at each entry into the Secure Zone with only authorized employees accessing the data center rooms. No cameras, cell phones and jackets are allowed in the secure work areas and all our employees are subject to criminal background check, credit check and random drug testing. Closed loop video surveillance cameras track activities in every room except the obvious. And, Docufree grants access to users based on a strict set of permissions for controlled access.



Security Checklist

Physical Environment

- ✓ **Secure Area:** IT facilities supporting critical or sensitive business activities are located within secure areas.
- ✓ **Physical Security Perimeter:** Strategically located barriers around defined perimeters provide physical security protection throughout the facility where sensitive business activities occur.
- ✓ **Physical Entry Controls:** Only authorized personnel can gain access to secure areas by use of biometric fingerprint scan.
- ✓ **Security of Data Centers & Computer Rooms:** Physical security for data centers and computer rooms is established that is commensurate with possible threats.
- ✓ **Isolated Delivery & Loading Areas:** The data center and computer room delivery and loading areas are isolated to reduce the opportunity for unauthorized access.
- ✓ **Equipment Location & Protection:** Equipment is located to reduce risks of environmental hazards and unauthorized access.
- ✓ **Power Supplies:** Electronic equipment is protected from power failures and other electrical anomalies.
- ✓ **Cabling Security:** All power and telecommunications cabling is protected from interception or damage.
- ✓ **Equipment Maintenance:** Procedures are established to correctly maintain IT equipment to ensure its continued availability and integrity.

- ✓ **Separation of Development & Operational Facilities:** Development and operational facilities are segregated to reduce the risk of accidental changes or unauthorized access to production software and business data.
- ✓ **Environmental Monitoring:** Host computer environments, including temperature, humidity, and power supply quality, are monitored to identify conditions that might adversely affect the operation of computer equipment and to facilitate corrective action.
- ✓ **Media Handling and Security:** Computer media is controlled and physically protected to prevent damage to assets and interruptions to business activities.
- ✓ **System Planning & Acceptance:** Advance capacity planning and preparation ensures the proper availability of adequate capacity and resources as customer demands grow.

Network Management

- ✓ **Protection from Malicious Software:** Precautions are taken to prevent and detect the introduction of malicious software to safeguard the integrity of software and data.
- ✓ **Virus Controls:** Virus detection and prevention measures and appropriate user awareness procedures have been implemented.
- ✓ **Network Monitoring:** Security of computer networks are monitored 24x7 and managed to safeguard information and to protect the supporting infrastructure.
- ✓ **Network Security Controls:** Appropriate controls ensure the security of data in networks and the protection of connected services from unauthorized access.

Electronic File Access

- ✓ **256 Bit Encryption:** Data stored on the file server is encrypted using 256-bit encryption.
- ✓ **Secure Transmission:** All communication is delivered using industry standard TLS 1.3
- ✓ **Access Controls:** User access to files is strictly granted on permissions basis where administrators can quickly change permissions.
- ✓ **Active Directory Integration:** You can manage your users from Active Directory ensuring you only need one user store.

Policies & Procedures

- ✓ **Clear Desk Policy:** Employees working with or viewing sensitive information must work on a clear desk to reduce risks of unauthorized access, loss, or damage outside normal working hours.
- ✓ **Data Handling Procedures:** Procedures exist for handling sensitive data to protect such data from unauthorized disclosure or misuse both when onsite or in transit.
- ✓ **Removal of Property:** Personnel are required to have documented management authorization to take equipment, data or software off-site.
- ✓ **Operational Procedures & Responsibilities:** Responsibilities and procedures are established for the management and operation of all computers and networks.
- ✓ **Documented Operating Procedures:** Operating procedures are clearly documented for all operational computer systems to ensure their correct, secure operation.
- ✓ **Incident Management Procedures:** Incident management responsibilities and procedures are in place to ensure a quick, effective, orderly response to security incidents.
- ✓ **Operational Change Control:** **Documented** procedures are established for controlling changes to IT facilities and systems to ensure satisfactory control of all changes to equipment.
- ✓ **Data Back-Up:** Documented procedures are established for taking regular back-up copies of essential business data and software to ensure that it can be recovered following a computer disaster or media failure.
- ✓ **Operator Logs:** Routine procedures are established for taking back-up copies of data, logging events and faults, and where appropriate, monitoring the equipment environment.
- ✓ **Management of Removable Computer Media:** Procedures exist for the management of removable computer media such as tapes, disks, cassettes, and printed reports.
- ✓ **Fault Logging:** Procedures exist for logging faults reported by users regarding problems with computer or communications systems, and for reporting and taking corrective action.
- ✓ **System Acceptance:** Acceptance criteria for new systems are established and tested are prior to customer rollout.
- ✓ **Vulnerability Testing:** Procedures exist to test for all OWASP categories of vulnerabilities on an ongoing basis.



Compliance

PCI-DSS 4.01

Docufree shows its commitment to secure processing and protection of information by completing the **Payment Card Industry Data Security Standards (PCI DSS)** program. Through the PCI DSS Program, several security and policy requirements must be addressed including access to data, firewall integrity, encryption of stored data, physical security and a wide range of business, human resources, and policy issues. Annual audits by Qualified Secured Assessors ensure Docufree's compliance with the security and policy requirements of the PCI program.

HIPAA / HITECH

Annual assessments performed by qualified assessors ensure Docufree's compliance with the privacy and policy requirements of the **Health Insurance Portability and Accountability Act (HIPAA)**. HIPAA stipulates how healthcare related Personally Identifiable Information should be protected from fraud and theft. It is composed of national regulations for the use and disclosure of Protected Health Information (PHI) in healthcare treatment, payment and operations by covered entities.

SOC 2 Type II

Annual audits ensure that Docufree has the policies and processes in place to ensure the operating effectiveness of validated and tested controls. A SOC-certified organization has been audited by an independent certified public accountant who determined the firm has the appropriate SOC safeguards and procedures in place. It requires companies to establish and follow strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

Summary

Docufree prides ourselves on our focus to each granular detail in securing our customers sensitive data so that your data is much safer with us than it would be in your environment. We secure the physical environment tightly, screen our employees prior to and after hire, and follow rigid security methodology in our development lifecycle process and continuously test our source code for any vulnerabilities. If you have additional questions about our security policies and activities, please send us an email or call using the information below. Also, if you'd like to tour one of our centers we can arrange this for you too.