Privacy + Security + Integrity

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® 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. Data is securely transmitted using industry standard TLS 1.2 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.

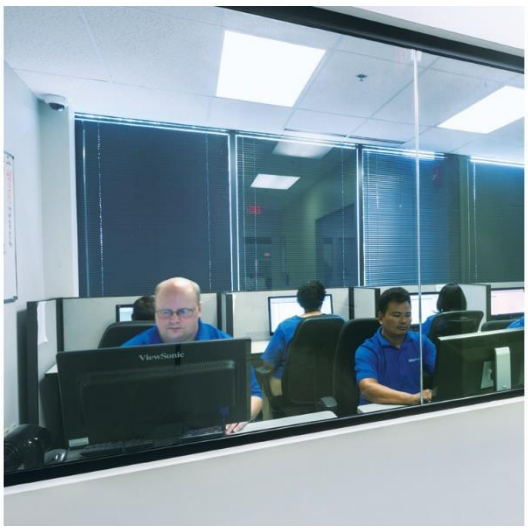
Docufree frequently performs security assessments drawing on software vulnerability categories from National Institute of Standards and Technology (NIST), Common Weakness Enumeration (CWE), and OWASP to provide a thorough risk assessment. Some of the areas of the application that are tested for various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

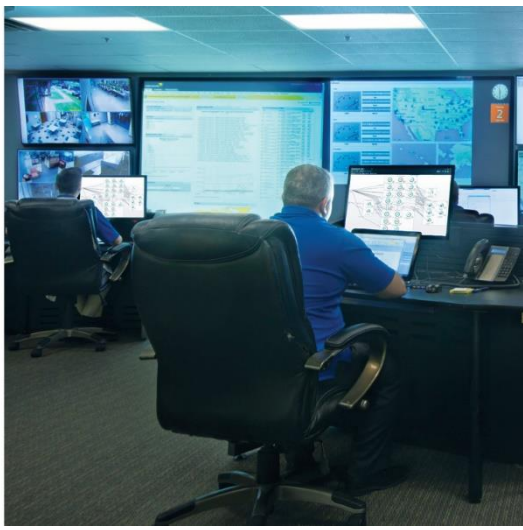
- Access Control
- Administration Interface
- Application Server Configuration
- Authentication
- Caching
- Code Quality
- Cross-site Scripting
- Cryptography
- Denial of Service
- Error Handling
- External Communications
- Input Validation
- Interpreter Injection
- Logging
- Malware
- Privacy and Compliance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

Docufree® 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 redundant data center to ensure that your data will always be available. Our remote back-up data center located in Cincinnati, OH is also an industry leading Tier 3 data center hosting well known high demand applications.

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, or 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.





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 at rest is encrypted using 256-bit encryption.
- ✓ **Secure Transmission:** All communication is delivered using industry standard TLS 1.2
- ✓ **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.

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, follow a 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 or would like to schedule a tour of our facilities, please send us an email or call using the information below.

(877) 362-3569
info@docufree.com
www.docufree.com

Compliance

PCI DSS

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.

Privacy Shield

Docufree is compliant with both the **EU-US Privacy Shield Framework** and the **Swiss-US Privacy Shield Framework**. The Privacy Shield is a framework for regulating transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. One of its purposes is to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens.

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.