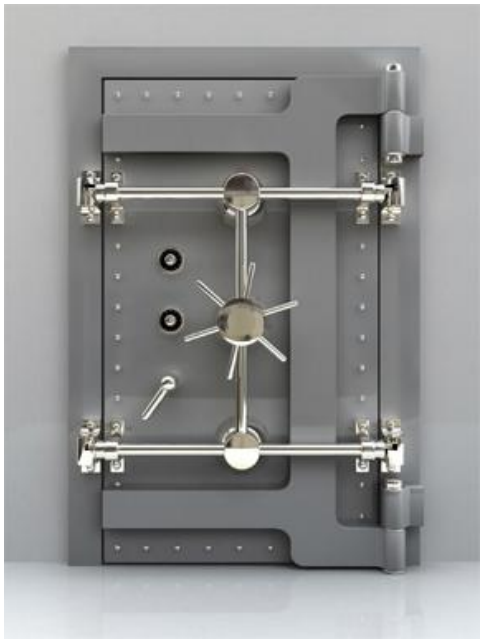
RICOH

Security White Paper

Software as a Service
Document Management



As more organizations turn to the “cloud” and the Software as a Service (SaaS) model for solutions to address a wide range of business needs; security remains a top concern. This paper examines security features of Software as a Service (SaaS) solutions and Ricoh’s DocumentMall, a SaaS document management solution. It is intended to offer information to assist organizations evaluating SaaS solution providers and solutions such as DocumentMall. Section one (1) discusses SaaS and it’s advantages compared to traditional in-house solutions. Section two (2) provides high-level security requirements to help organization evaluating SaaS providers. Security is examined from the physical, technical and process aspect SaaS vendors can take to ensure the safety and security their clients’ data including SSAE 16. Section three (3) describes the security features of Ricoh’s SaaS platform and the DocumentMall document management solution.

Ricoh Americas Corporation | 5 Dedrick Place | West Caldwell, NJ 07006

This page is intentionally left black for duplex printing

Table of Contents

This page is intentionally left black for duplex printing

1 In-House vs Software as a Service (SaaS)

The concept of Software as a Service (SaaS) has been receiving considerable notice of late as an attractive alternative to in-house software applications for many businesses. In-house systems are those that are purchased, installed, and maintained by the customer. For many years this has been the traditional approach to deploying and using software applications. SaaS systems can provide the same functions as an in-house system, but are accessed remotely by the customer, and these systems are owned and maintained by a third party vendor.

So why would a company consider an outsourced or SaaS solution rather than a more traditional in-house solution? There are some obvious answers to this question and some that are less obvious, and most have to do with the inherent differences between these two approaches to providing application capabilities.

Cost of ownership: According to Gartner, a global IT research firm, the annual cost to own and manage software applications can be up to four times the cost of the initial purchase. As a result, companies end up spending more than 75% of their total IT budget just on maintaining and running existing systems and software infrastructure. This is particularly troublesome for small to medium sized businesses (SMBs) that have limited IT resources. SMBs and large corporation are faced with increasing regulations and demands for information security. While there are many solutions designed to address these challenges, a full enterprise-level solution can run into millions of dollars. SMBs and large corporations alike are turning to the SaaS model to deliver the same capabilities as in-house systems, but at a fraction of the cost and with virtually no IT involvement on their part. SaaS Systems are owned and managed by a trusted third party vendor, so there are minimal software, capital, and support costs incurred by the customer.

Rapid Deployment and Ease of Use: Large in-house systems can take many months or even years to deploy. SaaS systems can often be made accessible to the user literally in minutes, with little or no client-side software installation or configuration required. This ability makes SaaS systems ideal for companies who need to begin using the systems quickly. In addition, SaaS systems are often configured specifically to allow even casual users to quickly and easily become proficient without requiring substantial training.

Remote Access and Collaboration: Most of today's SaaS systems are accessed through the internet, and as such allow information to be made available remotely from anywhere in the world, 24 hours a day. SaaS systems also provide their own security models to control what users are authorized to access on the system and under what conditions. These determinations are under the control of the customer, and require no changes to their existing internal networks or security policies. In combination, these two facts make SaaS systems ideal for companies who need to share business information or collaborate with remote offices or external business partners.

Focusing on Core Competencies: Todays business applications are often very complex requiring considerable expertise to install, configure, and maintain. Likewise, for most effective use, those charged with managing the systems must have specific domain expertise for the

application in question, whether it is targeted to financials, human resources, or document management. For in-house systems, this expertise must reside with the customer. Unless this application is directly related to the customer's core business, this causes a distraction of focus to an area outside the company's core competency. With a SaaS system, the domain expertise resides with the vendor, and the customer can dedicate their resources to what they know best.

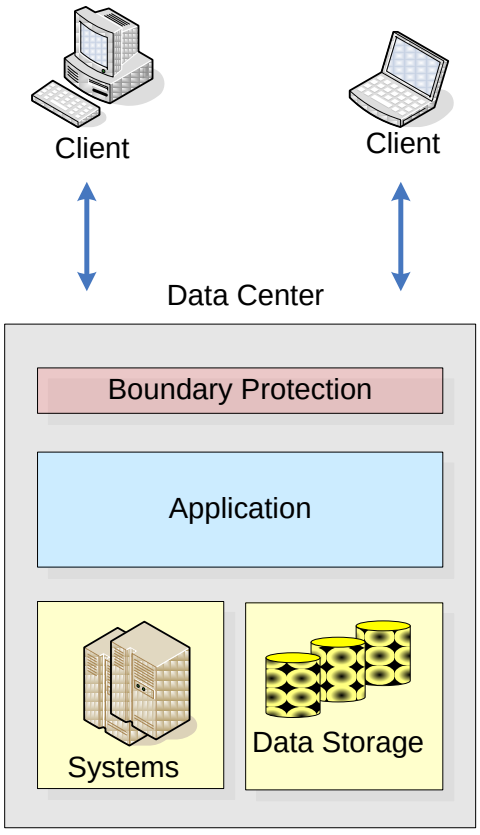
Security and Disaster Readiness: One of the most compelling advantages of a SaaS system is the potential to dramatically improve security and protect the customer's business assets. These advantages are realized due to a number of factors inherent in a well-designed SaaS system. The best systems of this type are designed and implemented by technical experts to ensure maximum security for their customers' data. The application itself provides far greater access control and security than typical paper filing systems. Since the data is stored remotely from the customer's site and located in data center operations, the risk of data being destroyed should the customer's facility suffer a fire, flood or any natural disaster or criminal activity is eliminated. Data center procedures as well as physical and virtual security can also drastically reduce employee theft and misuse of data. All data maintained by a SaaS system is routinely backed up and stored in redundant locations, so the ability to recover from nearly any type of disaster is dramatically improved.

Given the importance of security as a key component of any SaaS system, the remainder of this document will address in a broad sense some of the key aspects of security that a user or customer should consider.

2 Security Requirements for a SaaS System

2.1 What is Security?

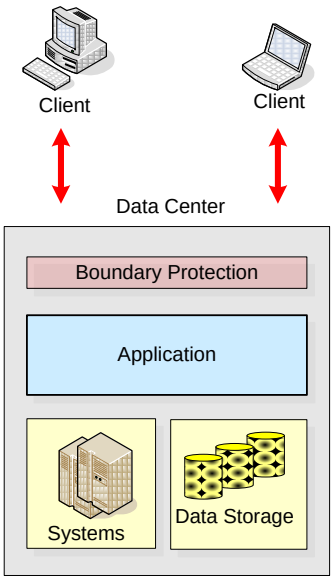
Foremost among many customers' concerns with remotely managed, or SaaS system is the assurance that the critical corporate data they are managing with the solution will remain safe, secure, and accessible. Security in a broad sense encompasses many different aspects of process and technology, but in a general sense "safe" means the data will be physically protected from loss or corruption, "secure" means only authorized personnel inside or outside the customer's organization can use the data, "accessible" means that the data is available to authorized users whenever and wherever it is needed. These high-level requirements should be considered paramount when evaluating any on-demand software or service offering, and any vendor providing such a solution must ensure that all physical, technical, and process aspects of their offering are specifically designed to address these requirements. The simplified diagram will be used to illustrate various facets of security in an on-demand system.



The following sections provide a brief overview of some of these security considerations.

2.2 PROTECTION OF CONFIDENTIAL DATA

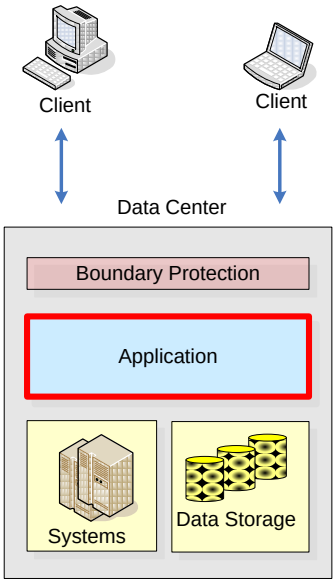
2.2.1 TRANSMITTING INFORMATION



The nature of a SaaS offering is such that the application itself (server) resides remotely from the user (client), so data is routinely transmitted over a network, often the public Internet. Unless precautions are taken, it is possible that proprietary data being transmitted from one location to another could be intercepted and accessed without the user's knowledge. To prevent this possibility, all sensitive data transmissions between the client and server should be encrypted. While encryption does not prevent the transmitted data from being intercepted, it renders it unintelligible and unusable should it be captured in transit. There are a number of well-respected companies that provide digital certificates allowing strong 128-bit encryption of data as it is being transmitted back and forth between different locations. This method of encryption is a well-accepted standard in the industry and is used by many financial institutions for secure online processing of customer information.

2.2.2 INTERACTING WITH THE APPLICATION

Assuming the transmission of data between the client and server is secure, the next consideration is how the application itself ensures that data is accessible to only those people authorized to use it. The application has to address this requirement at several levels. First, any access to the application must be restricted to individuals authorized by the customer's administrator. Each individual user must have a unique user name and password, and the administrator should be able to set password policies consistent with the customer's unique security requirements. Password policies may be set to require a minimum number and combination of characters (upper/lower case, special characters, etc), reject easily-guessed passwords, or force users to change their passwords after a given period of time. Using such policies can reduce the likelihood of unwanted users accessing the system.



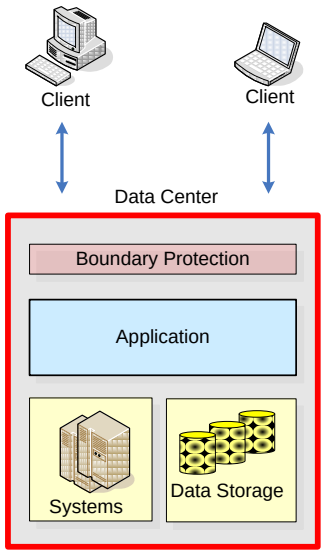
Within the application itself, options must be provided to define what levels of access users have to any particular piece or collection of data. For example, if personnel documentation is being managed, everyone in the Human Resources department may have complete authority to create, edit, or delete the document, while an individual's manager may be able to read the documents but not change them, and everyone else is prevented from seeing the documents at all. Some advanced systems will provide multiple levels of access control to allow flexibility over each individual's level of access to each item of information being managed.

2.2.3 UNDERSTANDING AND MONITORING USAGE

Even when all security policies and controls within an application are adhered to, it is possible for authorized users to abuse or misuse information. Oftentimes this is not a shortcoming of the system itself, since is can be completely dependent on the customer's particular information policies, but more advanced systems will provide capabilities for customers to understand and monitor usage of their information. Such capabilities may include transaction tracking, auditing, and reporting on how, when and who is using the data in the system. The ideal scenario is that every transaction on every piece of data is captured and can be reviewed by the customer's administrative or security staff.

2.2.4 SECURING STORED DATA

Most SaaS systems utilize a 3rd party service provider to provide data center facilities and services. Data centers are typically designed and built for the purpose of running large computer systems and storing vast amounts of data. The data center vendor is responsible for maintaining systems and protecting the data from loss, corruption, or unauthorized access. Ensuring that the data storage remains safe and secure encompasses both physical security and data/network security in compliance with established security standard. Physical security protects the storage systems themselves from unwanted interference or damage. Data and network security protect the stored data to prevent unauthorized access through network breaches or data corruption by viruses, worms, or other malicious means.



Physical Security: SaaS systems can vary widely in their security models and facilities. To ensure the highest level of safety, security and availability SaaS systems should utilize a reputable vendor that can provide

- A purpose-built facility featuring power management, Heating/ Ventilation/Air Conditioning (HVAC), fire suppression, seismic engineering, tier 1 Internet connectivity
- Access controls such as security guards, cameras and biometric security with 24 x 7 surveillance and monitoring to prevent unauthorized access to the facility and the data within.

Data and Network Security: Customer data stored in the vendor's data center must be protected from loss, corruption, and unauthorized access. The network and production systems supporting the application would ideally include:

- Perimeter defenses to prevent unauthorized access to the systems and internal network. Such defenses include firewalls and intrusion detection/prevention systems, with monitoring and event logging to evaluate potential threats and take appropriate countermeasures.
- Multi-tiered system architecture to limit access and vulnerabilities due to security breaches.

- Redundant storage (RAID5) devices to prevent data loss and ensure integrity.
- Regularly scheduled data backups of files and databases and a documented recovery plan.
- Hardened operating systems on all production machines with regular security patching and vulnerability scanning.
- Virus protection to prevent malicious data corruption.

Procedural Security and Compliance: The 3rd party facility host systems relevant to their customers' financial reporting are responsible for certain controls over those systems, such as physical and environmental security. These facilities should be reviewed to ensure processes and procedures conform to recognized security standards. Statement on Standards for Attestation Engagements (SSAE) No. 16, known as SSAE 16 is the auditing standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). SSAE 16 addresses engagements undertaken by a service auditor for reporting on controls at organizations (service providers) that provide services to user entities (customers), for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). Additionaly, SSAE 16 requires that the service organization provide a description of its "system" along with a written assertion by management.

2.3 System Availability and Accessibility

A SaaS system is of no use to the customer if it is not available, so the ability for the vendor to ensure 24x7 access is a critical consideration. Achieving high levels of availability is dependent on the reliability of the physical facility in which the application resides, design of the production network and systems, and skill of the system support personnel.

2.3.1 Data Center

For reliability and availability, the data center or facility in which the SaaS system is hosted should provide full redundancy for all critical functions, including air conditioning and environmental controls, communication backbone, and electrical power.

2.3.2 Production Systems

To ensure continuous availability of a SaaS system, the production network and systems on which the application is supported must be designed with full redundancy and fail-over configurations. This includes redundant power and connectivity as provided by the data center itself. SaaS systems can be very complex, with different machines and different modules handling different parts of the job. For each distinct function, redundancy must be provided so the failure of one component does not prevent the system from functioning while remedies are made. Redundancy may be configured at one level using "hot spares", which can be swapped in by systems personnel should a primary component fail, although replacing a failed component entails some downtime for the user. A preferred approach is to have duplicate components set up for each module to provide load balancing and automatic fail-over to a secondary device, which eliminates downtime for the user.

2.3.3 SYSTEM SUPPORT

No matter how well a SaaS system is designed or developed, it is inevitable that enhancements and maintenance of the system will be required to continue to provide good service to the end user. Routine maintenance must be provided to ensure that the application is running optimally, and that the latest software and protective measures, such as virus protection, are in place to protect the system from unwanted consequences. This requires highly qualified systems personnel to manage the hardware, networking, and software components provided by the vendor.

Systems personnel must be available 24 hours a day, 7 days a week to ensure that the system remains accessible at all times, and real-time monitoring should be implemented to immediately notify the support staff should a problem occur. Given the complexity of many SaaS systems, a range of skills and experience will be necessary, and system personnel may be certified in the various components including the core application, the database, hardware, networking components, etc.

Storage systems should be fully redundant to minimize the chance of lost data or corruption, and documented backup and recovery procedures should be in place. Data backups should be done regularly and stored at a safe location, either on a separate storage area network or away from the data center for added protection.

2.4 OPERATIONAL AND PROCESS SECURITY

Security threats to internet-based applications can change on a daily basis, and require constant vigilance to protect the contents of the system. Threats may come from viruses, worms, denial of service attacks, or malicious behavior by individuals. In addition to the protective systems such as firewalls and intrusion detection systems, it is important that the vendor have documented and enforced security policies. These may include routine audits or penetration testing by a trusted third party security expert.

One way for the vendor to strengthen their system's security policies is to adopt a process leading to one of a number of well-recognized security certifications such as SSAE16. The sheer growth in outsourcing, coupled with rigorous mandates for security, governance, and compliance will force more and more businesses to comply with the SSAE 16 third party reporting standard for service organizations. SSAE 16. requires that the service organization provide a description of its "system" along with a written assertion by management.

2.4.1 SUMMARY

Security is a key factor when considering or evaluating a SaaS system for a business's requirements. Security for internet-based applications is a broad topic comprising many different aspects, each of which contributes to the overall acceptability of a solution. A well-designed and implemented SaaS system by a reputable vendor can provide the user with improved security at virtually every level, and add to the assurance that the customer's critical business information remains safe and secure.

3 DocumentMall

DocumentMall is a SaaS document management system provided by Ricoh Americas Corporation, a subsidiary of Ricoh Company Ltd., the leading supplier of office automation equipment and electronics, which for fiscal year 2007 had sales in excess of $22 billion. DocumentMall is based on the industry-leading EMC/Documentum Enterprise Content Management platform, and was designed and developed from the outset to be provided as a SaaS system. DocumentMall has been in production since 2000, and is hosted and maintained at a Savvis, Inc facility that complies with the SSAE 16 attestation standard. Recognized as a leader in Gartner's Magic Quadrant for Cloud and Infrastructure as a Service, Savvis is a global IT utility services provider in delivering secure, reliable and scalable hosting, network, and application services. With an IT services platform that extends to 45 countries, Savvis one of the world's largest providers of IP computing services.

Since DocumentMall is specifically designed and developed as an internet-based service, security of the system and the customers' data is paramount. The following sections will provide a brief overview of DocumentMall security, and address the key factors described in the previous sections.

3.1.1 Transmitting Information

All data being transmitted to and from DocumentMall uses 1024-bit SSL encryption with digital certificates by VeriSign, the industry leader in encryption technologies. With the incorporation of encryption in all DocumentMall communications, users can be sure that the information they are using remains unavailable to prying eyes.

Encrypted transmissions are used when interacting with the DocumentMall web client, when doing large-scale uploading or downloading, and when authenticating users with the system. In addition, DocumentMall is tightly integrated with Ricoh family multi-function products (MFPs – scanner/FAX/printer/copiers) to allow immediate uploads of scanned images into DocumentMall while ensuring secure 2-way communication between the MFP and the back-end system.

3.1.2 Interacting With the Application

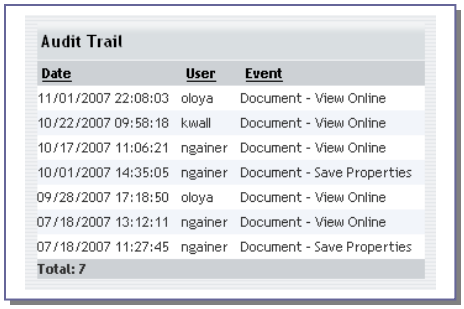
DocumentMall provides multiple levels of security within the application to ensure that customers' data is accessible to only those people authorized to use it. Through unique user names and passwords, access to DocumentMall is restricted to only those individuals authorized by the customer's administrator. The administrator can easily set password policies to support their unique security requirements. Password policies may be set to require a minimum number and combination of characters (upper/lower case, special characters, etc), reject easily-guessed passwords, or force users to change their passwords after a given period of time.

DocumentMall also provides options to allow the account administrator to define what users have access to any particular piece or collection of data. This is provided by a very sophisticated system of permission settings, which can be defined by the administrator. Seven levels of access control are provided and can be used in combination to create account-specific permission sets, or access control lists (ACLs), which can then be applied to any document or folder in DocumentMall. The supported access levels include:

- **None** - No access is permitted to the item
- **Browse** - Users can view the item's properties but not the item's content
- **Read** - Users can view both the properties and content of the item
- **Relate** - Users can do the above plus they can add annotations to the item
- **Version** - Users can do the above plus they can modify the item's content and they can check in a new version of the item (with a new version number). Users cannot overwrite an existing version or edit the item's properties
- **Write** - Users can do the above plus they can edit item properties and check in the item as the same version
- **All** - Users can do all the above, and they can delete items

3.1.3 UNDERSTANDING AND MONITORING USAGE

DocumentMall provides integrated capabilities for customers to understand and monitor usage of their information. Within DocumentMall, every transaction (uploading, reading, editing, deleting, etc.) is captured and can be used by the customer's administrator or security personnel for auditing and reporting on how data in the system is being used, by whom, and when. Transaction and audit information can be exported for use with any reporting tool the customer may want.


Audit Trail

Date	User	Event
11/01/2007 22:08:03	oloya	Document - View Online
10/22/2007 09:58:18	kwall	Document - View Online
10/17/2007 11:06:21	ngainer	Document - View Online
10/01/2007 14:35:05	ngainer	Document - Save Properties
09/28/2007 17:18:50	oloya	Document - View Online
07/18/2007 13:12:11	ngainer	Document - View Online
07/18/2007 11:27:45	ngainer	Document - Save Properties

Total: 7

Transaction tracking and audit trails are important components of many security policies, including Sarbanes Oxley, HIPAA, etc.

3.1.4 SECURING STORED DATA

Physical Security: DocumentMall is hosted at a secure data center purpose built data center located in Piscataway, New Jersey. The data center provides unsurpassed security and availability for the application. Data center security features include:

- Non-descript, purpose built data center with numerous prevention and detection technologies integrated into structure. 24-hour security monitoring and control.
- Redundant fire detection and suppression with FM200 gas suppression and/or dry pipe sprinkler system. VESDA, Smoke, Heat, and Water detection systems are also provided.

- Proximity protection provided by 24-hour security guards, video surveillance, access cards with biometric hand scanning identification, and infrared intrusion detection systems.

- Environmental Control provided by redundant CRAC cooling systems with monitored temperature and humidity controls designed with n+1 reliability.

Data and Network Security: DocumentMall's systems and procedures are designed and maintained for maximum security of customer data to protect against loss, corruption, or unauthorized access. Among the security aspects of the DocumentMall production systems and network are:

- Network perimeter defenses to prevent unauthorized access to the systems and internal network, including redundant firewalls and intrusion detection/prevention systems, with 24-hour monitoring and event logging to identify and respond to potential threats.

- Multi-tiered system architecture to limit access and vulnerabilities due to security breaches.

- Redundant and Stripped storage (RAID 50) devices to prevent data loss, ensure integrity, and improve performance.

- Continuous data replication to a physically separate storage area network (SAN) within the Savvis facility and a documented recovery plan.

- Hardened operating systems on all production machines with regular security patching and vulnerability scanning.

- Virus protection to prevent malicious data corruption.

Procedural Security and Compliance: Data center facilities for DocumentMall are provided by Savvis, Inc., a global leader in outsourced managed computing and network infrastructure. Savvis' is compliant with the SSAE 16 attestation standard and has been issued a Service Auditior's Report certifying management's description of a service organization's system and the suitability of the design and operating effectiveness of controls.

3.2 System Availability and Accessibility

3.2.1 Data Center

The data center provides 24x7 availability to ensure business continuity for DocumentMall customers. Specifically:

- Two (2) feeders from two (2) diverse electric substations provide power. The Data Center contains five (5) Power Buses. Each power Bus has two (2) 750kVA UPS and 2.0 mega-watt generators. The power system is built with n+1 redundancy.

- Internet connectivity is provided by OC-192 based IP backbone at 9953.28 Mbit/s, with redundant firewalls and routers connected to one of the largest Tier-1 Networks in the world.

3.2.2 PRODUCTION SYSTEMS

All DocumentMall system components and modules are fully redundant for maximum uptime and availability of the application. Complete redundancy allows load balancing for improved performance, as well as automatic fail-over in the event of a hardware or network failure. Ricoh has consistently exceeded our Subscription Agreement, which equates to service availability of 99.7%

3.2.3 SYSTEMS SUPPORT

DocumentMall system support is provided by a seasoned team of system and networking professionals, certified in all key components of the physical production systems and the DocumentMall application. Systems personnel are available 24 hours a day, 7 days a week to ensure that the system remains accessible at all times, and real-time monitoring is implemented to immediately notify the support staff should a problem occur.

Routine maintenance is performed to keep the application running optimally, and make sure the latest software and protective measures, such as virus protection, are implemented. All DocumentMall storage systems are fully redundant to minimize the chance data of loss or corruption, and documented backup and recovery procedures are in place.

3.2.4 DOCUMENTMALL BACKUP SECURITY

Ricoh currently mirrors two sets of on-line data at the Savvis data center. The second set of online data is continuously replicated to a physically separate storage area network (SAN). The specifications of the secondary SAN are identical to the primary production system with guaranteed availability of 99.999% uptime. In addition, real-time replication of the files and the Oracle DB are done to an alternate SAN and changes to the data are maintained for 7 days in the backup. The Backup mechanism is continually scanning all SAN content areas to maintain full synchronization of the data.

Real-time off site replication also occurs to a secondary Savvis data center located in Chicago, IL. This replication is done in real-time from the primary data center in NJ, to a backup facility in Chicago, IL. Replication occurs over a secure SSL over VPN connection utilizing a 10Mbs bandwidth peer to peer connection. The secondary Chicago replication is conducted via a disk to disk backup strategy to ensure optimal restoration times in the case of a loss of data at the primary site.

3.3 OPERATIONAL AND PROCESS SECURITY

To ensure maximum security in all phases of DocumentMall development and support, Ricoh Americas Corporation has formalized Information Security Management Systems (ISMS) policies and procedures that are documented and enforced. Developed by the International Organization for Standardization (ISO), ISO 27001 provide the guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. To ensure compliance with defined procedures, regular audits are conducted.

3.4 SUMMARY

As an industry-leading SaaS document management system, DocumentMall provides unparalleled levels of accessibility and security to our customers. From the physical infrastructure to application functionality to human factors, DocumentMall's dedication to security gives our customers the assurance and confidence they need that their critical information assets are completely secure and available 24 hours a day, 7 days a week from anywhere in the world.