1409

18

AIS
Access Imaging Solutions

Price Quote

Quote 20200731-02
Account Manager: Aemery
Email: Aemery@accessimagingsolutions.com
Office: 210-590-8338
Fax: 210-590-8322

Attn: Dan Teed
Date: 7/31/2020

Client: Navarro County
Address: P.O. Box 1018
Corsicana TX 75151
Tel #: 903-875-3330
Email: Dteed@NavarroCounty.org
Valid until: 30 Days from issue

Quantity	Part Number	Description	Unit Price	Ext. Price
1	250K 36M DM subscription	Filebound 250,000 document count, 36 month term, Document Mangmenet Licensed cloud hosted server. -Billed Yearly -Unlimited users -Unlimited Projects -includes yearly discounted rate	$6,546.00	$6,546.00
1	100K 36M DM subscription	Filebound 100,000 document count, 36 month term, Document Mangmenet Licensed	$4,627.00	$4,627.00
1	Migration Services	Perform all tasks listed within the titled documents, "Navarro County SOW.pdf" -One-time conversion cost	$3,500.00	$3,500.00
		*** Filebound is licensed by the volumn of docuemnts you are managing in your system This allows you to have unlimited users in your system. If we determine you have under 100k documents the license will be less than the 250K license. I provided both costs. If we can determine excatly how many you have in the current system we can figure out which will work for you to get started.		
			Subtotal:	
			Shipping:	
			Tax:	
			Misc:	
			TOTAL	

Access Imaging Solutions, LLC
4224 Centergate St.
San Antonio, TX 78217
www.accessimagingsolutions.com

Please email or fax all purchase orders to AIS, fax number 210-590-8322. Thank you in advance for your continued support.

(Product pricing, product availability, and product discontinuation are subject to change without notice. The quotation is valid 30 days from the date listed above.)

1410

AIS
Access Imaging Solutions

Effective January 1, 2020

Features	Document Management (DM)	[redacted]	Workflow (WF)	[redacted]	Enterprise (EN)
Document Management	X		X		X
Document Capture	X		X		X
Flexible Configuration (Defined Fields)	X		X		X
Document Library Services (Revisions, Document Locking)	X		X		X
Document Notation (Annotations, Signatures, Stamps)	X		X		X
Granular Security	X		X		X
Web-Based Viewing	X		X		X
PDF Forms	X		X		X
HTML Forms	X		X		X
Global Search	X		X		X
Online Indexing	X		X		X
Mobile Application (iOS & Android)	X		X		X
Full Text Site OCR Process	X		X		X
Advanced Workflow Processing			X		X
Flexible Workflow Designer			X		X
Automated Document Validation			X		X
Automated Escalations			X		X
Scheduled Workflow Execution			X		X
Automated Document Import					X
Automated Email Import					X
Automated Social Media Import					X
Automated Document Classification & Indexing					X
Scheduled Report Delivery					X
Responsive Web Forms					X
Responsive Web Form Designer					X
Public Search Portal					X
Forms Portal					X
Analytic Dashboards					X
DocuSign Integration					X
Records Management	Additional Cost		Additional Cost		Additional Cost

Capture	3 seats	5 seats	10 seats
FileBound Connect	X	X	X
Importer Pro	X	X	X

1411

Access Imaging Solutions

RVI MIGRATION & SETUP PROCEDURE
FOR Https://NavarroTx.filebound.com

Navarro County utilizes NetData with Real Vision Software version 8.1.1387 which was released in August 2007, to digitize, manage, and store Navarro Counties registered voter's application packages.

AIS will be providing Navarro County with the exact migration of images with the current voters file index information into Navarro Counties new Cloud FileBound site, including all FileBound project and user access setup needed.

FileBound and **AIS** will provide the FileBound Connect application that will allow Navarro County to connect the registered voter's digital application package to their voters maintenance page with in TEAMs, to eliminate the need to toggle between both application's.

AIS will setup and configure **FileBound Capture** to automate importing and filing the Texas DPS applications downloaded from TEAMs by Navarro county employee's.

AIS will setup and configure **FileBound Capture** to scan and automatically file Navarro Counties returned application in the mail.

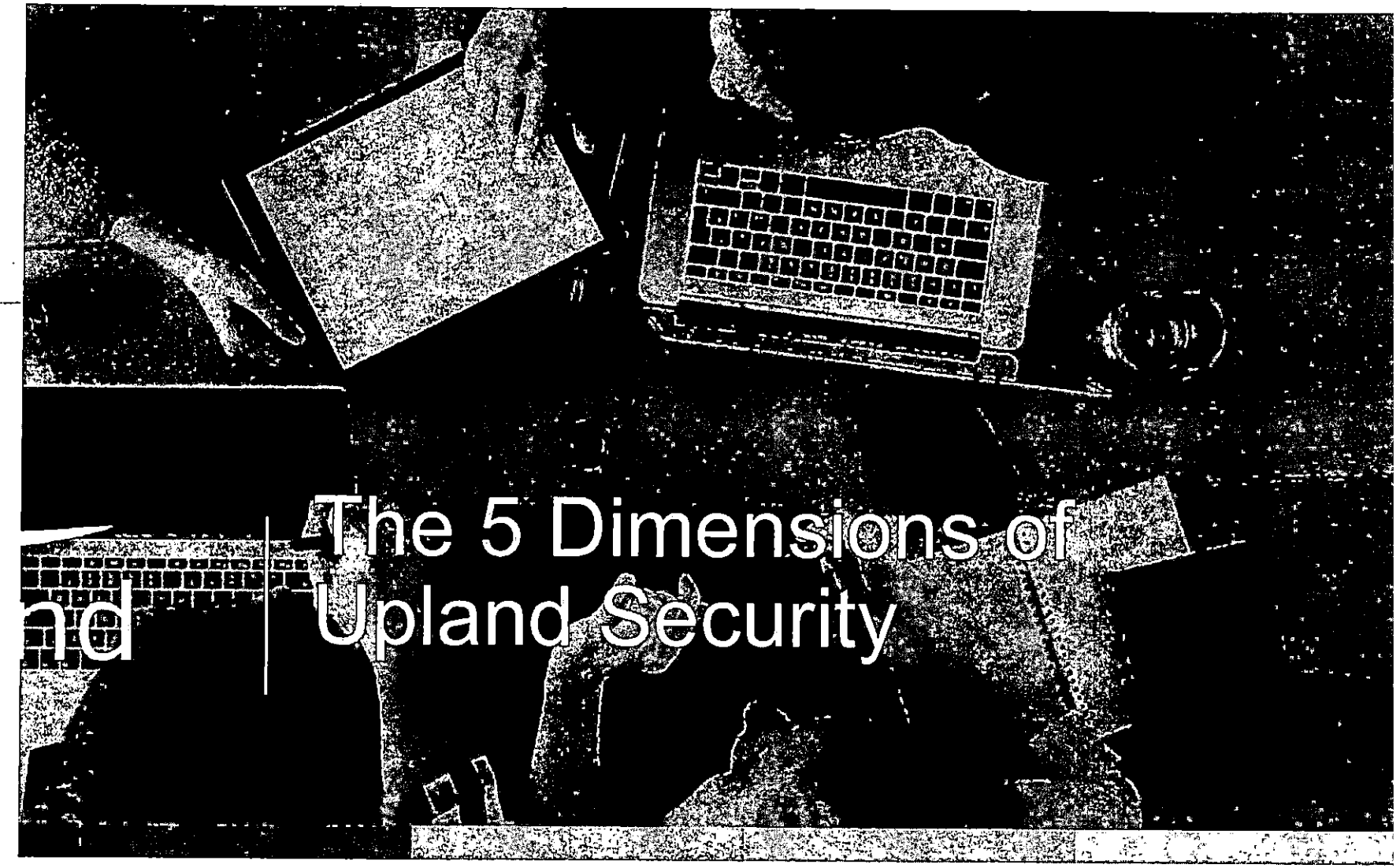
AIS will provide **Navarro County** voter registration office with the ability to maintain any of its volunteers using FileBound to automate the registration, training and testing , and deputizing of any process needed.

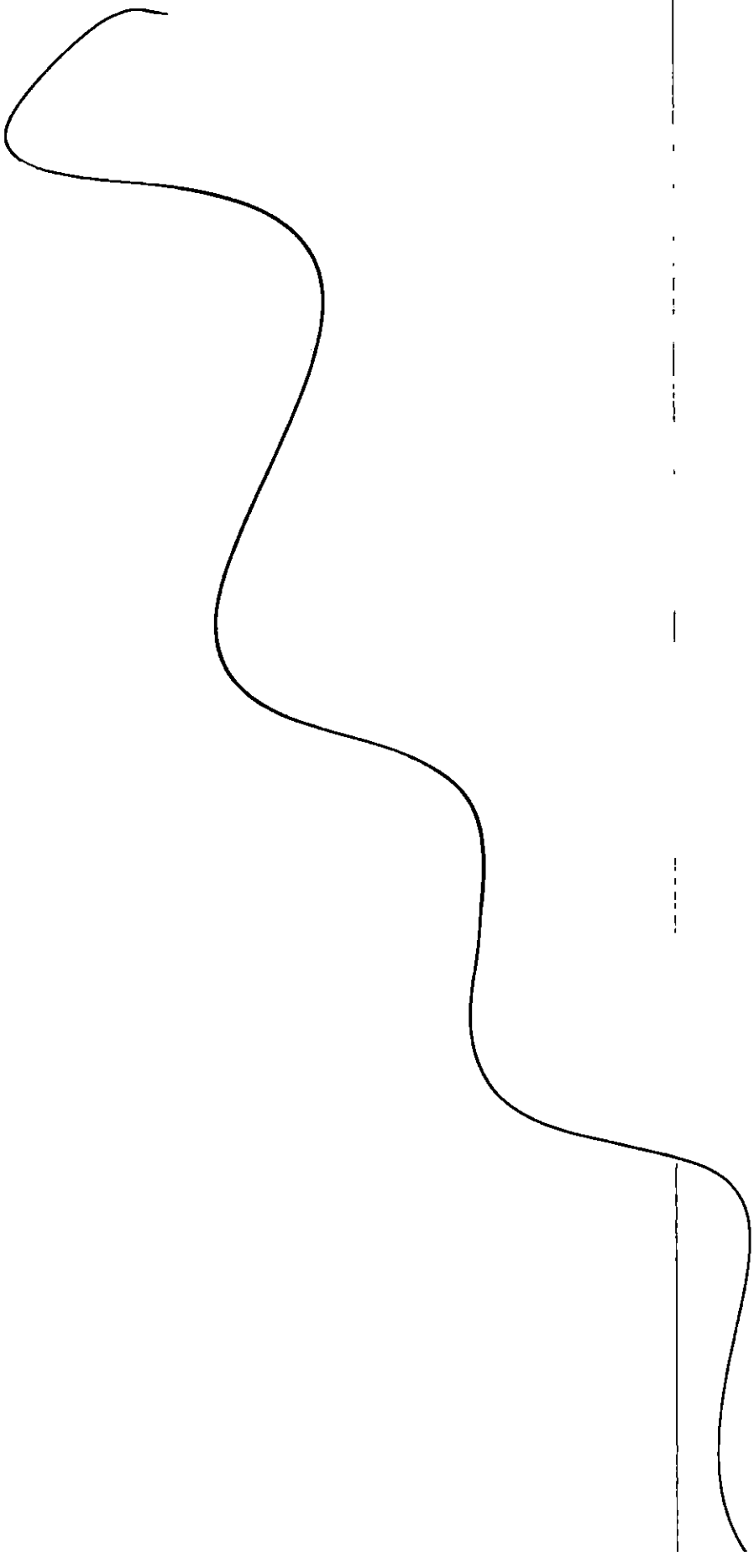
AIS intends to take the following steps for the migration procedure to export the records from the current system into **FileBound.**

1. Step 1
2. Step 2
3. Step 3
4. Step 3
5. .....

4224 Centergate St. San Antonio, Texas 78217
P 210.590.8338 F 210.590.8322

1412

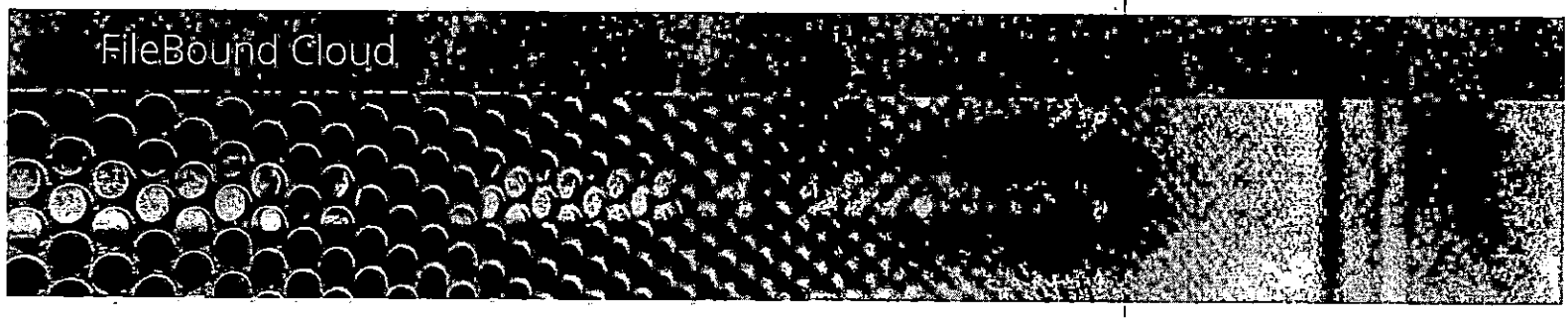




1414

upland FileBound

AIS
Access Imaging Solutions



Delivering Agile, Secure Document and Workflow Automation in the Cloud

Cloud technology has become ubiquitous. Once seen only as an opportunity for SMB organizations to scale effectively and affordably, it has become a standard for enterprises of all sizes to become more agile and focus resources more effectively.

Long before most people had even heard the term cloud, Upland was developing cloud-native solutions, making Upland's FileBound one of the most mature and robust on-demand information management applications.

Why Cloud?

- Not all work is done sitting at a desk in a central location. Cloud software is always available no matter where, when or how you want to work.
- Deploying traditional premises-based software often relies on the availability of internal resources, ranging from provisioning hardware to training administrators. Cloud Software is ready when you are, so you don't have to wait to get the benefits of your software investment.
- Needs change quickly. You might need to add new projects, additional volumes of work or new users — or maybe even a whole new division if there is an acquisition or merger. With cloud software, you can respond quickly because you don't have to wait for the system to be scaled to meet your need as it can grow to meet your needs.
- The traditional software licensing model can be a roller coaster ride of expensive upfront purchases, maintenance fees and upgrade cycles. Cloud software lets you take advantage of the economies of scale and pay a smaller, predictable fee incrementally. You realize even more savings by relying on product experts to administer the system, rather than having to train and hire additional IT resources.

Why FileBound's Cloud?

- FileBound's state-of-the-art data centers meet exacting standards for outstanding security, reliability and performance and are overseen by FileBound software experts.
- Software in the FileBound Cloud isn't just a hosted version of a legacy solution. Because FileBound is cloud-native, you don't have to compromise on functionality when you opt for a hosted solution.
- Based on your usage needs, FileBound's flexible, predictable subscription pricing is easy to understand and doesn't "nickel and dime" you by making you pay extra for every capability.

upland

1415

Concerned About Cloud Security? So are We!

Many studies show that despite the broad awareness and use of cloud solutions, security remains a major concern for most potential users. It's a major concern at FileBound too, as are performance, reliability and disaster recovery.

To safeguard our customers' critical data, FileBound has invested in best-of-breed products and services that meet the needs of customers in some of the most highly regulated industries:

- Daily vulnerability tests are performed by MacAfee, the world's largest dedicated security technology company.
- FileBound employs four independent monitoring systems, including uptime and responsiveness monitoring, from 10 locations worldwide.
- The FileBound Cloud is built using best-of-breed equipment for maximum performance and uptime, including industry-leading technology from companies like F5, Cisco, Dell, IBM and VMWare.
- Independent auditors conduct regular SSAE 16 SOC 1 Type II audits of FileBound processes ranging from product development to data center management. SSAE 16 is the standard for reporting on controls in service organizations.
- Encryption capabilities are employed to ensure that in the unlikely event that that documents are accessed by an unauthorized person, s/he won't be able to view any data.
- Quarterly third-party vulnerability assessments exceed industry security standards.
- IP-based access restriction ensures that the most sensitive data isn't shared in less secure environments, such as a mobile device connected via free airport or coffee shop Wi-Fi, by limiting the physical locations from which data can be accessed.
- Patented route control technology selects best routing path over 11 major bandwidth suppliers for optimal responsiveness.
- Data centers in Chicago, Los Angeles, Montreal and London backed up to secondary data centers in real time to ensure business continuity.
- Customer data stores are segregated to create a multi-tenant environment without having your data shared in the same logical location with someone else's.

About Upland Software

Upland Software (Nasdaq: UPLD) is a leading provider of cloud-based Enterprise Work Management software. Our family of applications enables users to manage their projects, professional workforce and IT investments, automate document-intensive business processes and effectively engage with their customers, prospects and community via the web and mobile technologies. With more than 1,600 customers and over 225,000 users around the world, Upland Software solutions help customers run their operations smoothly, adapt to change quickly, and achieve better results every day. Learn more at uplandsoftware.com.

AIS upland
Access Imaging Solutions

Access Imaging Solutions

SERVICE LEVEL AGREEMENT

The purpose of this document is to define the service levels that Supplier will endeavor to provide for the maintenance and support of the Application that Customer has obtained a subscription to pursuant to the Contract for Services Rendered ("**CSR**") between Customer and Supplier or other written agreement between Customer and Supplier governing Customer's access to and use of the Application (the CSR or other applicable agreement, the "**Agreement**") and this document (the "**SLA**") is hereby incorporated by reference into the Agreement. Capitalized terms not otherwise defined herein have the meaning set forth in the Supplier's then-current standard form of MSA applicable to the Application.

1. Application Administration. Supplier will make commercially reasonable efforts to provide the following during the applicable Subscription Term in accordance with this SLA:

- ***Technical Support***. Online and telephone support during coverage hours
- ***Service Management***. Client activation, security monitoring, change control, problem management, and escalation procedures
- ***Application Administration***. Installation and server setup, support, monitoring, response, repair, tuning and capacity planning
- ***Data backup and retention***. Backups of Customer Data stored within the Application

Customer is responsible for purchase and maintenance of its own equipment, hardware and access, including but not limited to network and data connection, to establish a connection to the Internet.

2. Service Measures

2.1. Supplier will make commercially reasonable efforts to meet the following for each Application:

Measurement	Definition	Supplier SLA
Software Availability	The periods of time that the Application is Available for use by the Customer not including scheduled downtime. **"Availability" or "Available"** means that an Authorized User can log in and access the Application.	Available in all material respects 99.5% average over a month (calculated on a 24 x 7 x 365 basis, other than Scheduled Downtime (defined below) and other than any period of downtime that lasts 5 continuous minutes or less).

4224 Centergate St. San Antonio, Texas 78217
P 210.590.8338 F 210.590.8322

Backups	Service Supplier shall conduct a full backup nightly.	Full database backups are performed nightly. Backup files will be retained for 5 days.
Restoration of Services	In the event of a major disaster, such as flooding of the hosting facility or an earthquake that destroys the infrastructure or as otherwise deemed necessary by Supplier.	Backup will be restored within 24 hours.

2.2. Exceptions to Service Levels. The Availability of the Application and the Supplier's obligations with respect to the other service measures set forth herein may be subject to limitations, delays, and other problems inherent to the general use of the Internet and other public networks or caused by Customer, Authorized Users or third parties.

Supplier is not responsible for any delays or other damage resulting from problems outside of Supplier's control; however, Supplier is responsible for the conduct of its third-party agents and contractors. Without limiting the foregoing, the following are exceptions to Supplier's obligations under this SLA:

a failure or malfunction resulting from scripts, data, applications, equipment, or services provided and/or performed by Customer;

outages initiated by Supplier or its third party suppliers at the request or direction of Customer for maintenance, back up, or other purposes;

outages occurring as a result of any actions or omissions taken by Supplier or its third party Suppliers at the request or direction of Customer;

outages resulting from Customer's equipment and/or third party equipment not within the sole control of Supplier or Supplier's agents or contractors;

events resulting from an interruption or shut down of the Application due to circumstances reasonably believed by Suppler to be a significant threat to the normal operation of the Application, the facility from which the Application is provided, or access to or integrity of data (e.g., a hacker or a virus attack);

outages due to system administration, commands, file transfers performed by Customer representatives;

other activities Customer directs, denial of service attacks, natural disasters, power and other utility outages, internet service outages, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, or other events caused by circumstances beyond Supplier's reasonable control

Customer's negligence or breach of its material obligations under this SLA, the Agreement, or any other agreement between Customer and Supplier; and

lack of availability or untimely response time of Customer to respond to incidents that require its participation for source identification and/or resolution.

2.3. Priority Levels. If the Application is not accessible as specified in Section 2.1 (an **"Issue"**), Supplier will use reasonable efforts to correct the Issue with a level of effort commensurate with the severity of the Issue. Supplier and Customer will comply with the following resolution procedures for all Issues reported by Customer:

2.3.1. Notice of Issue. If Customer encounters an Issue, Customer must sufficiently define the Issue in a written notice to Supplier (which notice may be via email). After receipt of written notice of an Issue from Customer, Supplier will notify Customer if Supplier cannot identify the cause of the Issue. If Supplier cannot identify the cause of the Issue, Customer will provide additional information regarding the Issue as Supplier may request in order to assist Supplier with identifying the cause of the Issue. Customer will provide a separate written notice for each Issue encountered by Customer. All notices pursuant to this SLA may be provided via email or a phone call followed-up by an email.

2.3.2. Issue Classification. In its notice of an Issue, Customer will reasonably classify for Supplier the initial priority of the Issue. Customer will use the nature of the Issue and Customer's business situation to initially classify each Issue. Customer will classify each Issue in accordance with the severity classification table below. To the extent that Supplier disagrees with any Issue classification provided by Customer, Supplier will promptly advise Customer of the revised classification of any Issue and the parties will resolve through good faith negotiations any disagreement regarding classification.

2.3.3. Response Time. Supplier will use reasonable efforts to respond to each of Customer's written notices of an Issue within the period set forth in severity classification table below. Response time is the elapsed time between Customer's first report of an identified Issue and the provision of a plan for resolution by a Supplier technical contact.

2.3.4. Expedited Response Time. To the extent that Customer may seek Supplier to respond to any written notice of an Issue within a time period other than as set forth in the table below, Customer

may request such response and Supplier may elect to provide such additional services to Customer on terms and conditions as the parties may agree upon in writing (which may include, without limitation, additional costs and expenses payable by Customer to Supplier in connection with such any expedited services). Notwithstanding the foregoing, Supplier will have no obligation to enter into any such agreement with respect to any such additional services. To the extent that the parties enter into any such agreement, Supplier will invoice Customer for, and Customer will pay, any such additional amounts as set forth in this Agreement (unless otherwise agreed upon by the parties in writing).

Priority Level	Issue Description	Initial Response SLA	Target Resolution Time SLA	Commitment
Priority 1	The Issue causes complete loss of service or use of the Application cannot reasonably continue as a feature or function does not allow completion of work and its operation is mission critical to Customer's business. Examples: a. Majority or all of the Authorized Users are unable to use the Application, b. Highly important reports (such as invoicing) cannot be generated, c. System crashes repeatedly after restart attempts.	1 hour during Primary Coverage hours (one hour after hours if Customer has a current subscription to a 24 x 7 x 365 support plan)	Worked on continuously until a solutions found, however, targeting an 8 hour resolution time or until a viable workaround can be applied	The Issue will be worked on until fixed or a reasonable workaround is applied. Updates will be provided to Customer every 4 hours.
Priority 2	A major Application function is experiencing a reproducible problem that causes a major inconvenience to the Customer. An acceptable workaround may or may not be available, however, operation can continue in a restricted fashion. The current release should be patched if a permanent workaround cannot be found	4 hours during Primary Coverage hours (4 hours after hours if Customer has a current subscription to a 24 x 7 x 365 support plan)	3 Business Days	The Issue will be worked on until fixed or a reasonable workaround is applied. Updates will be provided at the end of every day.

	and the next release is not imminent.			
Priority 3	The Issue causes minor loss of service or is a minor error. The impact is an inconvenience that may require a workaround to restore functionality or is a minor error, incorrect behavior, or a documentation error that does not impede the operation of a system.	24 hours during primary coverage hours	5 days or mutually agreed to time	Supplier will work with Customer to mutually prioritize and schedule resolutions into regular release cycles.

2.4. Downtime/Maintenance. Supplier periodically adds, repairs, and upgrades the data center network, hardware and the Application and shall use commercially reasonable efforts to accomplish this without affecting the Customer's access to the Application; however, repairs of an emergency or critical nature may result in the Application not being available for the Customer's usage during the course of such repairs. Supplier reserves the right to take down the server(s) at the data center in order to conduct routine maintenance to both software and hardware according to the following protocols.

Item	Description	Commitment
Standard Maintenance Window	As communicated to Customer by Supplier, not to exceed 20 hours per month.	N/A
Scheduled Uploads	Regular planned uploads of new functionality will take place during the standard maintenance window.	Minimum of 10 days' notice prior to the upload going into the production environment. The notice will be displayed on the main site where the Application is accessible
Scheduled Maintenance	Routine, scheduled maintenance will be performed inside the maintenance window.	A message will be displayed on the main site stating Supplier will be down.
Non-Scheduled/ Emergency Maintenance	May be performed outside the maintenance window and will be counted as unscheduled downtime	Customer will be notified via a message on the main site stating the Application will be down.

Periods the Application is unavailable as a result of Items 1, 2, 3 and 4 are included in the calculation of Availability.

3. Compatibility with New Third Party Software. Customer consents and acknowledges that prior to upgrading third party software, the Customer is solely responsible to verify and insure that such third party software is compatible with their current or future versions of the Application. The most significant applications that Customer should carefully check for compatibility before upgrading are: new versions of operating systems, databases, web servers, report engines, business intelligence software, accounting software, project planning tool, CRM application, reporting tools, or any other third party tools used by or integrated with the Application. Supplier will not be responsible for any failures or malfunctions' resulting from such upgrade and reserves the right not to provide support for such installations.

4. Customer Obligations

4.1. Trained Contacts. Customer will appoint up to two individuals within Customer's organization to serve as primary contacts between Customer and Supplier with regards to the Application. Customer must initiate all requests through these contacts.

4.2. Reasonable Assistance. Customer will provide Supplier with reasonable access to all necessary personnel to answer questions regarding Issues reported by Customer.

4.3. Good Standing. The provision of the Application by Supplier during the term of this SLA is contingent upon Customer's performance of its payment and other obligations under the Agreement. Supplier reserves the right, in addition to other remedies available, to suspend its provision of the Application for so long as Customer is not current with its obligations.

5. Limitation of the SLA. The scope of coverage under this SLA expressly excludes the following:

a. Maintenance and support for non-production environments and sand boxes

b. Data migration

c. Training

d. Installation, configuration and technical support for Customer equipment or operating systems

e. Technical support, consultation or problem resolution pertaining to software or applications other than those supplied by Supplier and described in this Agreement including SharePoint and Microsoft Reporting Services

f. Resolution of problems resulting from negligence of users of the Application, including specifically incorrect data entry, use of altered data and failure to use the Application according to the instructions provided in the applicable user guide

g. Support for development (Supplier SDK, Web pages, etc.), integration and custom reports, whether developed by Customer or any party other than Supplier

h. Any alterations or additions, performed by parties other than Supplier, except for programs using product interfaces provided by Supplier

i. Use of the Application on an operating environment other than that for which such the Application was designed, except as expressly prescribed in the user guide

If Customer requires that a member of Supplier's staff provide services pertaining to any of the above exclusions and Suppler agrees to provide such services, Customer hereby agrees to pay Supplier for these services according to the daily support service rate then in effect, prorated hourly.

6. Disclaimers

6.1. The parties expressly recognize that it is impossible to maintain flawless security, but Supplier shall take reasonable steps to prevent security breaches in Supplier's server interaction with Customer's network, and security breaches in Supplier's server interaction with resources or users outside of any firewall that may be built into Supplier's server. Customer agrees that it will only access and use the Application via authorized access provided by Supplier (e.g. password protected access). Supplier's Application and Data Access Control policies are available upon request.

6.2. Downloading of Data or Files. Customer agrees that it shall be solely responsible for implementing sufficient procedures to satisfy Customer's particular requirements for accuracy of data input and output, and for maintaining a separate means for the reconstruction of any lost data.

6.3. Accuracy Disclaimer. Customer is solely responsible for the accuracy and integrity of its own data, reports, and documentation. Supplier or third parties may provide links to other web sites or resources as part of the Application. Supplier does not endorse and is not responsible for any data, software or other content available from such sites or resources. Customer acknowledges and agrees that Supplier shall not be liable, directly or indirectly, for any damage or loss relating to Customer's use of or reliance on such data, software or other content.

7. Terms of Use. In addition to the terms of the Agreement and any restrictions set forth therein, the following applies to Customer's use of the Application and receipt of services hereunder. The examples of prohibited use set forth below are non-exclusive, and are provided as guidelines to Customer.

Violation of the terms of this Section 7 is strictly prohibited. In the event of any actual or potential violation, Supplier reserves the right to suspend or terminate, either temporarily or permanently, any or all services provided by Supplier, to block any abusive activity, or to take any other actions deemed appropriate by Supplier in its sole discretion.

7.1. Illegal Use. The Application may be used only for lawful purposes. The transmission, distribution, or storage of any information, data, or material in violation of any applicable law or regulation is prohibited. Without limitation of the foregoing, it is strictly prohibited to create, transmit, distribute, or store any information, data, or material which a) intentionally infringes any copyright, trademark, trade secret, or other intellectual property right (or after written notification of such infringement, fails to remedy same in a timely manner), b) is obscene or constitutes child pornography, c) is libelous, defamatory, hateful, or constitutes an illegal threat or abuse, d) violates export control laws or regulations, or e) encourages conduct that would constitute a criminal offense or give rise to civil liability.

7.2. Circumvention of Security Measures. Violations of system or network security are prohibited, and may result in criminal and civil liability. Supplier will investigate potential security violations, and may notify applicable law enforcement agencies if violations are suspected. It is strictly prohibited to attempt to circumvent the authentication procedures or security of any host, network, network component, or account (i.e. "cracking") to access data, accounts, or servers which the Customer (or its users) is not expressly permitted or authorized to access. This prohibition applies whether or not the attempted intrusion is successful, and includes unauthorized probes or scans performed with the intent to gather information on possible security weaknesses or exploitable configurations.

7.3. Attacks. Customer is prohibited from interfering or attempting to interfere with service to any other user, host, or network on the Internet ("denial of service attacks"). Examples of such prohibited activity include without limitation (a) sending massive quantities of data with the intent of filling circuits, overloading systems, and/or crashing hosts, (b) attempting to attack or disable any user, host, or site, or (c) using, distributing, or propagating any type of program, script, or command designed to interfere with the use, functionality, or connectivity of any Internet user, host, system, or site (for example, by propagating messages, via e-mail, Usenet posting, or otherwise, that contain computer worms, viruses, control characters or trojan horses).

Access Imaging Solutions

RVI MIGRATION & SETUP PROCEDURE
FOR Https://NavarroTx.filebound.com

Navarro County utilizes NetData with Real Vision Software version 8.1.1387 which was released in August 2007, to digitize, manage, and store Navarro Counties registered voter's application packages.

AIS will be providing Navarro County with the exact migration of images with the current voters file index information into Navarro Counties new Cloud FileBound site, including all FileBound project and user access setup needed.

FileBound and **AIS** will provide the FileBound Connect application that will allow Navarro County to connect the registered voter's digital application package to their voters maintenance page with in TEAMs, to eliminate the need to toggle between both application's.

AIS will setup and configure **FileBound Capture** to automate importing and filing the Texas DPS applications downloaded from TEAMs by Navarro county employee's.

AIS will setup and configure **FileBound Capture** to scan and automatically file Navarro Counties returned application in the mail.

AIS will provide **Navarro County** voter registration office with the ability to maintain any of its volunteers using FileBound to automate the registration, training and testing , and deputizing of any process needed.

AIS intends to take the following steps for the migration procedure to export the records from the current system into **FileBound**.

1. Step 1
2. Step 2
3. Step 3
4. Step 3
5. .....

4224 Centergate St. San Antonio, Texas 78217
P 210.590.8338 F 210.590.8322

1425

FileBound

Central Administration, Security Setup and Reports

FileBound Central Administration:

The Central Administration is an interface that allows a user with administrator rights to manage projects, users, groups, and other aspects of FileBound. Access to the various functionalities of FileBound is based on the group the user belongs to.

Note: General users do not have access to the Central Administration window.

User Types:

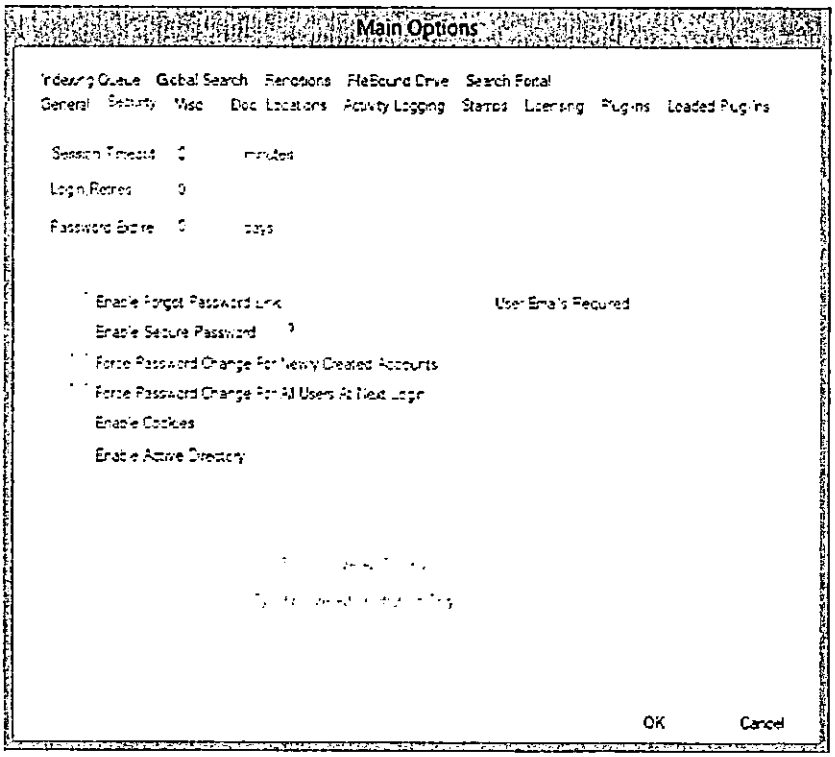
A user with System Administrator rights has access to all the features of FileBound and has rights to perform all the tasks. For example, System Administrators can create, configure, and manage users, groups, projects, and vendors.

A user with Project Administrator rights can configure and manage one or more projects assigned to the group the user belong to. For exam Project Administrator can set up dividers and separators, or setup index fields for the project, and other various options for the project.

A user with General User Rights has access to FileBound based on group membership.

Main Option Settings

Security:



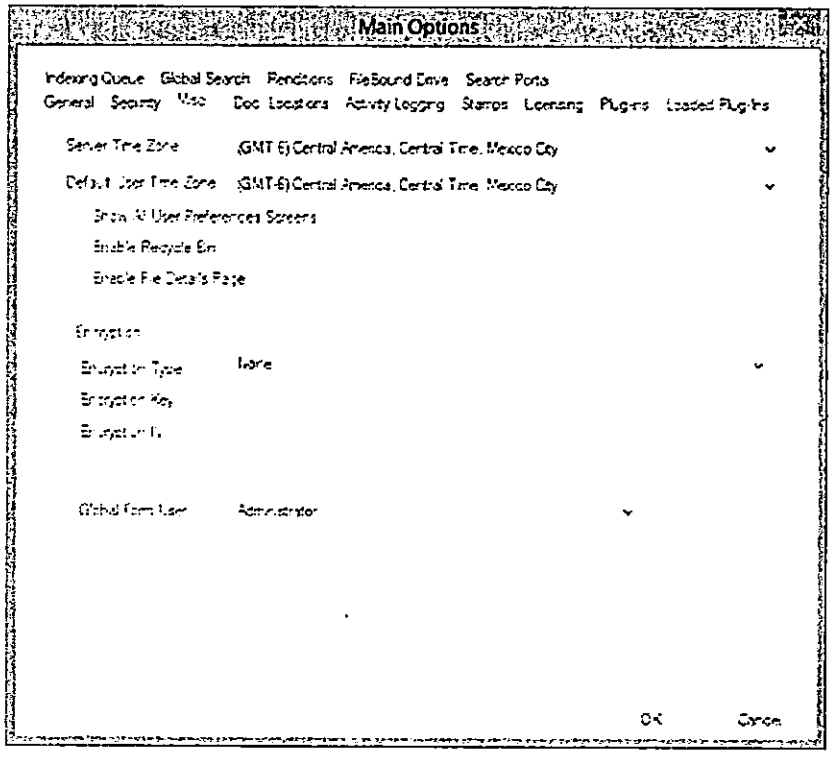
Miscellaneous:

FileBound allows you to encrypt documents while they are stored within the FileBound document storage location, and while transferring the documents through Secured Socket Layer (SSL). After you set up the document encryption, it is applied to the new documents that are created and saved. The previously saved documents are not encrypted. You can open and save previously saved documents to apply encryption.

FileBound provides AES and TiepleDES encryption type to encrypt documents. An encryption key is used to encrypt the document when it is stored. The key needs to be 24 alpha or numeric characters long.

The encryption initialization vector (IV) needs to be 8 alpha or numeric characters long when using the TripleDEs encryption type. The IV needs to be 16 alpha or numeric characters long when using the AES encryption type.

Note: Ensure to copy the keys and save them at another location because if these keys are lost. there is no way to decrypt the documents.



Activity Logging:

Choose from four different levels of activity logging

Main Options

Indexing Queue Global Search Renditions FileBound Drive Search Portal
General Security Misc Doc. Locations Activity Logging Stamps Licensing Plug-ins Loaded Plug-ins

Select Level of Activity Logging

ALL

Activity of the following items will be logged

- Project
- Group
- User
- File
- Document
- Archive
- Divider
- Document Signature
- Form Template
- Separator
- Annotation
- Template
- Document Location
- Field
- Server
- Setting
- Plugin

OFF

- Form Process
- Form Process Step
- File Security

OK Cancel

1429

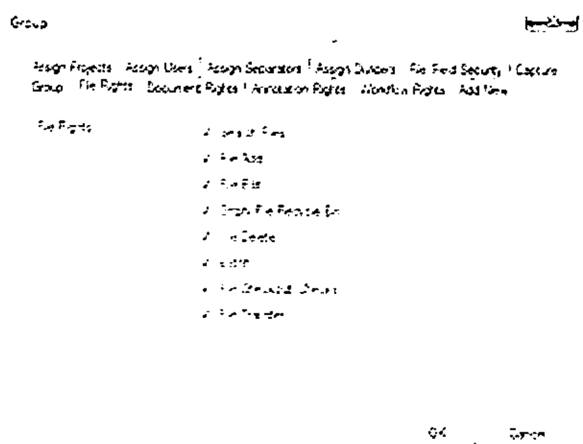
FileBound Groups:

A FileBound group is a collection of users with similar access rights that allows you to implement security for the FileBound system. You can assign various rights related to files, documents, dividers, separators, annotations, and workflow to a group. FileBound allow users to be assigned to one or more groups based on their roles in the system. You can configure a group to specify what rights the users will have, which projects they will have access to, and what operations they can perform.

Group Settings:

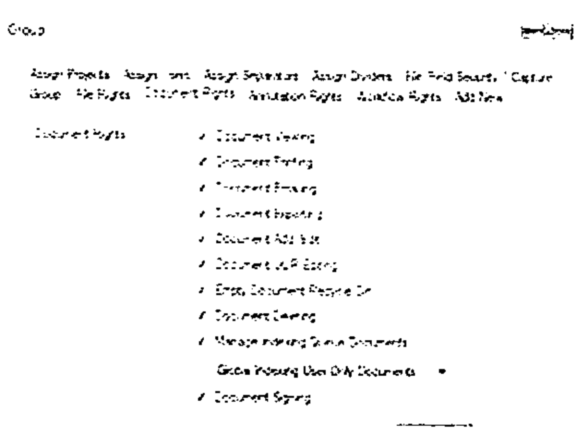
File Rights ... Group

File Rights:



Document Rights ... Group

Document Rights:

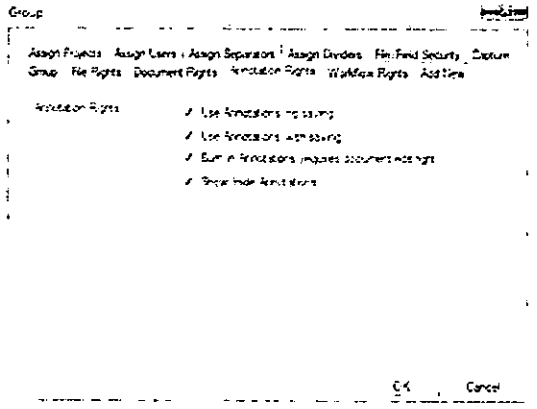


Group Settings: (Continued)

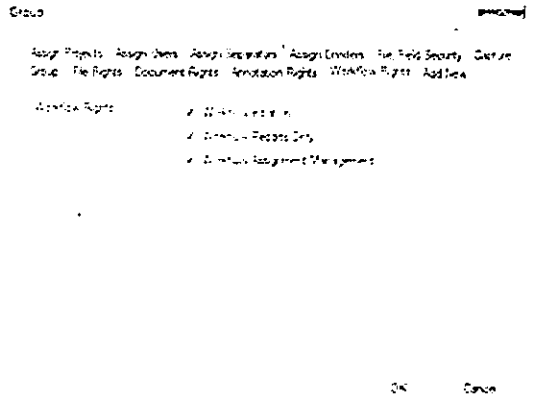
[illegible] Annotation Rights [illegible] Group [illegible]

[illegible]

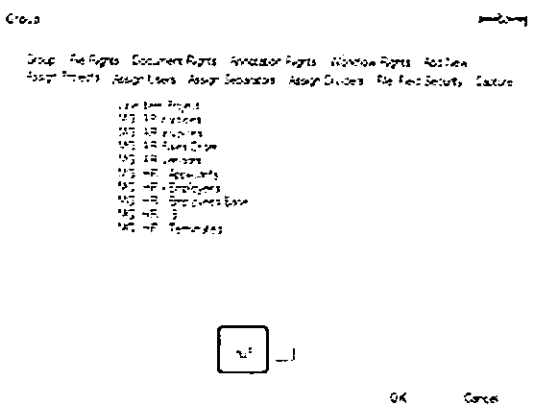
Annotations Rights:



Workflow Rights.



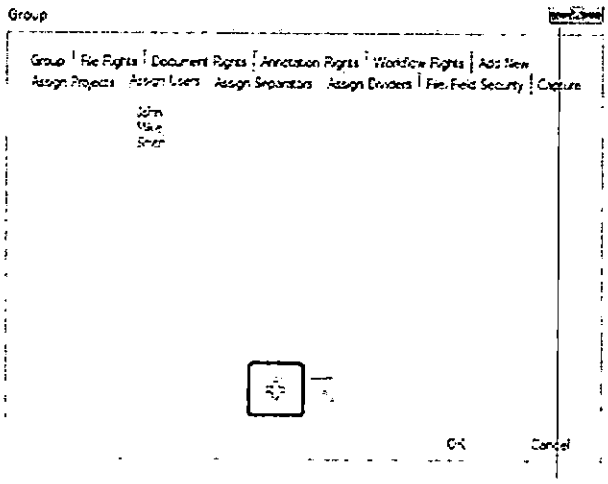
3. Assign Projects to the Group



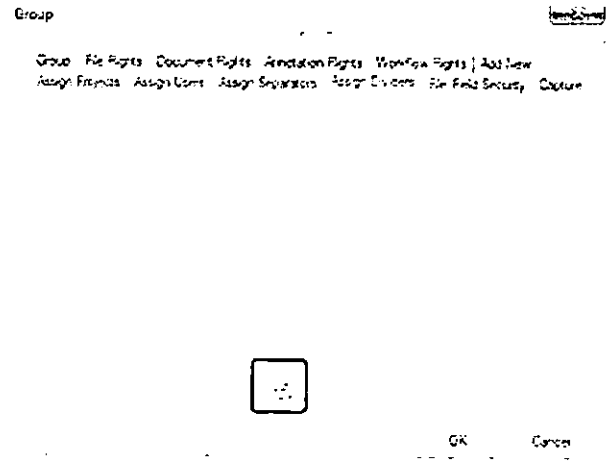
[illegible]

Group Settings: (Continued)

3. Assign Users to the Group

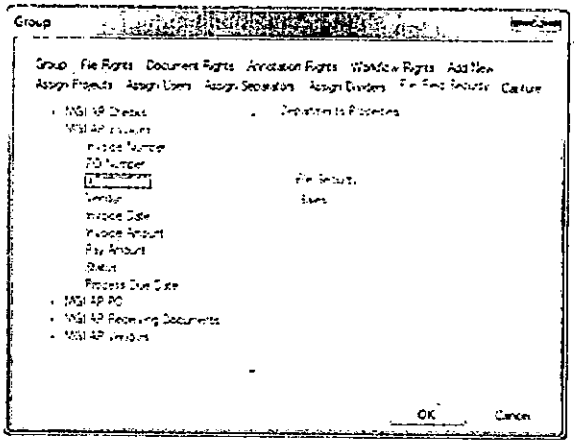


3. Assign Dividers to the Group



File Security is used for restricting access of users to specific files based oncertain index criteria. For example, an Invoices project will use an index file labeled "Department" and a group of users will need to be restricted to only view files with a value of "Sales" in the department field for the project.

4. Specify the Value for the Index Field



Audit Reports:

User Login Report gives details about successful logons for the user(s). The report shows user ID, user name, full name, session ID, login date and time, IP address and activity. User Login Report is available under the category System Reports on the FileBound site.

Note: User Login Report is only available to System Administrators.

File Activity Report shows the type of activity performed by users on files within a specified date range. This is a project dependent report and displays the activity for the selected project only. File Activity Report is available under the category Audit Reports on the FileBound site.

Document Activity Report shows the type of activity performed by users on documents within a specified date range. Document Activity Report is available under the category Audit Reports on the FileBound site.

Activity Audit Log Report shows the business activity monitoring report and provides information about the activities performed for various entities of FileBound such as projects, groups, users, file, and so on. For a selected entity, this report shows the activities performed by a user or all of the users for a specified date range. You can also filter the report to display information about a specific activity. Business activity report is available by the name Activity Audit Log under the category Audit Reports on the FileBound site.

Note: The level of reporting detail in this report depends on the level of reporting that has been set by a system administrator for the FileBound system.

Deletion Report displays name of the documents and files that have been deleted within a project. The report can be filtered based on a file or document, the project, the user or all users responsible for deletion and a specific date range. Deletion Report is available under the category Audit Reports on the FileBound site.

Note: When a file is deleted all documents within that file are deleted too. In this report, names of all those deleted documents and files are shown

File Analysis Report displays a list of files and documents with or without separators, dividers, or documents for a selected project. You can select a specific separator or divider from a list to report on as well. File Analysis Report is available under the category Audit Reports on the FileBound site.

User Rights Report displays all the group names that a user belongs to, and all of the rights that user has. User Rights Report is available under the category Audit Reports on the FileBound site.

Document Signature Report is used to find documents that are signed by users. This is a project dependent report and displays the activity for the selected project only. Document Signature Report is available under the category Audit Reports on the FileBound site. For each report, following details are displayed:

- Document ID
- User name of the user who has signed the document
- Date and time when the signature was applied
- Status of the signature, which can be active or inactive
- User name of the user who has unsigned the document
- Date and time when the signature was removed

Locked Document Report is useful to find documents that are locked by users. This is a project dependent report that will only be available if the Document Locking option has been enabled for the project. The Locked Document Report option is available under the Audit Reports category.

1433

White Paper

Upland Software Cloud Security and Data Center Standards

AIS upland
Access Imaging Solutions

Introduction

Upland Software understands that confidentiality, integrity, backup, and availability of your information are vital to your business operations. With our Enterprise Grade Cloud Operations, that's where we excel.

We take standards and procedures very seriously as a cloud-based Software-as-a-Service (SaaS) provider. Providing connectivity, reliability, speed, and scalability across the enterprise, Upland enables amazing outcomes for our customers. Upland's data centers provide best-in-class, cloud-delivered security, with superior infrastructure security and integrity, strict standards, true multi-tenant service, high resiliency, and scalability.

Service Provider Accreditation and Best Practices

All of Upland Software's product lines are accredited or follow best practices as defined by various bodies in relation to their standards and procedures. These include, but are not limited to:

+ SSAE 16 SOC 1 Type II
+ ISO 27001
+ Safe Harbor (EU and Switzerland)
+ TRUSTe

All data centers hold Safe Harbor certifications, which ensure the proper selection of adequate and proportionate security controls to protect all information assets in data centers. Also, Upland's European data centers are held to international standards and regulations.

Within Upland's Cloud Operations, there are several Engineers holding DoD clearance, adding trusted, certified, and validated security expertise and experience to the team.

Service-Providing Infrastructure Standards and Procedures

Upland Software maintains the following standards and undertakes the following procedures in relation to the infrastructure that provides its services:

+ Stress testing of all production design prior to deployment
+ Redundant servers for critical systems
+ Firewalls and routers, configured in active-passive configuration
+ Load balancers
+ Switches
+ Network interface cards (NICs)
+ Power supplies
+ RAID storage
+ Continuous monitoring of all components, sub-components, and internal/external/front-end/back-end applications to assist infrastructure and service integrity

Infrastructure Redundancy

Upland's primary data centers provide global average uptime of >99.9999%. That means each of the data centers typically experience outages totaling less than 5 minutes and 15 seconds over the course of a year.

To ensure availability, all facilities provide a minimum of N+1 power redundancy, meaning every mission-critical component has at least one backup. Our data centers also store enough fuel on site to provide a minimum of 24 to 48 hours of emergency power using backup generators, and they have guaranteed fuel delivery contracts to replenish those supplies. They also provide at least N+1 redundancy for all environmental controls equipment.

Network Security

Upland's network is protected by a number of layers, including firewalls, IDS, IPS, F5, and other smart-routing technologies.

In addition, encryption is utilized to protect data in transit, including SSL (TLS 1.1, 1.2) encryption over HTTPS connections utilized for secure communications between Upland and customer end users. Authorized IT engineers access production network equipment and data stored at the third party data center remotely, via secure VPN tunnels protected by IPsec encryption.

Data Backup

For backups of critical company data, several methodologies are utilized, including the following:

+ **Certified industry standard backup utilities for file-based backups to tape**
+ **SQL backup functionality**
+ **MySQL backup functionality**
+ **SAN-to-SAN replication to a geographically redundant data center**
+ **Data Center-to-Data Center replication**
+ **Physical Security**

Access to the buildings, data floors, and individual areas are monitored by 24/7 security. Personnel access each of the Upland data center facilities by using a proximity card security system, with variable rights granted to the office space, communications rooms, and local non-production server rooms. A third party security company monitors all locations after hours.

Upland co-locates our primary data center for critical production servers and cloud-hosted applications. Upland utilizes the services of a third party data center, with a minimum SSAE 16 SOC 1 Type II audit performed annually, for business continuity failover.

Minimum Data Center Facility Standards

Upland Software is architected with availability, maintainability, scalability, and customer security at the top of the list. Every data center implementation meets or exceeds the following specifications:

+ Redundant firewalls
+ Redundant F5 load balancers with SSL acceleration
+ Redundant web farms
+ Multi-processor servers connected by multiple gigabit NICs
+ Redundant database disk using real-time replication
+ Redundant (failover) database servers
+ Tape library for off-site data storage

In addition to the robust computing architecture, each data center supports the Upland Cloud via:

+ Dedicated substation on utility grid
+ Four or more onsite diesel generators
+ Independent rack power sources
+ Dual entry network connectivity
+ 3+ Internet backbone providers
+ Less than 40% peak network utilization
+ 99.999% availability of power and cooling

Minimum Network Service Standards

For a network service to be considered suitable for access to Upland's Enterprise Grade Platform, the following is required:

+ 24/7/365 monitoring of the site's network infrastructure
+ 24/7/365 customer service desk to respond and support customers with incidents and service requests
+ Minimum 99.50% network uptime service level agreement
+ Diverse network feeds into the data center site

Additional Third-Party Applications

In partnership with Dell Boomi, the Upland Integration Manager capabilities will provide customers:

+ Integration between Upland's family of cloud-based products and with a customer's existing set of applications to improve organization objectives and security controls
+ Greatly reduced time to deployment for additional integrations and simplified management
+ Secured process of complete data transparency between system silos to increase efficiency and deliver actionable outcomes

Also providing services to Upland products and our customers, Akamai is a cloud-based service provider specialized in content acceleration and security.

+ Akamai leverages their network of globally distributed servers.
+ They provide end users with caching, route optimizations, distributed security, and firewall mechanisms.
+ By combining those mechanisms with its platform, Akamai can deliver increased performance and defense against cyber-attacks.

Internal and Third-Party Testing and Assessments

New product features are tested prior to code completion to identify features that do not work properly. Security testing is integrated into feature testing and regression testing. Additional application security testing is provided in the form of source code scans of modified or added code. Every Upland release is subjected to a third-party application vulnerability assessment prior to release.

In addition, all application servers are comprised of three segments. Each segment is configured to recognize legitimate requests. Only those requests are passed on to the application servers. All other requests are blocked.

Regulatory Compliance

Upland's Enterprise Grade Platform is designed and certified to meet many of the compliance requirements of the most demanding environments. The security landscape continues to evolve, and you can rely on Upland to stay ahead of the threats. Note that some compliance offerings are unique to Upland, and not all regulatory frameworks listed below are applicable to all available Upland products. Also note that other pricing considerations may apply.

PCI DSS Service Provider Level 1	NIST 800-53 Moderate Control (National Institute of Standards and Technology)	U.K. Data Protection Act 1998, and all other E.U. National Legislation
HIPAA (Health Insurance Portability and Accountability Act)	FISMA (Federal Information Security Management Act)	E.U. Data Privacy Directive 95/46/EC
Family Education Rights and Privacy Act	DIACAP (DoD Information Assurance Certification and Accreditation Process)	E.U.-U.S. Safe Harbor Registration
GLBA (Gramm-Leach-Bliley Act)	FIPS 140-2 (Federal Information Processing Standard)	SSAE 16 (Statement on Standards for Attestation Engagements)

Risk Assessment

Upland's Security Organization is responsible for identifying risks that threaten services and systems. We have implemented a process for identifying relevant risks, which includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding on actions to address them. We have established strategic operating, reporting, and compliance factors in order to identify potential risk events, and we take into account external and internal factors so that our risk assessments efforts can adequately support business decisions and respond to potential threats.

Risk analysis is an essential process to an organization's success. Upland's methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

+ Estimating the significance of a risk
+ Assessing the likelihood (or frequency) of the risk occurring
+ Considering how the risk should be managed, including an assessment of what actions need to be taken

Monitoring

Upland's Security Organization performs monitoring activities in order to continuously assess the quality of internal control over time. These activities are used to initiate corrective action through department meetings, client conference calls, and informal notifications. Management performs monitoring activities on a continuous basis, taking necessary actions as required to correct deviations from company policy and procedures.

Reporting

Upland Software manages incidents by identifying and responding to them quickly, notifying key support and management personnel in a timely manner, restoring service as soon as possible, determining the cause of the incident, and taking appropriate steps to prevent future incidents. Our incident management process also allows us to quickly notify external organizations that may have been affected by an incident, including customers and partners. We employ internal and external monitoring systems that periodically verify the state of each Upland cloud-based software product.

Along with incident handling, Upland understands the importance of having a security incident response process in place. As such, we ensure that any instance of suspected disclosure of sensitive information is reported immediately and escalated appropriately to Upland's Information Security Representative and Legal Counsel. The Security Team will handle initial responses and assume leadership and direction for the Computer Incident Response Team (CIRT). Together, these teams — Legal, Security, and CIRT — would effectively coordinate, collect, respond, and report security events.

For More Information

For more information about Upland Software's cloud-based Enterprise Work Management solutions, please visit uplandsoftware.com or call 855-944-PLAN.

About Upland Software

Upland Software (Nasdaq: UPLD) is a leading provider of cloud-based Enterprise Work Management software. Our family of applications enables users to manage their projects, professional workforce and IT investments, automate document-intensive business processes and effectively engage with their customers, prospects and community via the web and mobile technologies. With 2,000 customers and over 235,000 users around the world, Upland Software solutions help customers run their operations smoothly, adapt to change quickly, and achieve better results every day. To learn more, visit uplandsoftware.com.

AIS upland
Access Imaging Solutions

FileBound

Central Administration, Security Setup and Reports

1440

FileBound Central Administration:

The Central Administration is an interface that allows a user with administrator rights to manage projects, users, groups, and other aspects of FileBound. Access to the various functionalities of FileBound is based on the group the user belongs to.

Note: General users do not have access to the Central Administration window.

User Types:

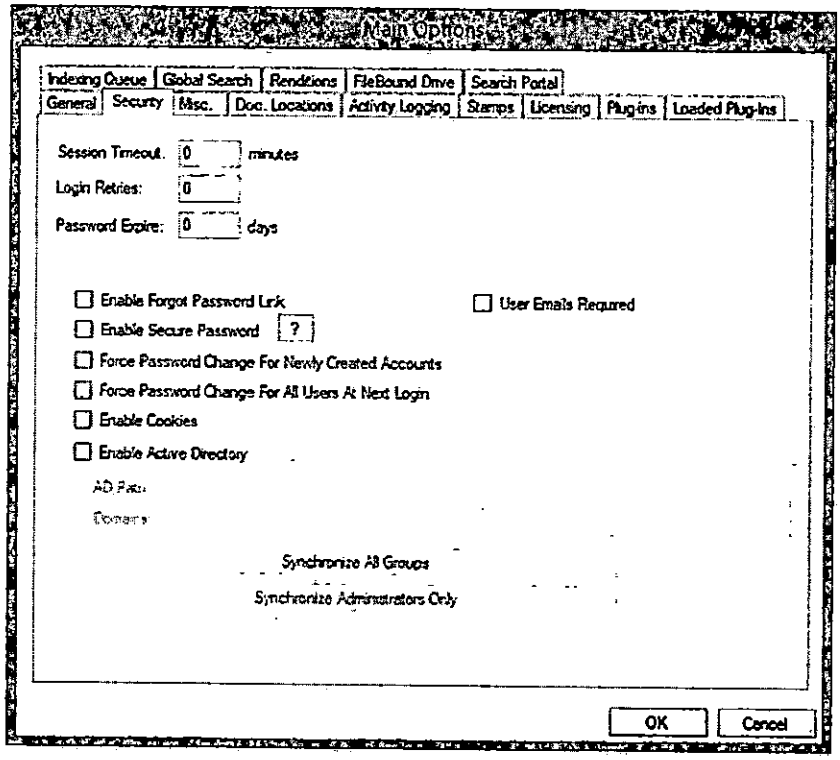
A user with System Administrator rights has access to all the features of FileBound and has rights to perform all the tasks. For example, System Administrators can create, configure, and manage users, groups, projects, and vendors.

A user with Project Administrator rights can configure and manage one or more projects assigned to the group the user belong to. For exam Project Administrator can set up dividers and separators, or setup index fields for the project, and other various options for the project.

A user with General User Rights has access to FileBound based on group membership.

Main Option Settings

Security:



Miscellaneous:

FileBound allows you to encrypt documents while they are stored within the FileBound document storage location, and while transferring the documents through Secured Socket Layer (SSL). After you set up the document encryption, it is applied to the new documents that are created and saved. The previously saved documents are not encrypted. You can open and save previously saved documents to apply encryption.

FileBound provides AES and TiepleDES encryption type to encrypt documents. An encryption key is used to encrypt the document when it is stored. The key needs to be 24 alpha or numeric characters long.

The encryption initialization vector (IV) needs to be 8 alpha or numeric characters long when using the TripleDEs encryption type. The IV needs to be 16 alpha or numeric characters long when using the AES encryption type.

Note: Ensure to copy the keys and save them at another location because if these keys are lost, there is no way to decrypt the documents.