Service Level Agreements - FileNet Enterprise Content Management

Version 1.3

Contents

- Document Approvals
- Service Level Agreement Overview
- Description of Services
    - Services Included
    - Services Specifically Excluded
- Service Performance
    - Hours of Operation
        - Regular Business Hours
        - After Hours
    - Maintenance
        - Regularly Scheduled Maintenance
        - Emergency Maintenance
        - Impact on Service During Maintenance Operations
    - Response on Services Offered
    - General Performance Metrics
    - Incident & Problem Management
    - After Hours Assistance
    - Incident Priority & Response Time Guidelines
- Service Costs
- PROVIDER & CLIENT Responsibilities
    - PROVIDER Duties & Responsibilities
    - CLIENT Duties & Responsibilities
- Problem Management & Disaster Recovery
    - Service Recovery Priority
    - Change Management Process
    - Escalation of Issues
        - Escalation of Nontechnical Issues
        - Escalation of Technical Issues – Routine & Moderate Priority Issues
        - Escalation of Technical Issues – High, Critical & Major Issues
- Term, Review & Termination of Agreement
    - Review
    - Termination of Agreement
- Liability
- Glossary of Terms & Acronyms
- Revision History

Document Approvals

Approver Name & Title	Role	Method*	Date
Linh Nguyen Manager, eDocs IT Team	Service Manager		
Marina Arseniev Director, Central Services	Service Executive		
Linh Nguyen Manager, eDocs IT Team	Document Owner		

*Approval method of **Email** indicates that approval was received via email message. **Signature** indicates that the approver signed a hard copy of the document and that copy is on file with OIT and the client.

Service Level Agreement Overview

This Service Level Agreement (SLA) is for the purpose of identifying the basic services and any specific optional services to be provided by Office of Information Technology (OIT) Central Services (PROVIDER) to (CLIENT) regarding IBM FileNet software.

The section of this document titled *Glossary of Terms & Acronyms* is the authoritative definition of terms, acronyms, and abbreviations used in this document.

Description of Services

This agreement authorizes CLIENT to use the IBM FileNet software provided and maintained by PROVIDER to develop content including FileNet repositories and case manager solutions. CLIENT is authorized to access the content and case information. Authorized users are determined by CLIENT via campus KSAMS.

Services Included

- **Central Services Provided**

    - PROVIDER will provide and maintain the FileNet infrastructure including gateway(s), dispatcher(s), content manager(s), content store(s) and load balancer(s). PROVIDER will provide the virtual and/or physical computing environment necessary to run the FileNet infrastructure, including server(s), networking, and firewalls. PROVIDER will configure, secure, administer and maintain these central services. PROVIDER will configure these services so as to provide separate environments for development/testing and production deployment of FileNet content.
- **Client Tools Provided**
    - PROVIDER will provide and CLIENT shall be authorized to install and use FileNet client tools including IBM FileNet Framework Manager, IBM FileNet Insight, IBM FileNet Transformer and IBM FileNet Cube Designer. The installation and configuration of these client tools shall be the responsibility of CLIENT, as determined by any existing CLIENT Desktop Support agreement.
    - The use of all IBM FileNet client tools shall be governed by applicable IBM Software License Agreements.

Services Specifically Excluded

The following services are specifically excluded from this Agreement:

- The use of related IBM software products such as TM1, SPSS Statistics or SPSS Modeler.
- The development, maintenance, security and use of CLIENT database systems or networks.
- Damages resulting from misuse of services or use of services in violation of OIT's and UCI's Privacy and policies. (See *Liability* section, below.)

Service Performance

Hours of Operation

Regular Business Hours

PROVIDER's regular business hours are defined as every non-holiday Monday – Friday between the hours of 8:00am and 5:00pm Pacific Time.

Email: oit@uci.edu
Phone: (949) 824-2222

After Hours

PROVIDER will provide after-hours technical support, outside regular business hours, for major or critical system-wide incidents that impact all or a large number of CLIENTs. The OIT Help Desk is staffed 24 hours a day, 7 days a week and provides a means for handling emergency after-hours incidents. Help Desk agents can notify on-call OIT technical staff and other resources when appropriate.

Email: oit@uci.edu
Phone: (949) 824-2222

Maintenance

Regularly Scheduled Maintenance

Services are periodically taken offline for regular maintenance such as upgrades, patches, and other noncritical support operations.

Operating System Updates

Updates are typically applied to the FileNet servers on the 3rd Saturday of each month, from 6:30 PM to 9:00 PM, or as otherwise specified by the OIT Windows Services Group.

FileNet Upgrades

IBM periodically updates FileNet to new versions and releases fix packs to existing versions. PROVIDER will schedule upgrades to the UCI FileNet infrastructure in order to remain current with the latest version of FileNet. Upgrades will be scheduled as follows:

A. When an upgrade or fix pack is released, PROVIDER will schedule dates for: 1) Deployment into the development/test environment; and 2) Deployment into the production environment.

B. On the scheduled development/test date, PROVIDER will apply the upgrade or fix pack to the development/test environment. CLIENT will have until the scheduled production deployment date to test its FileNet sytem (content, frameworks, reports, etc.). PROVIDER will work with CLIENT to mitigate any issues discovered during this testing.

C. On the scheduled production/deployment date, PROVIDER will apply the upgrade or fix pack to the production environment. CLIENT must re-test its production deployment in a timely manner to ensure that no further issues exist.

Any problems identified during the development/test phase that cannot be mitigated in time for production deployment will be handled on a case-by-case basis, and may result in rescheduling the production deployment date.

CLIENTs should make allowances for this maintenance window when scheduling production processes or activities.

Emergency Maintenance

On rare occasions, it will become necessary to interrupt access to a service to perform emergency (sometimes referred to as "out of band") maintenance. Given the nature of this type of maintenance it is not always possible to provide much notice before the service interruption occurs or to accurately predict the duration of the service outage. PROVIDER will make every effort to provide as much notice as far in advance as possible before performing such maintenance and to restore full service as soon as possible.

Impact on Service During Maintenance Operations

During the regularly or emergency scheduled maintenance window, access to PROVIDER's service may be reduced or completely unavailable. PROVIDER will notify CLIENT via email in advance of the maintenance window to inform them on what the impact on the service is likely to be. Impact on services during emergency maintenance will be communicated to CLIENT as soon as possible once it is determined the emergency maintenance is required.

Response on Services Offered

The following table defines anticipated response times for services ordered from PROVIDER. The target response times are based on work done during normal business hours. All response times are "not to exceed" estimates. Expedited service deliveries must be arranged and agreed to by both PROVIDER and CLIENT before work begins.

(NO SERVICES REQUIRE DEFINED SERVICE TIMES)

General Performance Metrics

The following service commitments apply to all services delivered and supported by PROVIDER.

Performance Metric	Service Commitment	Measurement
Availability of FileNet service	PROVIDER will provide continuous availability of the FileNet services at all times except as defined above under **Maintenance**.	Availability statistics published on ZotPortal

Incident & Problem Management

In order to serve CLIENT optimally, incidents affecting service delivery are prioritized based on their level of impact on business operations and the criticality of the service that is interrupted. PROVIDER staff will work with CLIENT to classify and prioritize incidents based on information provided by CLIENT and the results of preliminary troubleshooting. Generally, CLIENT can expect a response from PROVIDER within the time guidelines listed below, but these are not resolution time guarantees. Often, PROVIDER will be able to respond to incidents more quickly than the times listed, but in times of exceptionally heavy demand, incident response can take longer. Incidents reported during the defined maintenance window that are the result of the maintenance being performed will be acted upon at the end of the scheduled maintenance. Incidents that are not the result of scheduled maintenance will be prioritized and escalated normally.

After Hours Assistance

The response time guidelines below are only applicable during normal business hours. Outside of normal PROVIDER business hours, the response is typically the following business day. For emergencies that cannot wait until next business day, the person reporting the incident should contact the OIT Help Desk and indicate to the agent that the incident is an emergency and immediate assistance is required. The Help Desk Agent will determine the priority of the issue (using the guidelines below) and will contact appropriate on-call staff. On-call staff will take action to respond the problem within the guidelines indicated below and will coordinate with the OIT Help Desk to respond to the person who reported the emergency.

Incident Priority & Response Time Guidelines

Except where noted above in the section titled *General Performance Metrics*, the following definitions of Priority, Impact, Urgency, and Response Times will apply to all services provided under this Agreement.

IMPACT is a measure of the effect of an Incident on business processes. Impact is based on how service levels will be affected and the number of end users affected. Usually the ticket creator declares the initial impact. The impact of an incident can be adjusted as insight into the issue grows.

Campus-Wide	Multiple Groups	Single Group	Individual
• Campus-wide service down • Multiple locations' service completely down during operating hours • >250 individuals	• Campus-wide service working, but degraded performance or function • Single location's service completely down during operating hours • 10 - 250 individuals	• Single location's service degraded • Development or test service impact in noncritical period • Single/few users affected • 2 - 10 individuals	• Outside of service's operating hours • Effects only IT Services operations • Single individual

URGENCY is a measure of business criticality of an Incident. The urgency reflects the time available to respond to the incident before the impact is felt by the business. In practical terms, the client judges urgency.

Service Unavailable	Service Degraded	Interfering with Work	Tasks More Difficult
• No viable workaround • Caller indicates "emergency" • High financial or reputation risk or implications	• Complex workaround • Medium financial or reputation risk or implications	• Intermittent • Workaround is disruptive or risky • Low financial or reputation risk or implications	• Easy workaround • Failover in place • Not service disrupting (yet)

PRIORITY is a function of Impact and Urgency. Target response times are assigned based on Priority.

		Impact			
		Campus-Wide	**Multiple Groups**	**Single Group**	**Individual**
Urgency	**Service Unavailable**	Major 2 hours	Critical 4 hours	High 1 day	Moderate 2 days
	Service Degraded	Critical 4 hours	High 1 day	Moderate 2 days	Moderate 2 days
	Interferes With Work	High 1 day	Moderate 2 days	Moderate 2 days	Routine 7 days
	Tasks More Difficult	Moderate 2 days	Moderate 2 days	Routine 7 days	Routine 7 days

Service Costs

From time to time and as needed, PROVIDER may augment the FileNet infrastructure to support current or anticipated campus needs. Any such augmentation may incur additional hardware, software or licensing costs. The funding for such costs will be handled on a case-by-case basis, and may include additional one-time Client assessments.

Pricing:

1. Software License:
    a. Option 1: Enterprise Content Management (ECM) license = $49.06/AUVU/year. Functionality includes interaction with scanned or uploaded documents, annotation, redaction, encryption, simple record retention. License negotiated with IBM via ESSO agreement by UCOP every 3 years.
    b. Option 2: ECM and Case Manager license - $151.56/AUVU/year. License negotiated with IBM via ESSO agreement by UCOP every 3 years.
2. Secure storage and maintenance support pricing. Includes infrastructure support, upgrades, security and regular vulnerability scanning, backup and restores, purging according to record retention policy, secure database administration, and Disaster Recovery:
    a. $14.00 / GB / year
3. Custom software development, such as case manager solutions that include workflow, form routing, and encrypted document management:
    a. We follow the OIT Systems Development Life Cycle (SDLC) which includes requirement analysis and documentation, development of solution (typically about 2-3 weeks), user acceptance testing, and production roll out. Development, staging, and production environments will be provided.
    b. For typical medium complexity systems with PII data (such as social security numbers) that take 2-3 weeks of development, Filenet and Case Manager implementation costs will be waived by OIT. Otherwise, OIT will recharge departments $65/hour to implement a solution. Although Filenet system upgrades are included, application upgrades or enhancement may require additional OIT developer time, also rechargeable at $65/hour.
4. Centralized Paper Scanning Service:
    a. Services for paper scanning are provided by the A&BS Document Scanning group. Please contact Vanessa Lopez at (949) 824-1211 or email vrlopez@uci.edu for further information.
    b. Complex custom scanning applications may require additional OIT developer time. Scope of the project and cost will be estimated and provided per project.

Note that OIT may waive some of these costs for projects where the risk of exposure or breach of Personal Identity Information Data (Social Security Numbers, etc) is reduced by implementation of the Filenet encrypted document management solution. This is for cases where the business function does not allow for encrypted archival or purging of PII data.

OIT may renegotiate these services costs on a yearly basis as support costs may change.

PROVIDER & CLIENT Responsibilities

PROVIDER Duties & Responsibilities

1. Adhere to committed response times listed above for incidents involving interruption or degradation of services.
2. Provide a team of technical experts and technical managers to provide a team-centered organizational response to all support needs.
3. Provide management of appropriate service support operations (Help Desk, walk-in support, and field or on-site support).
4. Provide supervision and technical support for PROVIDER staff assigned to respond to incidents reported by CLIENT.
5. Communicate with all stakeholders regarding all planned and unplanned service-affecting issues and events.
6. Provide professional and competent services.
7. Ensure the safety of the technical staff and the clients being served.
8. PROVIDER may add, alter or delete guidelines as necessary to reflect best practices and ensure the efficient operation of FileNet for all UC Irvine constituents. PROVIDER will consult with CLIENT to ensure CLIENT understands these (and any additional) guidelines. PROVIDER and CLIENT will review CLIENT's database and framework designs, and CLIENT agrees not to put such designs into the production environment until they have been certified by PROVIDER.
9. PROVIDER shall make certain IBM FileNet computer-based training courses available via UC Learning Center or other means. CLIENT shall be authorized to provide these courses to its staff on an individualized and self-paced basis. PROVIDER will make every effort to ensure that such computer-based training is comprehensive and up-to-date, but does not guarantee that any particular course offering shall be available or reflect the current version of FileNet.IBM provides additional FileNet training coursework on an instructor-led, instructor-remote or self-paced-virtual basis. The enrollment and fees for any such coursework for CLIENT staff is the responsibility of the CLIENT.

CLIENT Duties & Responsibilities

1. Each team, functional unit, or other organizational unit that uses services provided under this agreement must identify a Client Representative to serve as the primary point of contact (POC) when it becomes necessary to communicate directly with users.
2. Specify the appropriate level of urgency and any specific expectations when requesting support services or reporting incidents.
3. Follow PROVIDER and CLIENT acceptable use policies to ensure that services and other resources are used responsibly.
4. CLIENT will determine which CLIENT data shall (and shall not) be accessible within FileNet, and the authorization requirements for such data. CLIENT and PROVIDER FileNet administrators will collaborate to ensure that such data are secured from unintended, unauthorized or inappropriate access.
5. CLIENT will obtain authorization through KSAMS to access any protected content for which there is a business need.

6. CLIENT acknowledges that IBM may specify compatible hardware, operating systems, and software (including browsers) for use with FileNet, including compatible versions of such operating systems and software (including browser versions and/or supported plug-ins). PROVIDER may provide additional guidelines for compatibility which augment or supersede IBM's specifications. CLIENT agrees to ensure that all desktop hardware, operating systems and software (including browser versions) used with FileNet comply with these guidelines.
7. CLIENT agrees, when requested by PROVIDER, to provide document's metadata and retention.

Problem Management & Disaster Recovery

In the event of a major emergency or disaster that affects PROVIDER's ability to deliver services, recovery procedures will be put into effect in accordance with PROVIDER's Business Continuity Plan. Details of this plan can be made available to CLIENTs by request.

Service Recovery Priority

In the event of a major emergency or disaster, priority for service recovery will be assigned as documented in PROVIDER's Business Continuity Plan. Details of this plan can be made available to CLIENTs by request.

Change Management Process

For required changes and updates that fall outside the normal maintenance window, the following general procedure will be followed:

1. PROVIDER will notify all CLIENTs affected by the change.
2. Changes will be made.
3. Changes will be tested.
4. Services will be restarted or otherwise restored.
5. PROVIDER will notify CLIENTs that services are available.

Where possible, changes will be made in such a way that they can be backed out and the service returned to its condition prior to the change. This may not be possible in all cases.

Escalation of Issues

PROVIDER staff will provide technical support and will answer technical questions about the status of provided services. In the event that an incident requires escalation, the following steps will be taken depending on the type of issue that is being reported.

Escalation of Nontechnical Issues

The Client Representative is primarily responsible for addressing nontechnical issues. Under normal operation, Client Representative will provide a best-effort response to end user concerns about nontechnical issues. If an end user requests escalation of a nontechnical issue from PROVIDER, then PROVIDER will direct the user back to the Client Representative. For nontechnical issues, the order of escalation is as follows:

Level 0: End user will contact Client Representative and provide information about the issue.

Level 1: Client Representative will work directly with end users regarding any nontechnical issues.

Level 2: Client Representative will collaborate with Service Manager to resolve the issue and communicate the overall status to end users

Level 3: At Service Manager's discretion, issues may be further escalated as appropriate

Escalation of Technical Issues – Routine & Moderate Priority Issues

PROVIDER is primarily responsible for addressing technical questions and providing solutions to routine and moderate priority technical problems. Client Representative will collaborate with PROVIDER to manage communications with end users. For routine technical issues reported under normal operating conditions, the order of escalation is as follows:

Level 0: Client Representative or end user will refer technical issues to PROVIDER via the OIT Help Desk.

Level 1: Help Desk will contact PROVIDER staff assigned to the issue for updates on issue status. PROVIDER staff assigned to the issue will communicate the status to Client Representative.

Level 2: Help Desk will contact Service Manager for updates on the issue and Service Manager will communicate the status to Client Representative and Help Desk.

Level 3: Help Desk will contact Service Executive for updates on the issue and Service Executive will communicate the status to Client Representative and Help Desk

Level 4: At Service Manager's discretion, issues may be further escalated as appropriate

Escalation of Technical Issues – High, Critical & Major Issues

PROVIDER is primarily responsible for addressing technical questions and providing solutions to high priority technical problems. Client Representative will collaborate with PROVIDER to manage communications with end users. For technical issues that require immediate or faster than routine response, the order of escalation is as follows:

Level 0: Client Representative or end user will refer technical issues to PROVIDER via the OIT Help Desk and will indicate that the issue is of higher than normal urgency.

Level 1: Help Desk will contact Service Manager for updates on the issue and Service Manager will communicate the status to Client Representative and Help Desk.

Level 2: Help Desk will contact Service Executive for updates on the issue and Service Executive will communicate the status to Client Representative and Help Desk

Level 3: At Service Manager's discretion, issues may be further escalated as appropriate

Term, Review & Termination of Agreement

Effective Date:
End Date:
Previous Review: N/A
Next Review: One month prior to End Date

Review

This Agreement is a dynamic document and will be periodically reviewed and changed when any of the following occurs:

- The environment changes.
- USERS' expectations or needs change.
- Workloads change.
- Better metrics, measurement tools, or processes become available.

At a minimum, this Agreement will be reviewed annually one month prior to its End Date. Contents of this Agreement may be amended as required and PROVIDER will communicate changes to all affected parties. PROVIDER will incorporate all subsequent revisions and obtain agreements and approvals as required.

Termination of Agreement

This agreement governs the support of basic services and any agreed upon optional services to be provided by PROVIDER as described in the previous sections. It may not be terminated except by decision of the Service Executive and approval by the Office of the CIO. All CLIENTs will be notified at least 60 days prior to the termination of this agreement or any of the services covered here.

Liability

PROVIDER expects every individual to be aware of and accountable for complying with the University's and OIT's Privacy requirements and to actively support the University's commitment to respect the privacy of individuals. PROVIDER assumes no liability for damages incurred by CLIENTs in violation of the University's privacy requirements. For more information on data Privacy and OIT's related policies, see:

http://www.security.uci.edu/privacy.php

Sensitive and Restricted Content

As described in http://security.uci.edu/plan-classification.php, information resources are broken into low, medium and high levels of risk. CLIENT agrees that data classified as high or medium risk will be protected from all access from within FileNet, and should be included in FileNet content only when there is a legitimate business need. If high or medium risk data are provided to FileNet, CLIENT agrees to work with the OIT Security team to produce a Security Risk Assessment Questionnaire (SRAQ) for the source system before exposing the sensitive data to FileNet.

Security

CLIENT acknowledges that it is imperative to maintain the security of systems and data, and agrees to operate FileNet in such a way that security is maintained. This includes, but is not limited to, the following:

A. Client tools: Staff will be given access to client tools (including IBM FileNet Framework Manager, IBM FileNet Insight, IBM FileNet Transformer and IBM FileNet Cube Designer) on an as-needed basis.

B. Web development tools: Staff will be given access to web-based tools (including Report Studio, FileNet Workspace, Workspace Advanced, Query Studio, Analysis Studio and Event Studio) on an as-needed basis.

C. Protection of content: Content developed within FileNet (frameworks, reports, dashboards, etc.) will observe the principle of least privilege. Access to such content will be provided on an as-needed basis, and always in such a way that defaults to denying access to content.

D. Protection of data: Data will be made available through reports, dashboards and other tools on an as-needed basis. Reports and other delivery methods should observe: 1) Vertical security: do not expose unnecessary data items; 2) Horizontal security: do not expose unnecessary rows of content; 3) Protection of sensitive data (FERPA, etc.) in accordance with any applicable rules of access for that type of data.

E. Security review: Prior to production deployment, developed content will undergo a security review, with representatives from each of the following: 1) Client FileNet developers; 2) Client functional representatives; 3) OIT security team; 4) OIT FileNet team.

F. Protection of privacy: CLIENT acknowledges that it is CLIENT'S responsibility to protect privacy, and agrees to perform an appropriate privacy assessment prior to deploying content within FileNet.

Glossary of Terms & Acronyms

Term	Definition
Client	A person or group that agrees to use a service provided by PROVIDER.
Client Representative	The person in an organization who acts as the primary point of contact during resolution of major issues. The Client Representative can provide a delegate to represent him or her but the Client Representative retains the responsibility for compliance with the terms of the Agreement. For the purposes of this Agreement, each team, functional unit, or other organizational unit that uses services provided under this agreement must identify a Client Representative.
Emergency	An event determined by OIT, PROVIDER or client staff to be of major or urgent priority based on consideration of the incident's impact and urgency.
End User	An individual (typically a person) at the end of a service who is using the service for the purpose for which it was intended. The term "end user" distinguishes the consumer of a service from intermediary users (developers, installers, administrators, system operators, etc.) who make the service available for the end user.
Maintenance Window	A defined period of time during which planned outages and changes to production services and systems may occur. The purpose of defining standard maintenance windows is to allow clients of the service to anticipate and prepare for possible disruption or changes.
Nontechnical Issue	For the purposes of this Agreement, a nontechnical issue is any issue that does not meet the definition of a technical issue. This includes but is not limited to the following: • Quality of service complaints. • Customer service quality complaints. • Requests for reimbursement. • General, nonspecific dissatisfaction with a service.
OIT	Office of Information Technology. OIT provides telephone, network, and computing services in support of research, administration, and education at UCI. OIT provides central computing services, computer laboratories, departmental and research-group support services, business application support, and campus-wide technical coordination. OIT supports the campus network infrastructure and provides connectivity on campus and to the Internet via wireless and mobile wired networks, e-mail accounts, interactive Unix accounts, and a network file-sharing service for students, faculty, and staff.
POC	Point of Contact. A point of contact is the person or department serving as the coordinator of information concerning an activity. A POC is used in many cases where information is time-sensitive and accuracy is important.
Resolution Time	The time it takes to resolve a USER's issue or answer their question. It is measured from the time an incident is recorded, either by USERS via an email or Web submission, or by an OIT Help Desk Agent or other support group manually creating a record, until the time the USERS are advised that the incident has been resolved. Resolution Time is the time from incident creation until the incident's status is set to "Resolved." Resolution Time is generally only recorded during normal business hours.
Response Time	The time it takes to acknowledge an incident in a non-automated way. It is measured from the time an incident is recorded, either by USERS via an email or Web submission, or by an OIT Help Desk agent or other support group manually creating a record, until the time that USERS are advised that the incident has been received and is being addressed. USERS should be contacted either by phone or email and the incident marked "In Progress" to stop the response time clock. Response Time is generally only recorded during normal business hours.
Service	A combination of people, processes, and technology that provides one or more end users or clients the ability to perform a specific function or business process. A service is typically used by a client in support of the client's business operations but is sometimes delivered directly to an end user. Individual services provided to USERS by PROVIDER under this specific Agreement are described in the section of this Agreement titled *Description of Services*.
Service Executive	The person in the group that provides the service who represents the service from an administrative standpoint. The Service Executive is typically an executive (director level or above) who works with providers and clients to prepare the Agreement, agree on recharge rates and performance metrics, etc.
Service Manager	The primary technical contact in the group that provides the service. The Service Manager is generally the expert on all technical aspects of the service being provided under the Agreement. The Service Manager will generally be consulted during the preparation of an OLA to make sure the commitments being made are reasonable and supportable from a technical standpoint.
Technical Issue	For the purposes of this Agreement, a technical issue is any issue that directly impacts any of the provided services and is outside USERS' ability to manage without assistance from PROVIDER.

Revision History

Date	Ver	Description of Change	Contact
27 Sep 2016	1.0	Initial document creation.	Marina Arseniev & Linh N Nguyen
November 14, 2106	1.1	Modified Service Costs section	Marina Arseniev
11 Mar 2019	1.2	Updated FileNet license cost. FileNet will be 45.68/user/year. Added $7.24 to case manager cost.	Linh N Nguyen
11 Dec 2019	1.3	Updated FileNet license cost for both content management and case manager	Linh N Nguyen