Agenda Topics	Status

Session Prep Work:

Session Staff Training/Orientation (OA & CA)
(Newbie/Returning Office & Committee Assistants; Newbie Legislators/Staff)

Delivery late Dec thru Jan;
Ongoing, as needed during Session

Security Training (classroom and online)

Delivery Dec/Jan and on-demand.

Facilities and Equipment Readiness

Conduct mid/late-Dec.

Session Staff Recruiting & Readiness

Recruiting Nov; Training mid/late-Dec.

Applications Services Work - KLISS[1]:

KLISS Biennium Rollover[2] (including core component upgrades)

Deliverables dropping
mid-Nov thru 02 Jan 2015.

Revisor Operations ("Amendatory" process priorities[3] – 4 groups)

Plan to drop Groups 1, 2, and 3
with new build in early Dec.

Chamber Operations (Journals, Calendars, UAM enhancements)

Ongoing deliverables
with mid-Dec wrap up.

KLRD Operations (Publications, Search)

Ongoing.

Committee System (Enhancements/Extension Interim Committees)

Mid-Dec wrap up for
ongoing deliverables

Ongoing Functional Improvements and Enhancements

Ongoing with wrap-up of ready to
go deliverables in mid-Dec.

Technical Services Work[4]:

2014 Legislative Printer Refresh[5]

Targeting LCC approval at 21Nov meeting.

State Security Council Work (update of ITEC Policies 7230[6] and 7230-A[7])

Approved by ITEC 05Nov2014

Cellular Phone Signal on Ground Floor and Sub Vaults

Working thru interference issues.

Capitol Wireless Network Upgrade

Completion targeted mid-Nov.

Security Training Event

Successful staff engagement.

Implement video training for session staff

In Progress

Server Upgrade (Virtualization)

Completed early Nov2014

Broadcast Media Access

Targeting completion late-Nov.

---

[1] Attachment A: Application Services Status Update as of 11/05/2014

[2] Attachment B: Biennium Rollover Work Plan as of 11/11/2014

[3] Attachment C: Office of the Revisor Amendatory Process Priorities

[4] Attachment D: Technical Services Status Update as of 11/05/2014

[5] Attachment E: Printer Refresh Inventory Workbook as of 11/10/2014

[6] Attachment F: ITEC Policy 7230 – Information Technology Enterprise Securit

[7] Attachment G: ITEC Policy 7230-A – Information Technology Security Standa

Law Making:

- Amendatory Reports: Jordan is near completion on the striking of multiple lines across pages, this should be completed this week and full testing of insert and strike rules can begin. The test team is working on setting up test fixtures for the amendatory rules. These fixtures will be many delta documents marked up similar to the amendatory rule samples provided by the Revisor office. These fixtures will allow us to run through a battery of tests to check amendatory output. A test build will be provided to the test team on 11/6/2014 to initiate the testing process.

- Delta Documents: Propylon and KLOIS staff met with Revisor staff on 10/30/2014 to review delta issue documentation. Revisor staff had updated several title and repealer issue documents that contain issue descriptions, screen captures, and test scripts. The group reviewed the issues by demonstrating each issue in the KLISS system on a large screen. The tickets will be updated with the issue documents. Bookmark issues were discussed briefly and the group decided the business analysts and developers would draft recommendations on bookmarks. The group will review the recommendations the week of 11/3/2014. Propylon is continuing work on the delta issues and code updates are being submitted into the KS source code repository. The KLOIS developer is reviewing the code updates and will be assisting the test team in testing the issues.

Chamber Automation:

- CA Thin client:
  - The following CI tickets are ready for deployment:
    - CI-16: Question of Germaneness not working for some amendments - gives an error.
    - CI-17: Rule 1507 action has processing issues.
    - CI-22: Bill jacket copied within itself upon execution of Committee Report task action.
  - The following CI tickets are in acceptance testing:
    - CI-1 and GASP-1: House resolution introduction and emergency adopt.
  - The following CI tickets are ready for acceptance testing:
    - GASP-127: Committees in BISC section only appear if they contain document numbers. (will be tested with GASP-136)
    - GASP-133: Committees in BISC section only appear if they contain document numbers.(will be tested with GASP-136)
  - The following GASP tickets under development:
    - GASP-118: House: Speed up Daily Calendar.
    - GASP-128: Both Chambers: OCCURRED field doesn't allow anything other than datetime objects (preview testing)
    - GASP-134: Biennium year type should dictate how calendar number is used to query results.
    - GASP-136: Calendar does not produce properly in testing
- CA Thick client:
  - The following issues have completed preview and regression testing and are ready for acceptance. A change request has been drafted for production change and release approval.
    - CAPRATCH-8 CLONE - Update and Edit Meta Data Failing.
    - CAPRATCH-7 Flagging: Style Changes
    - BARNUM-3 CA: Barnum 1a.18.7.3 - Testing
    - BARNUM-7 CA: Barnum 1a.18.7.4 - Testing

1-2

- DIB-1 Change destination folder and recipient. - Testing
- DCCR-1 CLONE - Change destination folder and recipient. - Testing
- DCR-3 CLONE - Change destination folder and recipient. - Testing
- DFA-2 CLONE - Change destination folder and recipient. - Testing
- The following issue is in the development:
  - CAPRATCH-5 Amended document brackets
- The following issues are in the development queue:
  - CAPRATCH-4 Journal Paging of elements in legislative_day subfolders
  - VCE-2 Various Day54 year2 journal elements are not visible

Decision Support:
- The new DS datastore was release into production on 10/3/2014 and a new DS client acceptance build was released to be used with the new DS 2015/16 production system.
- DS search:
  - Development work by Propylon will start mid-November (after CS interim updates are complete) to update the following:
    - Capture the LRMS revision document creation date so it can be added to the search index. Currently this is not being captured and the document creation date is not available to be searched on.
    - Capture the most recent LRMS document update entry and add the date to the search index. Currently this is not being capture and the last modified date is not available to be searched on.
    - Change the search UI "document type" field name to "file name"
    - Change the regular expression associated with number 3 to search for file name instead of document type
    - Update the lrms1_control_ra post commit service to fix a memory leak.
  - Re-index the DS datastore – will be performed by Kansas staff.
  - Liberty Search: May need to clear up a field name on the UI. For example change the work document type to file name. Ready to complete testing and implement.

Biennium Rollover:
- The CA and GL production system datastores and communications servers have been created.
- CA and GL systems are ready for cutover to production on 11/5/2014.
- The LI application has been forked and installed. The media server is being configured on the new 2015-16 LI and will be working with the new CA and GL systems.
- The UAM and AI updates will be deployed this week to work with the new production GL system.
- Next steps:
  - Acceptance test the CA build and install in chamber computers.
  - Implement the document mover post commit service in CA and DS as part of the biennium rollover system access enhancements.

1-3

UAM / AI Update:

- Appointments Interface updates (tickets AI-1 through AI-9) have been reviewed and are ready for deployment. Corey and Amy reviewed the updates on 10/17/2014. These updates will be deployed for use in the new GL system.
- Further enhancements to the UAM system have been reviewed and are ready for deployment. Corey, Susan, and Amy reviewed the updates on 10/30/2014. These updates will be deployed for use in the new GL system.:
    - Enhance the Committee zone propagation function to display which zones the committee is currently in.
    - Leadership assignment function to display assignment.
- UAM updates currently under development:
    - Run scripts when creating a user to create authorization and create datastore folders.
    - Add user interface for Division create and update.
    - Make title fields configurable – add and remove predefined titles from drop-down selections.
    - Rework Appointment Interface reports.
- A meeting was held on 10/27/2014 to complete the requirements on the member terms. These UAM updates are planned to be completed by Propylon.

Legislative Interface:

- The LI updates that correctly use the new committee and member status fields (from UAM updates) are ready for deployment. The following LI tickets will be deployed this week:
    - LI-46 - Inactive/Active Committee - Testing complete
    - LI-21 - Inactive/Active Member - Testing complete
    - LI-32 - Create Bills/Resolutions in Committee Report - Analysis
    - LI-42 - Modify LI Structure For Media Server
- LI updated in development:
    - LI-48 - Update the search inputs on the ELI to narrow searches by bienniums
    - LI-52 – Add a bill find input to the LI home page

Committee System:

- Interim Committee system - On track to have the following items ready for testing by 11/14/2014: Record member as excused or absent, Add/Edit Conferees, Assign substitute members to a committee, Assign Substitute staff to a committee, adding attendance list, auto-save for minutes, minute template updates, issue with time not saving correctly, and renaming of interfaces and buttons.

/-4

KLISS 2014 Biennium Rollover Plan
CA & GL Zone Task Summary

No	Project	Task	Start	End	Resource	Status
	CA Staging Server Setup:					
1		Create a TREX data archive from the current production server. (Note specific head revision of archive)	06/18/14	06/23/14		Done
2		Create the new TPOZ server.	06/23/14	06/24/14	Major, Brian	Done
3		Create server instances of the Comm, App, & LI servers (update comm server software).	06/23/14	06/24/14	Major, Brian	Done
4		Update the Molinar and Chisum documents.	06/23/14	06/24/14	Eric, Alan, ServerTeam	Done
5		Run Chisum.	06/23/14	06/24/14	Major, Brian	Done
6		Run Molinar.	06/23/14	06/24/14	Major, Brian	Done
7		Load past biennium data from the TREX archive – system folder (kpids & templates)	06/23/14	06/24/14	Kris	Done
8		Copy django auth user table from production to staging.	06/23/14	06/24/14	Kris	Done
9		Remove KPIDs of users that have been removed in Molinar.	06/23/14	06/24/14	Alan, Jenni	Done
10		Test basic server functionality, client access, and client applications (with old Barnum client and CI).	06/25/14	06/27/14	Eric, Eddie, Toni	Done
11		Repeat steps 2 to 9 as needed, making adjustments until tests are successful.	06/25/14	06/27/14		Done
12		CA Thick Client – Create new client build with updated Barnum.	06/27/14	06/27/14	Jordan	Done
13		Test basic server functionality, client access, and client applications with new Barnum client.	06/30/14	07/03/14	Eric, Eddie, Toni	Done
14		Repeat steps 2 to 13 as needed, making adjustments until tests are successful.	06/30/14	07/03/14		Done
15		Configure the IRC test vote system to connect to the updated CA staging system.	06/30/14	07/03/14	Timothy	Done
16		Test the IRC voting system integration to the updated CA staging system.	06/30/14	07/03/14	Toni, Timothy	Done
	GL Staging Server Setup:					
1		Create a TREX data archive from the current production server. (Note specific head revision of archive)	06/18/14	06/23/14		Done
2		Create the new combined UAM APP and TPOZ server.	06/23/14	06/24/14	Major, Brian	Done
3		Update the Molinar and Chisum documents.	06/23/14	06/24/14	Eric, Alan, ServerTeam	Done
4		Run Chisum.	06/23/14	06/24/14	Major, Brian	Done
5		Run Molinar.	06/23/14	06/24/14	Major, Brian	Done
6		Load past biennium data from the TREX archive – system folder (kpids & templates)	06/23/14	06/24/14	Kris	Done
7		Copy django auth user table from production to staging.	06/23/14	06/24/14	Kris	Done
8		Remove KPIDs of users that have been removed in Molinar.	06/23/14	06/24/14	Alan, Jenni	Done
9		Test basic server functionality, client access, and client applications (UAM and AI).	06/25/14	06/27/14	Eric, Eddie, Toni	Done
10		Repeat steps 2 to 8 as needed, making adjustments until tests are successful.	06/25/14	06/27/14		Done
	ELI Test Server Setup					
1		Create new TPOZ.			Major, Brian	
2		Configure LI APP and Varnish servers to connect to new TPOZ.			Major, Brian	
3		Set up ELI replication from the new CA staging for testing			Major, Brian	

KLISS 2014 Biennium Rollover Plan
CA & GL Zone Task Summary

No	Project	Task	Start	End	Resource	Status
	CA Production Server Creation:					
1		Select a cutover date and time with the Chamber staff.	06/30/14	06/30/14	Alan, Susan, Corey	Done
2		Create a new TPOZ server.			Major, Brian	Done
3		Run Chisum and Molinar on TPOZ server.			Major, Brian	Done
4		Create and configure Comm server.	10/09/14	11/04/14	Major, Brian	Done
5		Load past biennium data from the TREX archive – system folder (kpids & templates)	10/09/14	11/04/14	Kris	Done
6		Copy django auth user table from 2013-14 production to new 2015-16 production.	10/09/14	11/04/14	Kris	Done
7		Build new py deployment configs for CI/LI/CS	10/09/14	11/04/14	Donnie	Done
8		Install a second instance of the CS on the app server for concurrent interim committee work (2013_14 datastore - /cs_2014/ address) and standing committee work (2015_16 datastore - /cs/ address).	10/09/14	11/30/14	Donnie, Major, Brian	
9		Configure the IRC production vote system to connect to the updated CA production system.	10/09/14	11/04/14	Timothy	Done
10		Copy current pending appointments from CA 2013-14 system to new CA 2015-16 system.	10/09/14	11/04/14	Kris	Done
	GL Production Server Creation:					
1		Select a cutover date and time (same as chamber cutover date).	06/30/14	07/01/14	Alan, Susan, Corey, Amy	Done
2		Create a new TPOZ.			Major, Brian	Done
3		Run Chisum and Molinar on TPOZ server.			Major, Brian	Done
4		Load past biennium data from the TREX archive – system folder (kpids & templates)	10/09/14	11/04/14	Kris	Done
5		Copy django auth user table from 2013-14 production to new 2015-16 production.	10/09/14	11/04/14	Kris	Done
	ELI Production Server Setup					
1		Change test LI to ELI replication to new CA production server. (ELI test will become ELI production)	10/09/14	11/14/14	Major, Brian	
2		Configure new ELI to eliminate load balancer and eliminate one app server.	10/09/14	11/14/14	Major, Brian	
3		Configure ELI Google search to only search in kslegisalture.org/li/b2015_16/ (limit search to current biennium).	10/09/14	11/14/14	Apps Server Team	
	CA Final Production preparation					
1		Fork LI application for 2013/2014 and new 2015/2016	10/09/14	11/04/14	Donnie	Done
2		New LI varnish setup	10/09/14	11/04/14	Major, Brian	Done
3		Complete basic CA & LI server function tests	10/09/14	11/04/14	Eddie, Toni	Done
4		Configure historical 2013/2014 LI proxy on new 2015/2016 LI	10/09/14	11/04/14	Donnie, Kris	Done
5		Chamber staff stop updating current member and committee info in UAM	10/27/14	11/04/14	Corey, Susan	Done
6		Prepare chamber thick client for release.	10/09/14	11/04/14	Andrew	Done
	CA Cutover	**Cutover on 11/5/2014:**				
1		Limit access to the current production servers. Disable user accounts of chamber session staff. (CS users must remain enabled for Interim Committee work) (Chamber full time staff users must remain to allow 2014 updates).	11/05/14	11/05/14	Timothy	Done
2		Incremental copy of system folder from old server .85 into new server .97	11/05/14	11/05/14	Kris	Done
3		Implement new marauder deployment configs for CI (connects CI app to new datastore).	11/05/14	11/05/14	Donnie, Major, Brian	Done
4		Inform users the new biennium system is ready for use.	11/05/14	11/05/14	Alan	Done
5		Provide access information to Susan, Corey, & Amy	11/05/14	11/05/14	Alan	Done
6		Release chamber thick client.	10/09/14	11/04/14	Andrew	Done

KLISS 2014 Biennium Rollover Plan
CA & GL Zone Task Summary

No	Project	Task	Start	End	Resource	Status
	GL Final Production preparation					
1		n/a				
	Election	Election Day	11/04/14	11/04/14	SoS	Done
1		Message on 2013/2014 LI – "Information for the 2015 Legislature will be available after January 2, 2015"	11/04/14	11/04/14	Donnie	Done
2		Election Certified	11/30/14	11/30/14	SoS	
	GL Cutover	**Cutover on 11/5/2014:**				
1		Incremental copy of system folder from old server .91 into new server .78	11/05/14	11/05/14	Kris	Done
2		Implement new marauder deployment configs for UAM/AI.	11/05/14	11/05/14	Donnie, Major, Brian	Done
3		Inform users the new biennium system is ready for use.	11/05/14	11/05/14	Alan	Done
4		Provide access information to Susan, Corey, & Amy	11/05/14	11/05/14	Alan	Done
	Post CA & GL Cutover					
1		Install new thick clients on all chamber computers.	11/05/14	11/30/14	Brian	
2		Configure clients to access the new production server, 10.154.201.97 (DNS name=data.ca.kliss.loc) and test login.	11/05/14	11/30/14	Brian	
3		Implement doc mover service	11/05/14	11/30/14	Donnie, Major, Brian	
4		Configure LM comm server to connect to 2015-15 LM datastore and CA comm server (date set by Revisor Office – after statute publication)	11/05/14	11/30/14	Donnie, Major, Brian	
5		Configure DS comm server to connect to 2015-15 DS datastore and CA comm server (date set by KLRD)	11/05/14	11/30/14	Donnie, Major, Brian	
6		Convert statute files to HTML and post on 2015-16 LI (after statute publication)	11/05/14	11/30/14	Donnie, Major, Brian	
7		Update GASP to use marauder configuration in all zones and environments.	11/05/14	11/30/14	Donnie, Major, Brian	
	CS Cutover					
1		Implement new marauder deployment configs for CS (connects CS app to new datastore).	12/15/15	12/15/15	Donnie, Major, Brian	
2		Committee System available for Committee Assistant training.	12/15/15	12/15/15	Don	
3		Inform KLRD to use /cs.kliss.loc/cs/ to access Committee System for standing committees.	12/15/15	12/15/15	Jim, Alan	
4		Inform KLRD to use /cs.kliss.loc/cs_2014/ to access Committee System for the 2014 interim committees.	12/15/15	12/15/15	Jim, Alan	
5		Inform Committee Assistants to use /cs.kliss.loc/cs/ to access Committee System for standing committees.	12/15/15	12/15/15	Jim, Alan, Don	
	LI / ELI Cutover					
1		LI cutover from 2013/2014 biennium to new site 2015/2016 (2013/2014 under historical link)	01/02/15	01/02/15	Major	
2		Implement new marauder deployment configs for LI (connects LI app to new datastore).	01/02/15	01/02/15	Donnie, Major, Brian	
3		Configure LI server to access the new 2015/2016 site from li.kliss.loc/li/	01/02/15	01/02/15	Major, Brian	
4		Implement new marauder deployment configs for ELI (connects ELI app to new datastore).	01/02/15	01/02/15	Donnie, Major, Brian	
5		Configure ELI server to access the new 2015/2016 site from kslegislature.org/li/	01/02/15	01/02/15	Major, Brian	
6		Message on 2015/2016 LI – "Information on 2013/2014 legislature is available under Historical Data"	01/02/15	01/02/15	Donnie	
	2015 Session Start		01/12/15	01/12/15	Legislature	

KLISS 2014 Biennium Rollover Plan
LM Zone Task Summary

No	Project	Task	Start	End	Resource	Status
	LM Zone:					
	LM TPOZ Staging Server Setup:					
1		Update LM navigator app to new TPOZ CNAME.	06/18/14	06/18/14	Jordan	Done
2		Create a TREX data archive from the current production server. (Note specific head revision of archive)	06/18/14	06/23/14	Major, Brian	Done
3		Create the TPOZ server.	06/23/14	06/24/14	Major, Brian	Done
4		Create the Comm and Search servers (update Comm server software).	06/23/14	06/24/14	Major, Brian	Done
5		Update the Molinar document: - Set folder VVs to b2013_14/base_bills/ → b2013_14/new_base_bills/ on: role_lm_rev_1, role_lm_esec_1, role_lm_sec_1, role_lm_epro_1, role_lm_ped_1, role_lm_brev_1, & role_lm_clerk_1	06/23/14	06/24/14	Alan, Jenni	Done
6		Update the Chisum document.	06/23/14	06/24/14	Eric, Alan, And	Done
7		Run Chisum.	06/23/14	06/24/14	Major, Brian	Done
8		Run Molinar.	06/23/14	06/24/14	Major, Brian	Done
9		Load past biennium data from the TREX archive.	06/23/14	06/24/14	Kris	Done
10		Copy django auth user table from production to staging.	06/23/14	06/24/14	Kris	Done
11		Set all past biennium virtual view mappings to read-only in django admin.	06/23/14	06/24/14	Alan, Jenni	Done
12		Remove KPIDs of users that have been removed in Molinar.	06/23/14	06/24/14	Alan, Jenni	Done
13		Run the script to create shareout folders and sharein virtural views.	06/23/14	06/24/14	Kris	Done
14		Run script to add user in authorization system and create request folders.	06/23/14	06/24/14	Kris	Done
15		Test basic server functionality, client access, and client applications with old client.	06/25/14	06/27/14	Eddie, Toni	Done
16		Repeat steps 3 to 14 as needed, making adjustments until tests are successful.	06/25/14	06/27/14		Done
17		LM Thick Client – Create new client build with updated Barnum.	06/27/14	06/27/14	Jordan	Done
18		Test basic server functionality, client access, and client applications with new client.	06/30/14	07/03/14	Eddie, Toni	Done
19		Repeat steps 3 to 17 as needed, making adjustments until tests are successful.	06/30/14	07/03/14		Done

No	Project	Task	Start	End	Resource	Status
	KLISS 2014 Biennium Rollover Plan					
	LM Zone Task Summary					
	LM Zone:					
	LM Archive Staging Server Setup:					
1		Create the Archive server.			Major, Brian	
2		Configure Apache to serve files in the index format.			Major, Brian	
3		Load the statute base files for 2010, 2011, 2012, 2013, & 2014 years.			Kris, Donnie	
4		For year 2010, copy from 2011_12 production server time machine revision 1/10/2011.			Kris, Donnie	
5		For year 2011, copy from 2011_12 production server time machine revision 1/9/2012.			Kris, Donnie	
6		For year 2012, copy from 2013_14 production server time machine revision 1/10/2013.			Kris, Donnie	
7		For year 2013, copy from 2013_14 production server time machine revision 1/12/2014.			Kris, Donnie	
8		For year 2014, copy from 2013_14 production server time machine head revision (after 2014 hoist).			Kris, Donnie	
9		Configure search server to index and search these statute files.			Eric	
10		Create a TREX archive of the 2011_12 production server of the last revision in production.			Brian	
11		Create a TREX archive of the 2013_14 production server of the last revision in production (after it is shutdown for cutover).			Brian	
12		Store the TREX archives on the Archive Server.			Brian	
13		Create a web application to report APN history and to pull documents from the TREX Archive. This will be an admin application used by system admins.			Kris, Donnie	

1-10

No	Project	Task	Start	End	Resource	Status
	KLISS 2014 Biennium Rollover Plan					
	LM Zone Task Summary					
	LM Zone:					
	LM Production Server Creation:					
1		Select a cutover date and time with the Office of the Revisor.	07/07/14	07/07/14	Jim, Alan, Gordon	Done
2		Create a TPOZ server.	09/01/14	09/23/14	Major, Brian	Done
3		Update Comm server software.	09/01/14	09/23/14	Major, Brian	Done
4		Run Chisum and Molinar.	09/01/14	09/23/14	Major, Brian	Done
5		Load past biennium data from the TREX archive.	09/01/14	09/23/14	Kris	Done
6		Copy django auth user table from 2013-14 production to new 2015-16 production.	09/01/14	09/23/14	Kris	Done
7		Create backup of the new datastore	09/01/14	09/23/14	Major, Brian	Done
8		Confirm production system operation with basic system function tests	09/01/14	09/23/14	Test Team, Revisor Staff	Done
9		Reload datastore with backup to reset data after testing	09/01/14	09/23/14	Major, Brian	Done
	LM Cutover					
1		Make an archive of the current datastore server with TREX.	09/24/14	09/24/14	Kris	Done
2		Load the archive into the new 2015-16 production server. Load folders as defined in LM folder list document.	09/24/14	09/24/14	Kris	Done
3		Run the statute verification process.	09/24/14	09/24/14	Eric, Donnie	Done
4		Create backup of the new datastore.	09/24/14	09/24/14	Brian	Done
5		Install new thick clients on all Revisor computers.	09/24/14	09/24/14	Chad, Sandy	Done
6		Configure clients to access the new production server; DNS name.	09/24/14	09/24/14	Chad, Sandy	Done
7		Inform users the new biennium system is ready for use.	09/24/14	09/24/14	Chad, Sandy	Done
	LM Development, Test, and Staging Environment Server Creation:					
1		Create Staging, Test, and Development Environments Servers.	09/02/14	09/04/14	Major, Brian	Done

KLISS 2014 Biennium Rollover Plan
DS Zone Task Summary

No	Project	Task	Start	End	Resource	Status
	DS Zone:					
	DS datastore Staging Server Setup:					
1		Create a TREX data archive from the current production server. (Note specific head revision of archive)	06/18/14	06/23/14	Kris	Done
2		Create the datastore server.	06/23/14	06/24/14	Major, Brian	Done
3		Create the Comm and Search servers (update Comm server software).	06/23/14	06/24/14	Major, Brian	Done
4		Update the Molinar document.	06/23/14	06/24/14	Alan, Jenni	Done
5		Update the Chisum document.	06/23/14	06/24/14	Eric, Alan, Andrew	Done
6		Run Chisum.	06/23/14	06/24/14	Major, Brian	Done
7		Run Molinar.	06/23/14	06/24/14	Major, Brian	Done
8		Load past biennium data from the TREX archive.	06/23/14	06/24/14	Kris	Done
9		Copy django auth user table from production to staging.	06/23/14	06/24/14	Kris	Done
10		Set all past biennium virtual view mappings to read-only in django admin.	06/23/14	06/24/14	Alan, Jenni	Done
11		Test basic server functionality, client access, and client applications.	06/25/14	06/27/14	Eddie, Toni	Done
12		Repeat steps 2 to 10 as needed, making adjustments until tests are successful.	06/25/14	06/27/14		Done
13		DS Thick Client – Create new client build with updated Barnum.	06/27/14	06/27/14	Jordan	Done
14		Test basic server functionality, client access, and client applications with new client.	06/30/14	07/03/14	Eddie, Toni	Done
15		Repeat steps 2 to 13 as needed, making adjustments until tests are successful.	06/30/14	07/03/14		Done
	DS Archive Staging Server Setup:					
1		Create the Archive server.			Major, Brian	
2		Load the Liberty archive documents.			Major, Brian	
3		Configure Apache to serve files in the index format.			Major, Brian	
4		Configure search server to index and search these statute files.			Eric	
5		Create a TREX archive of the 2011_12 production server of the last revision in production.			Brian	
6		Create a TREX archive of the 2013_14 production server of the last revision in production (after it is shutdown for cutover).			Brian	
7		Store the TREX archives on the Archive Server.			Brian	
8		Create a web application to report APN history and to pull documents from the TREX Archive. This will be an admin application used by system admins.			Kris, Donnie	

KLISS 2014 Biennium Rollover Plan
DS Zone Task Summary

No	Project	Task	Start	End	Resource	Status
	DS Zone:					
	DS Production Server Creation:					
1		Select a cutover date and time with KLRD.	07/01/14	07/01/14	Alan, Amy	Done
2		Create a datastore server.	08/04/14	08/15/14	Major, Brian	Done
3		Update Comm server software.	08/04/14	08/15/14	Major, Brian	Done
4		Run Chisum and Molinar.	08/04/14	08/15/14	Major, Brian	Done
5		Load past biennium data from the TREX archive.	08/04/14	08/15/14	Kris	Done
6		Copy django auth user table from 2013-14 production to new 2015-16 production.	08/04/14	08/15/14	Kris	Done
7		Verify system operation	08/04/14	08/15/14	Test team	Done
	DS Cutover					
1		Make an archive of the current datastore server with TREX.	10/02/14	10/02/14	Kris	Done
2		Load the archive into the new 2015-16 production server. Load folders as defined in DS folder list document.	10/02/14	10/02/14	Kris	Done
3		Create backup of the new datastore.	10/02/14	10/02/14	Brian	Done
4		Install new thick clients on all KLRD computers. Remote install.	10/02/14	10/02/14	LuAnn, Carita	Done
6		Configure clients to access the new production server; DNS name.	10/02/14	10/02/14	LuAnn, Carita	Done
7		Inform users the new biennium system is ready for use.	10/02/14	10/02/14	LuAnn, Carita	Done
	DS Staging, Test, and Development Environment Server Creation:					
1		Create Staging, Test, and Development Environments Servers.	10/06/14	10/10/14	Major, Brian	Done

ISSUE (Per LM Document)	JIRA TICKET	NOTES	Collaboration Notes	Develop ment Sprint
Bookmark Issues				
Missing or moved bookmarks should never occur.	LMPRATCH-80 (EPIC) LMPRATCH-46 LMPRATCH-49 LMPRATCH-55 LMPRATCH-58 LMPRATCH-92			2
Title Issues				
Stricken language in the title remains stricken after importing. See test script: Title – Stricken language must be retained after importing.	LMPRATCH-54			3
The title should not contain repetitive references to K.S.A or K.S.A. Supp. See test script: Title – K.S.A. and K.S.A. Supp. should appear once in the title.	LMPRATCH- 96	Test this and ask about it. It doesn't seem to be reproducible	Re-tested, ticket created	3
Added language in the title is retained, including chamber styles. See test script: Title – Added language in the title is removed upon importing sections into the delta.	LMPRATCH- 85 LMPRATCH- 54			3
All automatically added language must be placed after automatically stricken language. See test script: Title – New language should always appear after stricken language.	LMPRATCH-86	(NEW ticket re-word "All" to specific case) Reproducible, use 2013 supp data.		3
Statute sections retain proper characters when imported. See test script: Title – Missing dash when statute section imported contains more than one dash.	LMPRATCH-87 (NEW)			3
Addition of statute sections that contain a letter update the title regardless if there is a statute section containing the same number. (Example: 12-4516 and 12-4516a) This occurred often during the 2014 Session but we have not been able to reproduce in testing.	LMPRATCH-23	Conflicts with request made LMPRATCH-23 need RS to clarify which one they want it to do.	RS clarified, same as LM-23	3
Repealer Issues				
Repealer – Markup must be retained after importing. Chamber styles strip out after importing. See test script: Repealer—Chamber styles not staying when imports are added to delta.	LMPRATCH-60			2

The word "is" automatically updates to "are" when adding statute section(s) to the delta and creates a bill with more than one statute section. The "is" is stricken (red) and always followed by "are" added (blue) in the Repealer and there is no space between the stricken and new language. See test script: Repealer — adding statute sections to a one statute section bill should properly update the Repealer.	LMPRATCH-5			2
Statute sections retain proper characters when imported. See test script: Repealer – Missing dash when statute section imported contains more than one dash.	See LMPRATCH-87			3
Table Issues				
Tables within amendatory sections will properly import and correct styles will be retained. Refer to LMPRATCH-62.	LMPRATCH-62	This should be top priority, do you want to remove some less important issues and move this in their place? (ex, commas out of place, plurals incorrect. Possibly remove LM-54 and put this one in its place.)	Unknown for now... 20140722 Gordon wants to see development time before he decides if this will be a priority.	4
Additional Delta Issues				
Remove section through KLISS menu should strike the section in the title, bill and repealer. See test script: Striking a section using KLISS Remove Section from delta.	LMPRATCH-88 (NEW)			4
Section numbers, subsection designations, and other sub-elements will automatically update when required in the delta. See scripts: System not automatically updating section or subsections and Delta – Section 1 renumbering issues.	LMPRATCH-89 (NEW) LMPRATCH-90 (NEW)	Import a range may solve this problem. This ticket has been broken down into two separate tickets.		4
Bill text imports will recognize sections from bills, including those with chamber mark up. See test script: Bill Text import from bill with Chamber section number markup: "Section not found"	LMPRATCH- 94	A space in front of the section is causing the problem. Incorrect formatting is causing it not to be recognized as a section.	Bill para norm, lm stat?- should not have 2 continuous spaces. Should not be a lead in blank space... Some tab tables may have one. Solution: Trim leading and trailing spaces if they exist. Fix universal formatting? This fixes across the board (drafts, deltas, etc...)	4
Statutory sections and bill text sections must apply the correct paragraph styles and backgrounds. Incorrect styles and backgrounds cause the amendatory language report to not contain all statute section text upon generation of the report. See test script: Delta – Statute import drops blue-gray highlight.	LMPRATCH-91 (NEW)	Imported statute losing blue/grey background when imported in ranges.		4

Remove Section KLISS function should correctly update the title in the bill. See test script: Delta – Remove section functionality removes "s" on sections and doesn't remove KSA number from the title.	LMPRATCH-46			2
A statute section with a grid should accurately import into the delta. See test script: Importing a statute section containing a Grid.	No Issue Found	Format statues to anchor to paragraph not page and it works fine.	Reproduced with success. No ticket created.	
Reinserting a section through an import that is previously stricken in the bill should update the title, properly appear in the bill with the correct styles applied, and update the repealer. See test script: Statute section stricken in bill and reinserted by amendment does not update correctly in the delta (Title, Bill and Repealer).	LMPRATCH-60			2
The system should add the correct text when adding a New Section 1. See test script: Adding a New Section – Adding "tion" and removing the period.	LMPRATCH-51			4
Title should remain in its correct location on the bill and not be altered when importing. Refer to LMPRATCH-64.	LMPRATCH-64.			3
The ability to create deltas and amendatory language on all types of resolutions is still needed.	No Issue Found			
The cursor should return to the end of the import into Deltas or bill drafts. Refer to LMPRATCH-9	LMPRATCH-9			4
Amendatory Report Issues				
Statutory sections and bill text sections must contain all language upon being imported. See test script under Delta Issues: Delta-Statute import drops blue-gray.	See LMRATCH-91	Repeated issue		4
Statutory sections and bill text sections must retain any mark up and any character styles (i.e., italics) from the source. See test script: Italics are not holding in amendatory language.	LMPRATCH-67			1
Language is stricken in the amendatory language report and does not match the correct mark up in the delta. See test script: Amendatory Language Report – Incorrect in report when striking a comma in the delta.	LMPRATCH-68			1
The correct instructions should generate from the delta into the amendatory language report. The report often generates with the language "On page RROR, in the title". See test script: amendatory Language Report – Instructions should be accurate	LMPRATCH-92 (NEW)	Switches sections to section and deletes the bookmark in the process. On page error doesn't occur in new build. Check to see if RS user has current production build.	Problem with Delta creating report.	2

The renumbering sections clause only appears once in the document and should be placed before any instructions for amendments to the repealer. If there is no repealer or no amendments to the repealer, the clause should be placed between the amendatory language and the title instructions. See test script: Amendatory Language Report – Section Renumbering Clause should be before the repealer language.	Will be part of epic LMPRATCH-83			1
The document name appears on the top, right corner of each page of the amendatory language document regardless of the original length of the amendatory language document before making it two or more pages. See test script: Amendatory Language Report – Document name on Page 2 incorrect.	LMPRATCH-47			1
Stricken material for an entire line in the bill should be referred to in the amendatory language as "all in line #" not appear as stricken in the instructions. See test script: Amendatory Language Report—Language should state when entire lines are stricken and not show stricken text.	LMPRATCH-97			1
The word "substitute" should be capitalized in the amendatory language report for substitute bills. Refer to LMPRATCH-48.	LMPRATCH-48			1
Correct heading should be generated with Substitute for Substitutes. Refer to LMPRATCH-48 and test script: Sub for Sub Committee Report and Bill Draft Heading are missing "for".	LMPRATCH-48			1
When sections are renumbered in the delta, the amendatory language should not include instructions for each renumbering individually. (Encountered during 2014 Session) **Example: On page 7, in line 43, by striking "9." And inserting "12."; On page 8, in line 25, by striking "10." and inserting "13.";			SHOULD NOT OCCUR IN THE NEW VERSION.	
The system should pull the correct title information into the committee report for a substitute bill. Refer to LMPRATCH-38.	LMPRATCH-38			3

Legislative Printer Refresh:
- Many of the legislative printers are 7+ years old. The printer refresh project will replace these printers. Newer printers will be kept in service.
- Printers/copiers currently owned by LAS will be replaced with leased models.
- The new lease contract is based on the current residual value of each printer. Printers with no residual value will have only service costs with zero lease cost. If the older printers break and can not be repaired, Logan will replace with an equivalent printer at no additional cost.
- Service costs for all printers, based on current volumes, is about $5,100/month.
- 129 total printers on Logan service contract; 59 printers with equipment lease cost and service cost; 70 printers with no residual value will be kept in service incurring service costs only.

State Security Council Work:
- A workgroup of the State Security Council made up of representatives from the KBI, INK, KU Medical Center, University of Kansas, Kansas State University, and the legislature updated the ITEC Policies 7230 and 7230-A.
- The policies were approved by ITEC on 11/05/2014.
- The new policy identifies the minimum security standards to be implemented by all state agencies.
- The workgroup will meet quarterly to create resource materials to assist agencies in implementing the new policy.

Cellular Phone Signal on Ground Floor and Sub Vaults:
- OFPM working with TFM Comm to install cellular signal repeaters
- The system interfered with the AT&T cellular signal. Installed an attenuator and working with AT&T on resolving the system configuration issue.

Wireless Network Upgrade:
- The wireless upgrade project will be completed 11/13/2014. Upgraded 43 existing access points and added 25 new access points – expected increase in capacity ~ 3x – 4x (actual change tbd).

Security Training:
- The Tunnel of Tech Terror had a Halloween theme, introduced users to 8 cybersecurity threats in an entertaining environment.
- Activities included: Norris cyber-attack tracking, USB flash drive virus, Hack a Password, web browser extensions, social media, altered ID cards, etc. Follow up planned.

Video Training:
- Courses are interactive using Mindflash to create online training courses.
- Record student's course history to provide documentation of required training
- Will be introduced to legislators and session staff in January, 2015

Server Virtualization Project:
- This project was completed in early November.

Broadcast Media Access:
- Final acceptance testing is scheduled for 11/24 – 11/25.
- Training will be 11/26 for OFPM, KLOIS, and OITS staff.
- A media introduction day will be held in December.
- Locations for live broadcasts are the House Chamber, South Steps, South Lawn, Ground Floor East Corridor (Media Row).

1-17

Attachment E: Printer Refresh Inventory Workbook as of 11/10/2014
JCIT Status Update -- 13 Nov 2014 -- Kansas Legislative Office of Information Services

1-18

DEPARTMENT	LOCATION	ID #	MAKE	MODEL	MONTHLY AVERAGE	Own or Lease	RETAIN	REASON	NEW PRINTER MAKE	NEW PRINTER MODEL	FOLLOW ME PRINTING	Pages per Minute	Color or B/W	Scanning	Finisher	11" x 17" Tray	Fax	Service Rate B/W	Service Rate Color	New 5Yr cost	New 3Yr Cost
Crows Nest	Missing	L4539	Lexmark	ES460DN		Lease	no	Missing	N/A	N/A											
House Appro.	111N	TOP2412	Lexmark	C782	0 B/W 0 COLOR	Lease	no	better equipment	Sharp	MXC402SC	yes	40	color	yes	no	no	no	0.0179	0.067	104.12	157.4
House Clerk	272W	LBM4488	Lexmark	ES460DN		Lease	yes											18.00 MO			
House Clerk	273W	LBM4432	Lexmark	ES460DN		Lease	yes											18.00 MO			
House Clerks	273W	TOP1893	Sharp	AR-M455U	60 B/W	Own	yes											0.012			
House Clerks	273W	TOP2442	Sharp	C782		Lease	yes											0.0179	0.067		
House Clerks	273W	LBM4493	Lexmark	ES460DN		Lease	yes											18.00 MO			
House Clerks	273W	TOP2403	Sharp	MX-7000N	3,000 B/W 1,000 COLOR	Own	yes				yes							0.0085	0.05		
House of Rep	House Chambers Back Wall	TOP2395	Sharp	MX-3100N	0	Own	yes				yes							0.012	0.067		
House of Representati	House Chamber (Clerks Desk)		HP	4250N		Lease	no	old service cost	Lexmark	M460DN 1ea From out of service tsock								18.00 MO			
House of Representati	House Chamber (Speakers Desk)		HP	4250N		Lease	no	old service cost	Lexmark	M460DN 1ea From out of service tsock								18.00 MO			
KLOIS	63W	TOP1747	Sharp	AR-M277	620 B/W	Own	no	old out of life	Sharp	MX314	yes	31	B/W	yes	no	yes	no	0.012		60.93	93.76
KLOIS	48S	TOP2410	Lexmark	C782	200 B/W 100 COLOR	Lease	no	replace with better equipment	sharp	MX301	Pending	30	color	yes	no	no	yes	0.012	0.067	50.82	78.19
KLOIS	58A-S	LBM4445	Lexmark	ES460DN		Lease	no	Not in use	N/A	N/A											
KLOIS	Store Room (000-S)	LBM3521	Lexmark	W840		Lease	no	Not in use	N/A	N/A											
KLOIS	58C-S	TOP2414	Lexmark	XM642E	0	Lease	no	Not in use	N/A	N/A											
KLOIS	58A-S	TOP1181	Sharp	AR-M620N	60	Own	yes											0.012			
KLOIS	63W	TOP2443	Lexmark	C534DN		Lease	yes											0.0179	0.067		
KLOIS	58A-S	TOP2416	Lexmark	C935		Lease	yes											0.0179	0.067		
KLOIS	48S	LBM4561	Lexmark	ES460DN		Lease	yes											18.00 MO			
KLOIS	63W	LBM4499	Lexmark	ES460DN		Lease	yes											18.00 MO			
LAS	220E	TOP0978	Sharp	AR-M237	850 B/W	Own	no	old out of life	Sharp	MXB402SC	yes	40	B/W	yes	yes	no	no	0.01		93.26	144.78
LAS	129A-E	TOP1697	Sharp	AR-M550N	4,000 B/W	Own	no	age, Volume, follow me print	Sharp	MXB402SC	yes	40	B/W	yes	yes	no	no	0.01		93.26	144.78
LAS	220E	TOP1689	Sharp	AR-M550N	3,000 B/W	Own	no	age, Volume, follow me print	Sharp	MXB402SC	yes	40	B/W	yes	yes	no	no	0.01		93.26	144.78
LAS	460W	TOP1684	Sharp	AR-M620N	8,700 B/W	Own	no	age, Volume, follow me print	Sharp	MXB402SC	yes	40	B/W	yes	yes	no	no	0.01		93.26	144.78
LAS	512 N	TOP1690	Sharp	AR-M620N	3,000 B/W	Own	no	age, Volume, follow me print	sharp	MXB402SC	yes	40	B/W	yes	yes	no	no	0.01		93.26	144.78
LAS	551S	TOP1248	Sharp	AR-M620N	7,000 B/W	Own	no	age, Volume, follow me print	Sharp	MX5141	yes	51	color	yes	yes	yes	no	0.01	0.05	225.72	364.26
LAS	RM 551S		HP 3ea	Printers		Lease	no	old service cost	Lexmark	M460DN 3ea From out of service tsock											
LAS	188N	TOP1698	Sharp	AR-M277	1,000 B/W	Own	yes	Back up										0.012			
LAS	188 N	TOP1688	Sharp	AR-M550N	3,200 B/W	Own	yes											0.012			
LAS	228E	TOP1696	Sharp	AR-M550N	5,100 B/W	Own	yes											0.012			
LAS	175A-W	TOP1256	Sharp	AR-M550U	6,400 B/W	Own	yes											0.012			
LAS	274W	TOP1618	Sharp	AR-M550U	1,300 B/W	Own	yes											0.012			
LAS	45S Copy Room	TOP0955	Sharp	AR-M550U	1,200 B/W	Own	yes											0.012			
LAS	360 W	TOP0824	Sharp	AR-M620N	5,250 B/W	Own	yes	add equipment from room 359	Sharp	MX363	yes	36	B/W	yes	yes	yes	no	0.012		161.61	148.66

Attachment E: Printer Refresh Inventory Workbook as of 11/10/2014
JCIT Status Update -- 13 Nov 2014 -- Kansas Legislative Office of Information Services

1-19

DEPARTMENT	LOCATION	ID #	MAKE	MODEL	MONTHLY AVERAGE	Own or Lease	RETAIN	REASON	NEW PRINTER MAKE	NEW PRINTER MODEL	FOLLOW ME PRINTING	Pages per Minute	Color or B/W	Scanning	Finisher	11" x 17" Tray	Fax	Service Rate B/W	Service Rate Color	New 5Yr cost	New 3Yr Cost
Leadership	472W (Intern)	TOP1687	Sharp	AR-M455N	500 B/W	Own	no	too old	Sharp	MXB402SC	yes							0.01			
Leadership (House Majority)	372W	TOP1699	Sharp	AR-M455N	11,000 B/W	Own	no	age, Volume, follow me print	sharp	MX465	yes	46	B/W	yes	yes	yes	no	0.0085		116.86	179.81
Leadership (House Majority)	472W	TOP2408	Lexmark	C782	1,300 B/W 250 COLOR	Lease	no	replace with better equipment	sharp	MXC402SC	yes	40	color	yes	no	no	no	0.012	0.067	103.29	158.66
Leadership (House Min)	359 W	LBM4491	Lexmark	ES460DN		Lease	yes											18.00 MO			
Leadership (House Min)	359 W	LBM4489	Lexmark	ES460DN		Lease	yes											18.00 MO			
Leadership (House Min)	359W	LBM5023	Sharp	MX-M363N	940 B/W	Lease	yes	replace and move to 360W	Sharp	MXC402SC	yes	40	color	yes	no	no	no	0.012	0.067	103.29	158.66
Leadership (House Speaker)	468W	TOP2411	Lexmark	C782	350 B/W 220 COLOR	Lease	no	replace with better equipment	sharp	MXC402SC	yes	40	color	yes	no	no	no	0.012	0.067	103.29	158.66
Leadership (House Speaker)	370W			HP2840		Lease	no	old, high cost	sharp	MX301	Pending							0.012	0.067		
Leadership (House Speaker)	369W	LBM4487	Lexmark	ES460DN		Lease	yes											18			
Leadership (Pro Tem)	381 W	TOP2441	Lexmark	C782		Lease	yes											0.0179	0.067		
Leadership (Pro Tem)	352 S	LBM4492	Lexmark	ES460DN		Lease	yes											18.00 MO			
Leadership (Sen VP)	341E	TOP2418	Lexmark	C782		Lease	yes											0.0179	0.067		
Leadership (Senate Min)	318E	TOP1259	Sharp	AR-M620N	3,400 B/W	Own	no	age, Volume, follow me print	sharp	MXB402SC	yes	40	color	yes	yes	no	no	0.01		94.07	144.78
Logan	Logan	L3522	Lexmark	ES460DN		Lease	no	Not in use	N/A	N/A											
Logan	Logan	TOP2440				Lease	no	Not in use	N/A	N/A											
Post Audit	1215	LBM4455	Lexmark	460DN		Lease	yes											18.00 MO			
Post Audit	1200	LBM4451	Lexmark	ES460DN		Lease	yes											18.00 MO			
Post Audit	1219	TOP2391	Sharp	MX-7000N	150 B/W 1,200 COLOR	Lease	yes				yes							0.0085	0.05		
Post Audit	1219	MAN2507	Sharp	MX-M850	24,000	Lease	yes				yes							0.004			
Post Audit	1200	TOP2415	Lexmark	XM642E		Lease	yes											0.012			
Research	77W Copy Room New Addition			MFP	Similar to MX7001	Lease	N/A	KLRD request	Sharp	MX-6240	yes	62	Color	Yes	Yes	Yes	Yes	0.0085	0.05	314.87	485.19
Research	68W Main Front	LBM4463	Lexmark	460DN		Lease	no	KLRD request	N/A	N/A											
Research	68W North Center	LBM4423	Lexmark	460DN		Lease	no	KLRD request	N/A	N/A											
Research	68W North Back	LBM4471	Lexmark	460DN		Lease	no	KLRD request	N/A	N/A											
Research	68W Main Back	LBM4466	Lexmark	460DN		Lease	no	KLRD request	Sharp	MX6240	yes	62	Color	Yes	Yes	Yes		0.0085	0.05	303.85	467.52
Research	77W North Front	LBM4461	Lexmark	460DN		Lease	no	KLRD request	N/A	N/A											
Research	55S South Hall Annex	TOP2396	Sharp	MX-3100N	330 B/W 300 COLOR	Lease	no	KLRD request	N/A	N/A											
Research	68W Copy Room Moving to Annex	LBM4559	Sharp	MX-5001N	8,400 B/W 6,000 COLOR	Lease	no	KLRD request	Sharp	MX6240	yes	62	Color	Yes	Yes	Yes	no	0.0085	0.05	303.85	467.52
Research	77W North Hall	TOP2400	Sharp	MX-7000N	9,000 B/W 5,000 COLOR	Lease	no	KLRD request	Sharp	MX6240	yes	62	Color	Yes	Yes	Yes	no	0.0085	0.05	303.85	467.52
Research	68W Bobbi	LBM4452	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W LuAnn	LBM4469	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W Amy	LBM4464	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W Melissa	LBM4462	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W Dylan	LBM4470	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W Deb	LBM4468	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W Sheila	LBM4424	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W J.G.	LBM4425	Lexmark	460DN		Lease	yes											18.00 MO			
Research	77W Rebecca	LBM4426	Lexmark	460DN		Lease	yes											18.00 MO			
Research	77W Rainey	LBM4320	Lexmark	460DN		Lease	yes											18.00 MO			
Research	68W Main Color 1	LBM4485	Lexmark	C796		Lease	yes											0.0179	0.067		
Research	68W North Color 2	LBM4484	Lexmark	C796		Lease	yes											0.0179	0.067		
Research	77W North Color 1	LBM4563	Lexmark	C796		Lease	yes											0.0179	0.067		
Research	77W Main Color 2	LBM4546	Lexmark	C796		Lease	yes											0.0179	0.067		
Research	62W Missy Reception	LBM4422	Lexmark	ES460DN		Lease	yes											18.00 MO			

1-20

DEPARTMENT	LOCATION	ID #	MAKE	MODEL	MONTHLY AVERAGE	Own or Lease	RETAIN	REASON	NEW PRINTER MAKE	NEW PRINTER MODEL	FOLLOW ME PRINTING	Pages per Minute	Color or B/W	Scanning	Finisher	11" x 17" Tray	Fax	Service Rate B/W	Service Rate Color	New 5Yr cost	New 3Yr Cost
Revisor	24E Front Copy Room	TOP0825	Sharp	AR-M620N	4,100 B/W	Own	no	Revisor request - old and slow to start up	Sharp	MX623	yes	62	B/W	yes	yes	yes	no	0.0085		289.57	445.57
Revisors	24E (In Session) 52AS (out)	LBM4543	Lexmark	460DN		Lease	???	Please quote both retain and upgrade with color, duplex, larger tray	lexmark	CS796DE		50	Color					0.0179	0.067	41.88	64.43
Revisors	24E (In Session) 52AS (out)	LBM4473	Lexmark	460DN		Lease	???	Please quote both retain and upgrade with color, duplex, larger tray	Lexmark	CS796DE		50	Color					0.0179	0.067	41.88	64.43
Revisors	24E Debra Davis	LBM4444	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Chad Champney	LBM4548	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Jill Wolters	LBM4477	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E I/T Room	LBM4472	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E I/T Room	LBM4465	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Scott Wells	LBM4498	Lexmark	ES460DN		Lease	yes	Please quote both		Add 550 sheet								18.00 MO		6.63	10.2
Revisors	24E Natalie Scott	LBM4475	Lexmark	ES460DN		Lease	yes	Please quote both		Add 550 sheet								18.00 MO		6.63	10.2
Revisors	24E Adam Siebers	LBM4481	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Chuck Reimer	LBM4479	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Norm Furse	LBM4483	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Pearlie Shupe	LBM4482	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Gordon Self	LBM4496	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2

DEPARTMENT	LOCATION	ID #	MAKE	MODEL	MONTHLY AVERAGE	Own or Lease	RETAIN	REASON	NEW PRINTER MAKE	NEW PRINTER MODEL	FOLLOW ME PRINTING	Pages per Minute	Color or B/W	Scanning	Finisher	11" x 17" Tray	Fax	Service Rate B/W	Service Rate Color	New 5Yr cost	New 3Yr Cost
Revisors	24E Nick Meyers	LBM4474	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Daniel Yoza	LBM4497	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Mike Heim	LBM4495	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Eileen Ma	LBM4476	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Renae Jefferies	LBM4467	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Tamera Lawrence	LBM4500	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Open Office	LBM4547	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E OpenCubicle	LBM4541	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Matt Sterling	LBM4453	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Nobuko Folmsbee	LBM4562	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Jason Long	LBM4478	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E David Weise	LBM4480	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Jason Thompson	LBM4454	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2

1-22

DEPARTMENT	LOCATION	ID #	MAKE	MODEL	MONTHLY AVERAGE	Own or Lease	RETAIN	REASON	NEW PRINTER MAKE	NEW PRINTER MODEL	FOLLOW ME PRINTING	Pages per Minute	Color or B/W	Scanning	Finisher	11" x 17" Tray	Fax	Service Rate B/W	Service Rate Color	New 5Yr cost	New 3Yr Cost
Revisors	24E Katherine McBride	LBM4542	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Eunice Peters	LBM4540	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Sandy Sadowski	LBM4477	Lexmark	ES460DN		Lease	yes	Please quote both retain and upgrade with duplex, larger tray		Add 550 sheet tray								18.00 MO		6.63	10.2
Revisors	24E Back Hall	TOP1694	Sharp	AR-275		Own	no	Revisor request - do not replace													
Revisors	24E Pod #1	TOP1049	Sharp	AR-M237	400 B/W	Own	no	Revisor request - do not replace	N/A	N/A											
Revisors	24E Pod #3	TOP1050	Sharp	AR-M237	500 B/W	Own	no	Revisor request - do not replace	N/A	N/A											
Revisors	24E - Revisor's Pod	TOP2409	Lexmark	C782	3,000 B/W 3,000 COLOR	Lease	no	Revisor request	Lexmark	CS796DE		50	Color	yes	Stands		yes	0.0179	0.067	41.88	64.43
Revisors	24E - Back Hall	TOP2413	Lexmark	C782	2,000 B/W 2,000 COLOR	Lease	no	Revisor request	Lexmark	CS796DE		50	Color	yes	Stands		yes	0.0179	0.067	41.88	64.43
Revisors	24E Pod #3	TOP2406	Lexmark	C782		Lease	no	Revisor request	Lexmark	CS796DE		50	Color	yes	Stands		yes	0.0179	0.067	41.88	64.43
Revisors	24E Pod #1	LBM4545	Lexmark	CS796DE		Lease	no	Revisor request		Add 550 sheet tray		50	Color	yes	Stands		yes	0.0179	0.067	7.37	12.25
Revisors	24E Pod #2	LBM4544	Lexmark	CS796DE		Lease	no	Revisor request		Add 550 sheet tray		50	Color	yes	Stands		yes	0.0179	0.067	7.37	12.25
Revisors	24E Debbie Meador	?????	Lexmark	ES460DN		Lease	no	Revisor request	Lexmark	CS796DE		50	Color	yes	Stands		yes	0.0179	0.067	41.88	64.43
Revisors	24E Front Copy Room	TOP2402	Sharp	MX-7000N	2,100 B/W 3,200 COLOR	Lease	no	Revisor request - old and slow to start up	Sharp	MX3640	yes	36	Color	yes	yes	yes	no	0.01	0.05	162.2	249.57
Revisors	24E I/T Room	TOP2496	Lexmark	W840		Lease	no	Revisor request	Lexmark	CS796DE		50	Color	yes	Stands		yes	0.0179	0.067	41.88	64.43
Revisors	24E Annette Duffy	TOP2495	Lexmark	W840		Lease	no	Revisor request	Lexmark	CS796DE		50	Color						0.0179	0.067	41.88	64.43
Revisors	24E Sara Stevens	TOP2444	Lexmark	W840DN		Lease	no	Revisor request	Lexmark	CS796DE		50	Color						0.0179	0.067	41.88	64.43
Revisors	24E Jan Fisher	TOP2493	Lexmark	W840DN		Lease	no	Revisor request	Lexmark	CS796DE		50	Color						0.0179	0.067	41.88	64.43
Revisors	24E Back Hall	TOP2494	Lexmark	W840DN		Lease	no	Revisor request	Lexmark	CS796DE		50	Color						0.0179	0.067	41.88	64.43
Senate Maj	427E	TOP2398	Sharp	MX-3100N	0	Lease	yes				yes							0.012	0.067		
Senate Maj	330E	LBM4537	Lexmark	TS654DN		Lease	yes											0.012			
Senate Pres	329E	TOP1691	Sharp	AR-M620N	12,000 B/W	Own	no	age, Volume, follow me print	sharp	MX565	yes	56	B/W	yes	yes	yes	no	0.0085		176.71	271.89
Senate Pres	333E	TOP2419	Lexmark	C782		Lease	yes											0.0179	0.067		
Senate Pres	329E	LBM4446	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Pres	331E	LBM4448	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Pres	434E	LBM4494	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Pres	430E	TOP2397	Sharp	MX-3100N	0	Own	yes				yes							0.012	0.067		
Senate Sec	429E	TOP1695	Sharp	AR-M455N	320 B/W	Own	no	age, Volume, follow me print		MXB402SC	yes	40	B/W	yes	no	no	no	0.01		73.29	112.73
Senate Sec	432E	TOP2407	Lexmark	C782		Lease	yes											0.0179	0.067		
Senate Sec	325E	LBM4450	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Sec	429E	LBM4459	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Sec	429E	LBM4460	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Sec	432E	LBM4447	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Sec	Sen Chamber (Pres Desk)	LBM4449	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Sec	Sen Chamber (Sen Sec Desk)	LBM4443	Lexmark	ES460DN		Lease	yes											18.00 MO			
Senate Sec	325E	LBM4774	Sharp	MX-5111N	4,000 B/W 2,000 COLOR	Lease	yes					yes							0.0085	0.05	56.32	78.16
Senate Ways & Means	545S	TOP1693	Sharp	AR-M455N	2,500 B/W	Own	no	age, Volume, follow me print	sharp	MXB402SC	yes	40	B/W	yes	no	no	no	0.01		73.29	112.73
																				4309.16	6543.97
Follow Me Printing																					234.79	361.26
InfoDynamic Indexing																					861.86	1326.09

Kansas Information Technology Executive Council

Information Technology Policy 7230 Revision 2 - Information Technology Enterprise Security Policy

1.0 TITLE: Information Technology Enterprise Security Policy

      1.1   EFFECTIVE DATE: 11/5/2014

      1.2   TYPE OF ACTION: Update

2.0 KEYWORDS: Enterprise Security Policy, Information Security, User Security, Physical Security, Default Security Requirements, Network Security, Security Administration, Security Incident Response.

3.0 PURPOSE: To define the minimum requirements for enterprise information technology security policy, standards, and procedures.

4.0 ORGANIZATIONS AFFECTED: All State of Kansas branches, boards, commissions, departments, divisions, agencies, and third parties used to process transmit or provide business capabilities on behalf of Kansas state government, hereafter referred to as Entities.

5.0 REFERENCES:

      5.1   K.S.A. 2013 Supp. 75-7203 authorizes the Kansas Information Technology Executive Council (ITEC) to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state entities.

      5.2   Kansas Information Technology Executive Council (ITEC), ITEC Policy 7300R1, Information Technology Security Council Charter.

6.0 DEFINITIONS:

      6.1   Security policy is defined as a collection of mandates, actions and required documentation governing the security protections and controls of an entity.

      6.2   The Information Technology Security Standards 7230A (7230A) is supplemental to this policy and is defined as a document published by the Kansas Information Technology Executive Council that contains minimum security controls all entities will apply to personnel, processes and assets.

7.0 POLICY:

      7.1   Entities shall implement an Information Technology Security Policy for their organization. All Information Technology Security Policies adopted by the Entity must be at least as stringent as this policy. Entities that do not implement their own Information Technology Security Policy shall implement this policy in accordance with the standards and procedures referenced in the Information Technology Security Standard 7230A.

      7.2   Planning and Risk Assessments:

            7.2.1   Entities shall ensure risk assessments are performed for information systems in accordance with 7230A Assessments and Security Planning standard and the Risk Management standard.

            7.2.2   Entities shall ensure the development and implementation of a security plan for information systems in accordance with the 7230A Assessment and Security Planning standard.

1-23

      7.2.3   Entities shall preform a vulnerability assessment and security assessments on information systems in accordance with 7230A System Operations standard.

7.3   Awareness and Training:

      7.3.1   Entities shall implement Security Awareness and Security Operations Training in accordance with 7230A Awareness and Training Standard.

7.4   Access Control:

      7.4.1   Entities shall ensure that only authorized users are granted access to systems and data in accordance with 7230A Access Control standard and Physical Security Standard.

      7.4.2   Entities shall ensure authentication accounts are actively managed in accordance with 7230A Access Control Standard and Personnel Security standard.

7.5   Configuration Management:

      7.5.1   Entities shall document standardized configurations settings for information systems in accordance with 7230A System Configuration standard.

      7.5.2   Entities shall maintain an asset inventory of information systems in accordance with 7230A System Configuration standard.

      7.5.3   Entities shall implement a change control process in accordance with 7230A Change Control standard.

7.6   Media Protection:

      7.6.1   Entities shall perform data/media sanitization in accordance with 7230A Data Protection standard and Physical Security standard.

7.7   System and Communication Protection:

      7.7.1   Entities shall protect information systems with dedicated protection mechanisms in accordance with 7230A System Configuration standard.

      7.7.2   Entities shall classify and protect both data and information systems in accordance with 7230A Data Protection, System Configuration, Assessment and Security Planning standards.

7.8   System and Information Integrity:

      7.8.1   Entities shall document application development standards in accordance with 7230A Application Processing standard.

      7.8.2   Entities shall monitor system configuration integrity in accordance with 7230A System Operation standard.

      7.8.3   Entities shall ensure that information systems are configured to log events in accordance with 7230A System Audit standard.

      7.8.4   Entities shall ensure that information systems are time synchronized in accordance with 7230A System Audit standard.

7.9   Third Parties:

      7.9.1   Entities shall not reduce its security profile for the purpose of conducting third-party audits.

      7.9.2   Entities shall ensure that physical and logical security control testing by third parties is conducted within pre-defined and documented parameters.

1-24

7.10   Incident Response:

   7.10.1   Entities shall document security incident response procedures in accordance with 7230A Incident Response standard.

   7.10.2   Entities shall report incidents as in accordance with 7230A Incident Response standard.

7.11   Physical and Environmental Protection:

   7.11.1   Entities shall implement physical access controls in accordance with 7230A Physical Security standard.

   7.11.2   Entities shall implement physical environmental controls in accordance with 7230A Physical Security standard.

7.12   Personnel Security:

   7.12.1   Entities shall document acceptable use of information system in accordance with 7230A Personnel Security standard.

7.13   System and Service Acquisition:

   7.13.1   Entities shall ensure proper due diligence in assessing security capabilities and requirements of any third party purchased or provided system in accordance with 7230A Secure Purchasing/Acquisition standard.

8.0 RESPONSIBILITIES:

8.1   Heads of entities are responsible for compliance with the requirements of this policy.

8.2   The State of Kansas Information Technology Security Council (ITSC) is responsible for the maintenance 7230A Information Technology Security Standards.

8.3   The Chief Information Technology Officer, Executive Branch is responsible for the maintenance of this policy.

9.0 CANCELLATION:

9.1   Rescinds: 7900 7900A 7400 7400A 7320 7320A

1-25

Kansas Information Technology Executive Council

1. **TITLE: INFORMATION TECHNOLOGY SECURITY STANDARDS 7230A**

   1.1. EFFECTIVE DATE: 11/5/2014

   1.2. TYPE OF ACTION: Update

   1.3. KEYWORDS: Kansas Information Technology Security Council, Enterprise Security Policy, Information Security, User Security, Personally Identifiable Information, Security Incident Response.

2. **PURPOSE:** To define the Information Technology Policy 7230 minimum security standards and procedures for state of Kansas information systems.

3. **ORGANIZATIONS AFFECTED:** All State of Kansas branches, boards, commissions, departments, divisions, agencies, and third parties used to process transmit or provide business capabilities on behalf of Kansas state government, hereafter referred to as Entity or Entities.

4. **REFERENCES:**

   4.1. K.S.A. 2013 Supp. 75-7203 authorizes the Kansas Information Technology Executive Council (ITEC) to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state entities.

   4.2. Kansas Information Technology Executive Council (ITEC), ITEC Policy 7300R1, Information Technology Security Council Charter.

   4.3. Kansas Information Technology Executive Council (ITEC), ITEC Policy 7230, Revision 1, General Information Technology Enterprise Security Policy.

   4.4. NIST Special Publication 800-53 Rev 2 – Recommended Security Controls for Federal Information Systems.

   4.5. NIST Special Publication 800-88 – Guidelines for Media Sanitization.

5. **DEFINITIONS:** The following definitions are applied throughout this policy and procedure memorandum.

   5.1. <u>Personal Financial Information (PFI):</u> Any non-public personally identifiable financial information that an entity collects about an individual in order to provide a financial product or service.

   5.2. <u>Personally Identifiable Information (PII):</u> Any information that can be used on its own or with other information to identify or locate a single person.

   5.3. <u>Sensitive Personally Identifiable Information (SPII):</u> Any non-public PII that 1) the data subject has not voluntarily disclosed, 2) is not subject to public release by an entity in accordance with statute or court order, or 3) an entity collected after notice to the data subject that the information is categorized for public release.

   5.4. <u>Individually Identifiable Health Information (IIHI):</u> Any information as defined in 45 CFR 160.103 – Code of Federal Regulations TITLE 45 – Public Welfare Part 160.103 Definitions.

   5.5. <u>Restricted-Use Information:</u> Includes but is not limited to SPII, IIHI or PFI as defined in this Standard.

   5.6. <u>Data Subject:</u> The individual person whose PII is contained in the record or Information Asset.

   5.7. <u>Voluntary Disclosure:</u> Information that a data subject provides without request or compulsion by state personnel, or that a data subject provides to the State with notice that it will be made publicly available.

   5.8. <u>Information System Component:</u> A discrete, identifiable information technology asset (i.e.,

1-26

----

hardware, software, firmware, or media (electronic and hardcopy)) that represents a building block of an information system. Information system components include commercial information technology products.

5.9.   Information System: A discrete set of information system components organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

5.10.   Critical System: Any information system that supports the core entity mission.

5.11.   Production Information System: Information Systems used to deliver essential services in the normal operating state of the entity.

5.12.   Source Record: The authoritative instance of a record within an entity

5.13.   Variance: A deviation from the control mandated in this document.

5.14.   Information Asset: A body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

5.15.   Security Assessment: An assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

5.16.   Vulnerability Scanning: Scans using specialized tools for the detection of vulnerabilities within the Information System.

6. **RISK MANAGEMENT STANDARD**

6.1.   Entities shall develop a hierarchal Information Asset classification standard that assigns appropriate controls to each Information Asset classification. The standard shall require the security controls specified in this document to be applied to Restricted-Use Information.

6.2.   Entities shall also set a default information classification for all information. If no default standard is created, all information shall be considered Restricted-Use Information.

6.3.   Entities shall ensure that Information Asset trustees are appointed for the following Information Assets:

- Intellectual property or
- Data compilations that contain or may be projected to contain Source Records on thirty (30) or more individuals of Restricted-Use Information.

6.4.   Information Asset trustees shall perform the following tasks for each information Asset:
- Determine the potential impact to the affected entity, individuals and the State in the event of a loss of confidentiality, integrity, and availability of the Information Asset.
- Classify the asset in accordance with the Entity's Information Asset classification standard.
- Ensure that the asset is handled in accordance with the Entity's Information Asset handling standard.
- Ensure that adverse events are reported to the Entity Information Security Officer (ISO).
- Appoint Information Asset custodians.
- Approve all access and use of the Information Asset.
- Recertify annually the classification, access, users and custodians of the Information Asset.
- Report classification of all Restricted-Use Information Assets to the Risk Management Committee.

1-27

6.5. Information Asset custodians shall perform the following responsibilities:

- Implement and operate the safeguards and controls for Information Assets as directed by Information Asset trustees.

6.6. Entities shall maintain a standing Risk Management Committee with the following responsibilities:

- Ensure that Restricted-Use Information Assets are identified.
- Review the classifications of Restricted-Use Information Assets by trustees.
- Ensure that risks are assessed.
- Process and approve variances from requirements in this document based upon risk and mitigating controls.
- Report approved variances in writing to the Enterprise Security Office (ESO), located within the Office of Information Technology Services (OITS), and the Entity Head.
- Direct the investigation, mitigation and acceptance of risks on behalf of the entity.

6.7. The Entity head shall appoint a Risk Management Committee that shall include participants from the following functions or roles if they exist within the entity:

- Legal
- Audit/Risk
- Line of Business Representative(s)
- Information Security Officer

7. ASSESSMENT AND SECURITY PLANNING STANDARD

RISK ASSESSMENT

7.1. Entities shall assess and document the risks to information systems that process, store or transmit Restricted-Use Information.

7.2. Entity risk assessments shall identify potential threats and characterize the likelihood and impact of the threat being realized.

7.3. Entities shall assess and document risks prior to placing an information system into service, whenever a significant change is made, and at least once every three (3) years thereafter.

SECURITY PLANNING

7.4. Entities shall document a security plan that specifies security controls based upon a risk assessment for information systems that process, store or transmit Restricted-Use Information.

7.5. The set of security controls in the security plan shall be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations and the state, based on the entity risk tolerance.

8. AWARENESS AND TRAINING STANDARD

SECURITY AWARENESS TRAINING

8.1. Entities shall provide and conduct security awareness training for all information system account holders.

8.2. Entities shall require all employees to complete security awareness training within ninety (90) days of hire and on an annual basis thereafter.

8.3. Entities shall retain a form of acknowledgement of training completion.

8.4. Entities shall review their security awareness training materials at least annually or more frequently as needed.

8.5. Awareness training shall address the following topics at a minimum:

1-28

- Passwords including creation, changing, aging and confidentiality
- Privacy and proper handling of sensitive information
- Physical security
- Social engineering
- Identity theft avoidance and action
- Email usage
- Internet usage
- Viruses and malware
- Software usage, copyrights and file sharing
- Portable devices
- Proper use of encryption devices
- Reporting of suspicious activity and abuse

9. ACCESS CONTROL

IDENTIFICATION AND AUTHENTICATION

9.1. User access to information systems that process, store or transmit Restricted-Use Information shall be authorized by an appropriate Entity official.

9.2. All users of information systems that process, store or transmit Restricted-Use Information shall be authenticated by a unique system identifier.

9.3. The unique system identifier will be associated with a unique information system authenticator (i.e. password, token, etc.).

9.4. Unique information system authenticators shall be delivered in a secure and confidential manner.

9.5. Passwords for system user accounts shall be constructed according to one (1) of the following two (2) methods.

  9.5..1. Passwords with complexity shall comply with the following requirements:

- A minimum of eight (8) characters in length
- Contain three (3) of four (4) of the following categories:
  o Uppercase
  o Lowercase
  o Numeral
  o Non-alpha numeric character
- Shall not contain the user id

  9.5..2. Passwords without complexity shall be a minimum of sixteen (16) characters in length.

9.6. Passwords shall not be changed more frequently than once every fifteen (15) days without system administrator intervention.

9.7. Passwords for system user accounts shall not have a lifespan that exceeds ninety (90) days.

9.8. Passwords shall be significantly different from the past ten (10) passwords.

9.9. Passwords shall not be viewable in clear text except by the account holder.

9.10. Passwords shall not be transmitted or electronically stored in clear text.

9.11. Passwords shall not be shared and shall be kept confidential.

9.12. Where physical tokens or authenticators are used:

- A defined process must be followed for token distribution.
- A defined process must be followed for token revocation.
- A defined process must be followed for the handling of lost, stolen or damaged tokens.

1-29

9.13. Where biometric data is used for authentication:

- A defined process must be followed for capturing user biometric data.
- A defined process must be followed for biometric revocation.
- A defined process must be followed for the handling of user biometric data.

ACCOUNT MANAGEMENT

9.14. All information system accounts shall provide the most restrictive set of privileges required. Separation of duties shall be enforced through account privileges; no single user shall have privileges to authorize, perform, review and audit a single transaction.

9.15. Information system accounts shall be restricted to a maximum of five (5) consecutive failed attempts before being locked out.

9.16. Accounts shall remain locked out for a minimum of thirty (30) minutes without administrator intervention.

SESSION MANAGEMENT

9.17. Information systems shall display a system use notification identifying system ownership, system usage restrictions, prohibition of unauthorized access, implied consent and associated penalties for unauthorized access. The user must acknowledge the system use notification before gaining access to the information system.

9.18. Entity authorization shall be required prior to deploying any remote access solution to information systems containing or processing Restricted-Use Information. Entities shall specify the acceptable methods of connection.

9.19. Remote sessions shall be encrypted, auditable and traverse managed access points.

9.20. Local console sessions on information systems that process, store or transmit Restricted-Use Information shall be locked after a period of thirty (30) minutes of inactivity.

9.21. Remote sessions to information systems that process, store or transmit Restricted-Use Information shall be terminated after a period of thirty (30) minutes of inactivity.

9.22. Authentication shall be required to unlock a console session or reestablish a remote session.

10. SYSTEMS CONFIGURATION STANDARD

CONFIGURATION MANAGEMENT

10.1. Entities shall build information systems that process, store or transmit Restricted-Use Information from a standard configuration baseline.

10.2. The standard configuration baseline shall include the specifications of the information system components and the security controls for each component.

10.3. Entities shall maintain an asset inventory of information systems components and update it as it changes and review it at least annually.

10.4. The asset inventory shall also identify and document the relationships between each of the information system components and the ownership of each component.

10.5. Collaborative infrastructure, such as video and teleconferencing, shall be configured to prohibit remote activation.

CHANGE CONTROL

10.6. Entities shall document and adhere to change control processes when making changes to production

systems.

10.7. Change control requests shall include proposed change description, justification, risk assessment, implementation plan, test plan, back-out plan, review and approval.

10.8. Entities shall maintain a change log for information systems containing Restricted-Use Information.

10.9. The change log shall include:

- Date and time of maintenance
- Name and organization of person performing change
- Name of escort, if required
- Description of maintenance performed
- List of affected information systems components or component elements

SYSTEMS PROTECTION

10.10. Entities shall implement boundary protection mechanisms with capability to monitor and control network communications.

10.11. Within the boundary, entities shall create security zones based on data and information system classification.

10.12. Entities shall employ malicious code protection mechanisms on systems that contain Restricted-Use Information.

10.13. Entities shall configure malicious code protection mechanisms to perform weekly scans of files on information systems.

10.14. Where malicious code protection mechanisms require regular signature or detection engine updates, entities shall employ a documented update mechanism that includes testing and installation of applicable updates.

11. DATA PROTECTION STANDARD

11.1. Entities shall employ mechanism(s) to ensure the confidentiality, availability and integrity of Restricted-Use Information.

11.2. Restricted-Use Information that has met the information retention schedule must be removed, destroyed or deleted in a verifiable manner.

11.3. Restricted-Use Information shall be protected from unauthorized disclosure.

11.4. Restricted-Use Information when transmitted electronically outside of a secure boundary shall be encrypted.

11.5. Media containing Restricted-Use Information shall be disposed of in accordance with NIST Special Publication 800-88 – Guidelines for Media Sanitization.

12. APPLICATION PROCESSING STANDARD

12.1. Entities shall define and document principles and procedures for secure application development.

12.2. The application element of all information systems components shall logically separate user functionality from administrative functionality such that the interface for the one cannot be used to operate the other.

13. SYSTEMS OPERATIONS STANDARD

ASSESSMENT OPERATIONS

13.1. Entities shall perform Security Assessments against all information systems that process, store or transmit Restricted-Use Information prior to installation on production environments and annually

/-3/

thereafter to ensure that security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements of the system.

13.2. Entities shall perform Vulnerability Scans against all information systems that process, store or transmit Restricted-Use Information prior to installation into production environments and biannually thereafter.

13.3. Entities shall document and implement a remediation plan for the security issues discovered in Security Assessments and Vulnerability Scanning, assign rankings and establish corrective actions that are reviewed quarterly.

13.4. Entities shall monitor for security alerts and advisories relative to the technologies that are operating within their environments.

13.5. Entities shall implement a documented patch management process that includes 13.4, testing and installation of applicable patches.

INTEGRITY OPERATIONS

13.6. Entities shall implement controls to ensure that configuration settings are within acceptable parameters.

13.7. Entities shall implement integrity monitoring on information systems that process, store or transmit Restricted-Use Information.

13.8. Entities shall document and investigate integrity discrepancies.

13.9. Entities shall validate, then circulate security alerts to appropriate personnel and ensure corrective action is taken.

MAINTENANCE OPERATIONS

13.10. Entities shall not operate information systems containing Restricted-Use Information without either redundant qualified in-house staff or by contract for vendor managed support.

13.11. Entities shall configure critical information systems to be fault tolerant.

13.12. Entities shall ensure that critical data is restorable to a known secure state of operations.

13.13. Entities shall test critical information system's restoration annually.

14. SYSTEM AUDIT

14.1. Information systems that process, store or transmit Restricted-Use Information shall be configured such that all user access interactions and system administrators' actions are logged to both internal and external log repositories.

14.2. The following data points shall be logged:

- Event date
- Event time
- Event source
- Event description

14.3. Information systems that process, store or transmit Restricted-Use Information shall be configured to raise alerts to administrative personnel in the event that logging space becomes limited, upon system logging failure or when inappropriate, unusual or suspicious activity is detected.

14.4. Information systems that store logging data shall be configured to continue logging by overwriting the oldest logs in the event available space is limited.

14.5. Information system logging data shall be manually reviewed according to a pre-defined period of

1-32

time or the logging system configured to automatically raise alerts to administrative personnel based on defined events.

14.6. All Production Information Systems shall be configured to have time synchronized with authoritative time sources.

15. INCIDENT RESPONSE STANDARD

15.1. Entities shall adopt a defined incident response plan which addresses the following stages:

15.1..1. Preparation

15.1..1..1. Entities shall appoint team members to incident response roles with the following skills:

- Communication and coordination
- Network analysis
- System administration
- Security analysis

15.1..1..2. Entities shall provide Incident Response (IR) training for all IR team members within ninety (90) days of initial assignment of the individual to the IR team.

15.1..1..3. Entities shall provide annual IR training for all IR team members.

15.1..1..4. Entities shall annually conduct IR operations testing using classroom, tabletop exercises or live incidents.

15.1..1..5. Entities shall conduct an exercise recreating a significant incident scenario that requires the full-scale execution of IR operations once every five (5) years.

15.1..2. Detection

15.1..2..1. Entities shall define what constitutes a security incident. The following shall be considered Reportable Security Incidents.

- Attempted or successful malicious destruction, corruption or disclosure of Restricted-Use Information or intellectual property.
- Compromised host or network device that processes, stores or transmits Restricted-Use Information.
- Compromised user account with access to Restricted-Use Information.
- Suspected criminal activity, such as theft, fraud, human safety or child pornography.
- Intentionally defeating a security control.

15.1..3. Analysis

15.1..3..1. Entities shall have dedicated tools and a process to conduct incident analysis, such as:

- Dedicated portable workstations
- Forensics analysis software and procedures
- Evidence collection tools and procedures

15.1..4. Containment

15.1..4..1. Entities shall have procedures to isolate and mitigate identified threats to prevent further impact.

15.1..5. Communication

15.1..5..1. Entities shall develop an incident communications plan to ensure adequate

----

communication of an incident, is provided, in a timely basis to stakeholders.

15.1..5..2. State of Kansas Enterprise Information Security Office shall be notified of Reportable Security Incidents.

15.1..6. Recovery

15.1..6..1. Entities shall recover affected systems and system components to a pre-compromised status and return to normal operations.

15.1..6..2. Entities shall maintain heightened monitoring of the affected system(s) for a period of time subsequent to an incident to ensure there are no lingering impacts.

15.1..7. Post-Incident Activity

15.1..7..1. Entities shall perform a post-incident review in order to document lessons learned and to improve information system protection in the future.

16. PHYSICAL SECURITY STANDARD

DATA CENTERS

16.1. Entities shall restrict physical access to data centers that process, store or transmit Restricted-Use Information to authorized personnel only.

16.2. Entities shall maintain a list of all authorized personnel with physical access to data centers that process, store or transmit Restricted-Use Information.

- This list shall be reviewed and updated annually.
- This list shall be updated as user access privileges change.

16.3. Entities shall require authorized personnel to authenticate themselves prior to entry to data centers that process, store or transmit Restricted-Use Information.

16.3..1. Visitors to data centers that process, store or transmit Restricted-Use Information shall be escorted by authorized personnel at all times.

16.3..2. Entities shall log all visitor access to data centers that process, store or transmit Restricted-Use Information.

16.4. Data centers shall implement physical environmental controls that mitigate or prevent damage from water, fire, temperature and humidity for information systems that process, store or transmit Restricted-Use Information.

16.5. Entities shall ensure sufficient power protection is available for critical information systems to perform an orderly shutdown.

MEDIA

16.6. Entities shall restrict physical access to media that store Restricted-Use Information to authorized personnel only.

16.7. Media that store Restricted-Use Information shall be stored securely within a controlled area and physical access to that controlled area shall be restricted to authorized personnel.

16.8. Entities shall ensure appropriate safeguards when media is transported by authorized personnel outside of a controlled area.

17. PERSONNEL SECURITY STANDARD

ACCEPTABLE USE

17.1. Acceptable use policies shall restrict the use of all equipment and access to public and private

1-34

networks to approved entity related operations.

17.2. Entities shall require employees and contractors to acknowledge adherence to the entity acceptable use policy prior to being granted access to information systems.

17.3. Entities shall include policy violation consequences in their acceptable use policies.

17.4. Entity acceptable use policies shall assert that violations will be investigated as a security event.

PERSONNEL OPERATIONS

17.5. Entities shall retain a form of acknowledgement of the acceptable use policy.

17.6. Entities shall assign all employees and contractors a user categorization.

17.7. Entities shall assign information system authorizations to users based on user categorization and information system classification.

17.8. Entities shall revoke system access or eliminate unnecessary permissions for accounts assigned to employees and contractors as they are transferred or terminated.

17.9. Entities shall assign review-only access for all accounts assigned to the terminated employee to that employee's immediate manager for a pre-defined period of time.

17.10. Entities shall recover all property that has been assigned to terminated personnel.

18. SECURE PURCHASING/ACQUISITION STANDARD

18.1. Entities shall include system security requirements to ensure that the system or solution proposed by proponents meet the security requirements of the entity with all Requests for Proposal, Information, Quotation (RFP, RFI, RFQ) or contracts.

18.2. All acquisition documents must specify the entity's security requirements and allow for the validation of those security requirements.

19. RESPONSIBILITIES:

19.1. The State of Kansas Information Technology Security Council (ITSC) is responsible for the maintenance of these standards.

19.2. These standards will be reviewed by the ITSC, at a minimum, every three (3) years.

19.3. Entities shall ensure demonstrable compliance with these standards no later than July 1, 2016.

1-35