DISASTER RECOVERY PLAN 4.1
rev. September 21, 2016

Personnel Cabinet – Office of Administrative Services
Division of Technology Services

DTS CIO/Director's Office
KSOB 501 High St
Frankfort, KY 40601

robbies.perkins@ky.gov
personnel.ky.gov

Table of Contents

ACRONYMS

ACH	Automated Clearing House
ADC	Alternate Data Center
BC	Business Continuity
BOBJ	Business Objects
BW	Business Warehouse
CDC	Commonwealth Data Center
COT	Commonwealth Office of Technology
CSD	Commonwealth Service Desk
DR	Disaster Recovery
DTS DO	Director's Office
DTS LT	Leadership Team
EBI	Enterprise Business Intelligence (SAP Business Objects hosted by COT)
eMARS	Electronic Management Administrative & Reporting System
ePAY	Electronic Payment (EFT solution hosted by KY Interactive, LLC)
F&AC	Finance & Administration Cabinet
KHRIS	Kentucky Human Resources Information System
OSBD	Office of State Budget Director

STATEMENT OF GOALS & OBJECTIVES

The primary objective of the Personnel Cabinet's Disaster Recovery and Business Continuity Plan (The Plan) is to protect the Personnel Cabinet and its customers; state employees, non-state employees paid via Personnel and health/life benefits only participants in the event that all or part of the Kentucky Human Resources Information System (KHRIS) and/or ancillary systems are rendered inaccessible at their primary site of operation, the Commonwealth Office for Technology's (COT) Commonwealth Data Center (CDC). Preparedness is the key to ensure a level of organizational stability and an orderly recovery after a disaster; thus, the purpose of The Plan.

The Personnel Cabinet, like most organizations, depends heavily on technology and automated systems. Disruption in business, even for a few days, could negatively impact the Cabinet's ability to pay employees, prevent external organization benefits bill payments, and/or create access to care issues for more than 250,000 public employees, retirees, and dependents. This risk is specific to the loss of all or part of KHRIS.

In the event of a disaster, the continued operation of the Personnel Cabinet's business and supporting systems depends on management's awareness of potential disasters. This awareness allows for the ability to develop and execute a plan which minimizes disruptions of critical functions and the capability to distribute pay, verify benefit plan information, invoice, and receive funds from benefit plan members and recover full system operations of KHRIS expediently and successfully in the event that The Plan is invoked.

The Plan is a comprehensive statement of consistent actions to be taken before, during, and after a disaster. The Plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster. The Plan is also an evolving plan with ongoing changes in both KHRIS and corresponding business requirements. Subsequent changes to The Plan, as administered through the DTS System Change Control Process (Personnel Cabinet Information Security Policy *030.101 Change Control*), will be updated in The Plan and logged in The Plan's Change Log, Section 8.0.

Objectives of The Plan are to:

1. Provide an alternate method to process state payroll and insurance billing
2. Provide an alternate method to verify access to care for benefit plan members
3. Provide a sense of security that a plan is in place to ensure continuity of business
4. Minimize decision making during a disaster
5. Minimize risk of delays in the event of a disaster
6. Guarantee the reliability of standby systems
7. Develop a plan for testing The Plan; insure The Plan is reviewed, tested and revised accordingly on an annual basis
8. Maintain an orderly process for system recovery and resumption of business
9. Ensure The Plan is properly communicated to Personnel Cabinet staff

PLAN ACTIVATION

Activation Criteria

The Personnel Cabinet will need to address the following questions to determine if part or all of The Plan should be enacted as it relates to COT hosted Personnel Cabinet systems:

1. Does an issue exist putting the Cabinet at risk of not being able to generate the state payroll, via KHRIS, within 6 (six) days after the stated pay date, as required by statute?

2. Is KHRIS unavailable to provide pertinent benefit member information for participants to verify access to care?

3. Is eMars (the Commonwealth's financial system) unavailable for an extended period of time, putting the state payroll at risk by not being able to complete the processing of payroll within 6 days after the stated pay date?**

4. Is the KY State Treasury unable to print payroll checks and/or submit ACH files for an extended time putting the state payroll at risk by not being able to complete payroll processing within 6 days after the stated pay date?**

5. Is there a loss of data requiring a partial or full restore of KHRIS data from backup?

6. Is the complete KHRIS environment unavailable due to a disaster at The Commonwealth Office of Technology's (COT) Commonwealth Data Center (CDC) warranting activation of COT's Alternate Data Center (ADC) in Florence, KY?

7. Is there a system loss of the Cabinet's SharePoint websites and/or incident reporting and change management requiring failover to the ADC in Florence, KY?

8. Is there a system loss of the Cabinet's Business Warehouse data mart preventing financial reconciliation of health/life insurance premiums, or inability to provide Access to Care (ATC) in the case of a KHRIS outage due to upgrade requiring failover to the ADC in Florence, KY?

9. Is there a system loss of the Cabinet's Business Objects reporting ability via the Enterprise Business Intelligence (EBI) portal preventing financial reconciliation of health/life insurance premiums, or inability to provide ATC in the case of a KHRIS outage due to upgrade requiring failover to the ADC in Florence, KY?

10. Is there a loss of the Cabinet's network file share drives data requiring restore?

11. Is there a system loss of the Cabinet's network file share drives requiring failover to the ADC in Florence, KY?

12. Is there a loss of the Cabinet's SQL database data requiring restore?

13. Is there a system loss of the Cabinet's SQL databases requiring failover to the ADC in Florence, KY?

**Note: KHRIS and ancillary systems are the first step of a three-part sequence required to fully process payroll and generate checks. The Finance & Administration Cabinet's eMars application is the second step. Generation of checks/vouchers and the ACH file by Treasury is the third step.

Considerations for Activation

What is the expected length of the outage?

- If the outage is expected to be of minimal duration, corrective response strategies at the CDC are in progress and deemed the appropriate course of action, a level of disruption is acceptable until resolved

- If the outage is expected to be of lengthy duration and corrective response strategies are not known/viable, then the DTS CIO/Director's Office and DR/Business Continuity Coordinators will consult with COT to determine the necessity of failover and recovery of COT hosted Personnel Cabinet systems at the ADC

The two agencies will communicate with their respective Cabinet Secretaries and stakeholders as practical and as necessary.

Activation Procedures

The DTS CIO/Director's Office and/or DR Coordinators will be made aware of an issue from internal staff, Personnel Cabinet leadership, KHRIS business owners, COT, Governor's Office, or other state agency staff.

- The issue(s) will be researched by the DTS CIO/Director's Office, DR/Business Continuity Coordinators, DTS Leadership Team, and affected business owners

- Research and recommendations for a response strategy for the identified issue will be assessed, and the DTS CIO/Director's Office will decide and document the course of action for the scenario through the DTS System Change Control Process and ultimately sign off on the change to activate any or all of The Plan.

- The DR/Business Continuity Coordinators will be responsible for execution and follow through with the DTS technical teams, as well as, the Personnel Cabinet business areas, COT, and other external staff, if required.

SCENARIO & RESPONSE STRATEGIES

This section will discuss scenarios covered in The Plan and the corresponding response strategy required for each.

KHRIS Scenario 1:

Is the state payroll at risk of not being able to complete the processing of payroll within 6 days of the stated pay date?

Response Strategy for Scenario 1:

- DTS and the Office of the State Budget Director (OSBD) will edit the previous payroll period's files incorporating new check numbers and pay dates. These files will then be passed to the eMars team for processing, followed by submission to Treasury to publish checks and produce the ACH file. All work will be documented and appropriate approvals attained throughout this process for audit purposes;
- Once KHRIS is available, the amount of pay will be tracked on a "loan" wage type to capture the pay processed "outside" of KHRIS;
- When a "loan" is captured and KHRIS is operable, KHRIS will adjust accordingly in the next payroll processing cycle. This will be handled by KHRIS issuing a retro for pay periods processed during the disaster event. The system will retro the captured loan and self-correct for the missed payroll(s) processed outside of KHRIS. The next payroll, when KHRIS is operable, will ensure accurate pay and allocations of the payrolls missed during the outage.

Testing of Response Strategy for Scenario 1:

- The 'July 1st payroll deferral' is ongoing and now considered a normal part of the production process that DTS supports. It provides an annual opportunity to test the response strategy outlined above in *Response Strategy Scenario 1.*
- The capturing of "claims', "loans" and/or "arrears" is a production feature of KHRIS and exists in most KHRIS payrolls. Additional special testing is not required other than as needed for any change through the Cabinet's Systems Change Control request process.
- Retro functionality is a production feature of KHRIS, and special testing is not required other than as needed for any change through Personnel Cabinet Information Security Policy *010.102 Change Control.*

KHRIS Scenario 2:

Is KHRIS unavailable to provide pertinent health and life insurance member information to verify access to care?

Response Strategy for Scenario 2:

The Department of Employee Insurance (DEI) needs to be able to access benefit plan information and participant coverage for its members via an alternate database if KHRIS becomes unavailable. The Benefits Access to Care Validation Disaster Recovery Database is utilized as a response to this scenario.

- DEI runs two Business Objects reports: Disaster Recovery – Boards and Disaster Recovery – Non-Boards. These disaster recovery extracts are broken into two separate extracts;
- There is also a separate query that captures current FSA enrollment located at the following share: \\pers502\Health\Confidential\Projects\BOBJ Reports\FSA\;
- This data is also imported and reformatted for use by DEI's Member Services Branch staff to access member information if KHRIS is unavailable to provide that information;

- These Business Objects queries are run on a weekly basis during off-hours, although data is not transported to MS Access except when needed. In this way, DEI ensures the most up to date information possible when KHRIS has scheduled or unscheduled outages. This ensures data is available if KHRIS and Business Objects both become unavailable/go down unexpectedly to maintain business continuity and ensure members have access to care.

Testing of Response Strategy for Scenario 2:
This process is used in production today when KHRIS is unavailable for limited times during planned maintenance and limited special maintenance windows. Special testing is not required other than as needed for any change through Personnel Cabinet Information Security Policy *030.101 Change Control.*

KHRIS Scenario 3:

Will the Finance and Administration Cabinet's eMars application be unavailable for six days or more following the stated pay date?

*Note: KHRIS is the first step of a three-part sequence required to fully process payroll and generate checks. eMARS is the second step. The third step is generation of checks/vouchers and the ACH file by Treasury.

Response Strategy for Scenario 3:
Refer to the Finance and Administration Cabinet's Disaster & Recovery Plan for eMars.

Testing of Response Strategy for Scenario 3:
Refer to the testing plan for the Finance and Administration Cabinet's Disaster & Recovery and Business Continuity Plan for eMars.

KHRIS Scenario 4:

Is the KY State Treasury unable to print payroll checks and/or submit ACH files for six days or longer after stated pay date, as required?

*Note: KHRIS is the first step of a three-part sequence required to fully process payroll and generate checks. eMars is the second step. The third step is generation of checks/ vouchers and the ACH file by Treasury.

Response Strategy for Scenario 4:
Refer to the Department of Treasury's Disaster & Recovery and Business Continuity Plan for Treasury.

Testing of Response Strategy for Scenario 4:
Refer to the testing plan for the Department of Treasury's Disaster & Recovery and Business Continuity Plan for Treasury.

KHRIS Scenario 5:

Is there a loss of data requiring a partial or full restoration of KHRIS data from backup files?

Response Strategy for Scenario 5:
Loss of data will be restored via the last backup available or the specific backup needed for the restoration.

Testing of Response Strategy for Scenario 5:

This process is used in production today, as system restores/refreshes are a part of routine production support. Special testing is not required other than as needed for any change through Personnel Cabinet Information Security Policy *030.101 Change Control.*

KHRIS Scenario 6:

Is KHRIS and associated systems unavailable due to a disaster at COT's CDC requiring a move to the ADC in Florence, KY?

Response Strategy for Scenario 6:
COT's Disaster Recovery Tasks/Responsibilities as Personnel's Hosting Partner are as follows:
Provide full disaster recovery services are not available at this time and are pending full implementation and testing at COT's ADC in Florence, KY with no definite ETA at this time for full and failover.

The COT UNIX, Windows VM and Storage Teams are obligated to provide restoration services for all AIX managed systems and storage, including server and open systems storage for designated KHRIS data. This includes recovering AIX O/S infrastructure and the TSM storage infrastructure.

Testing of Response Strategy for Scenario 6:
This process is used in production today, as system restores/refreshes are a part of routine production support. Special testing is not required other than as needed for any change through Personnel Cabinet Information Security Policy *030.101 Change Control.*

SharePoint / Team Foundation Server Scenario 7:

Is there a system loss of the Cabinet's SharePoint websites and/or incident reporting and change management requiring failover to the ADC in Florence, KY?

Response Strategy for Scenario 7:
Stand up Windows VM servers for SharePoint/Team Foundation Server and database at ADC in Florence. Restore from last good Microsoft Data Protection Manager (DPM) backup.

Testing of Response Strategy for Scenario 7:
COT Windows VM Server Support stands up server SharePoint/Team Foundation Server and database at ADC in Florence. COT Enterprise Storage Team restores systems from last good DPM backup and database to last good system level backup. DTS Technical team validates system operability and connections. DTS Functional team validates data and business processes in system.

Business Warehouse Scenario 8:

Is there a system loss of the Cabinet's Business Warehouse data mart preventing financial reconciliation of health/life insurance premiums, or inability to prove Access to Care (ATC) in the case of a KHRIS outage due to upgrade requiring failover to the ADC in Florence, KY?

Response Strategy for Scenario 8:
Stand up Windows VM server for network file share drive(s) at ADC in Florence. Restore from last good snap-backup.

Testing of Response Strategy for Scenario 8:
COT Windows VM Server Support stands up server for Business Warehouse at ADC. COT Enterprise Storage Team restores database to last good system level backup. DTS Technical team validates system operability and connections. DTS Functional team validates data and business processes in system.

Enterprise Business Intelligence Scenario 9:

Is there a system loss of the Cabinet's Business Objects reporting ability via the Enterprise Business Intelligence (EBI) portal preventing financial reconciliation of health/life insurance premiums, or inability to prove Access to Care (ATC) in the case of a KHRIS outage due to upgrade requiring failover to the ADC in Florence, KY?

Response Strategy for Scenario 9:
Refer to the Commonwealth Office for Technology's Disaster & Recovery and Business Continuity Plan for Enterprise Business Intelligence.

Testing of Response Strategy for Scenario 9:
Refer to the testing plan for the Commonwealth Office for Technology's Disaster & Recovery and Business Continuity Plan for Enterprise Business Intelligence.

Network File Share Drives Scenario 10:

Is there a loss of the Cabinet's network file share drives data requiring restore?

Response Strategy for Scenario 10:
Restore file(s) from last known good backup.

Testing of Response Strategy for Scenario 10:
Identify file(s) for test and clone to a separate test location. Clone file(s) and rename. Delete file(s). Contact COT's Commonwealth Service Desk requesting ticket be created to restore file(s). After ticket has been communicated from COT Enterprise Storage Team as having been processed and file(s) restored, compare restored file(s) to cloned renamed file to validate proper restore.

Network File Share Drives Scenario 11:

Is there a system loss of the Cabinet's network file share drives requiring failover to the ADC in Florence, KY?

Response Strategy for Scenario 11:
Stand up Windows VM server for network file share drive(s) at ADC in Florence. Restore from last good backup.

Testing of Response Strategy for Scenario 11:
COT Windows VM Server Support stands server for network file share drive(s) at ADC in Florence. Patching and GPO is updated and validated. COT Enterprise Storage Team restores database to last good backup. DTS Technical team validates share structure data files and file enumeration security.

SQL Databases Scenario 12:

Is there a loss of the Cabinet's SQL database data requiring restore?

Response Strategy for Scenario 12:
Restore database(s) from last known good backup.

Testing of Response Strategy for Scenario 12:
Identify database(s) for test and clone to a separate test location. Clone database(s) and rename. Delete database(s). Contact COT's Commonwealth Service Desk requesting ticket be created to restore

database(s). After ticket has been communicated from COT Enterprise Storage Team as having been processed and database(s) restored, compare restored database(s) to cloned renamed file to validate proper restore.

SQL Databases Scenario 13

Is there a system loss of the Cabinet's SQL databases requiring failover to the ADC in Florence, KY?

Response Strategy for Scenario 12:
Stand up Windows VM server for SQL Databases(s) at ADC in Florence. Restore from last good backup.

Testing of Response Strategy for Scenario 12:
COT Windows VM Server Support stands server for SQL databases(s) at ADC in Florence. Patching and GPO is updated and validated. COT Enterprise Storage Team restores database to last good backup.

BACKUP RESPONSIBLITIES & SCHEDULES

Per Executive Order 2012-880, COT assumed the following tasks/responsibilities as the Personnel Cabinet's hosting Partner will:

- Provide full backup and recovery services for identified application and data, currently consisting of IBM disk/tape hardware, TSM, DPM software tools.
- Upon request, will use Rocket Software's DB2 Cloning Tool to copy all data and system settings from one DB2 subsystem to another.
- Will back up daily non-production DB2 subsystems to local virtual tape resources.
- Will back up daily production DB2 subsystems to both virtual tape for transport to the ADC.
- Will back up hourly, daily and weekly Windows VM system-level snapshots to transfer to the ADC.
- Back-up <event schedule not supplied, refer to COT Storage Team> for Microsoft Data Protection Manager (DPM) for SharePoint 2013 for transfer to the ADC.

Backup schedules for identified DR systems are noted in the table below.

Server	System	Backup
Perregim2	FileNet	02:00
PersISRA1	FileNet-KHRIS Connector	**
Pers110	WS_FTP	**
Pers244	Business Warehouse Database	**
Pers243	Business Warehouse Application	**
Pers502	Confidential Data Share	**
Pers522	Personnel Home Drives Share	**
Pers560	SharePoint Database	22:00
Pers566	SharePoint 2013 Web Application	22:00
Pers567	SharePoint 2013 Web Application	22:00
Pers570	Big SQL	**
Persnt6	Small SQL Databases	**
Persnt25	File Shares	**
Persnt40	FileNet Print	**
Perstfs	Team Foundation Server	**
Khrisecpcs/khrisecpc1 khrisecpc2/khrisecpc3 Khriseppcs/khriseppc1/khriseppc2/khriseppc3	KHRIS Production	02:00
Khrisslmcs	KHRIS Production Solution Manager	03:00
khriscppci	Redwood Production	01:05
khrisbspcs	BSI Tax Factory Production	01:15
** COT Snapshot schedule for Windows VMs is 8 hourly, 7 daily and 5 weekly. Hourly snapshots are on the hour. Daily snapshots are 12am. Weekly snapshots are 12am Sunday.		

PLAN SCOPE/TESTING OF RESPONSE STRATEGY

The scope is to restore/recover the following servers/systems:

Server	System	Backup
Perregim2	FileNet	02:00
PersISRA1	FileNet-KHRIS Connector	**
Pers110	WS_FTP	**
Pers244	Business Warehouse Database	**
Pers243	Business Warehouse Application	**
Pers502	Confidential Data Share	**
Pers522	Personnel Home Drives Share	**
Pers560	SharePoint Database	22:00
Pers566	SharePoint 2013 Web Application	22:00
Pers567	SharePoint 2013 Web Application	22:00
Pers570	Big SQL	**
Persnt6	Small SQL Databases	**
Persnt25	File Shares	**
Persnt40	FileNet Print	**
Perstfs	Team Foundation Server	**
Khrisecpcs/khrisecpc1 khrisecpc2/khrisecpc3 Khriseppcs/khriseppc1/khriseppc2/khriseppc3	KHRIS Production	02:00
Khrisslmcs	KHRIS Production Solution Manager	03:00
khriscppci	Redwood Production	01:05
khrisbspcs	BSI Tax Factory Production	01:15
** COT Snapshot schedule for Windows VMs is 8 hourly, 7 daily and 5 weekly. Hourly snapshots are on the hour. Daily snapshots are 12am. Weekly snapshots are 12am Sunday. ◊◊ At the time of revision COT has not provided the schedule for the Microsoft Data Protection Manager (DPM) backup solution for SharePoint 2013 systems.		

Restores

- The COT Enterprise Storage Team backs-up and sends the identified systems to the ADC.
- The COT z/OS Server Support Team restores the z/OS mainframe and DB2 database from backup virtual tape.
- The COT UNIX Server Support Team establishes the base operational system environment and network connectivity between the AIX and z/OS mainframe.

Recoveries

- DTS/KHRIS Basis and COT/UNIX teams recover all required SAP application file systems for each application server
- DTS Basis Team and COT/Network teams establish connectivity between database and application servers
- DTS Basis Team starts SAP in ECP cs/app servers and applies licensing; then starts SAP in EPP cs/app servers and applies licensing; and then starts SAP in SLM cs.

- DTS Basis Team restores and recovers the BSI tax UNIX/LUW DB2 database from TSM and applies licensing
- DTS Basis Team starts the BSI application and tests connectivity to ECP
- DTS Basis Team restores and recovers the CPP Redwood UNIX/LUW DB2 database from TSM and applies licensing
- DTS Basis Team starts the Redwood application and tests connectivity to ECP
- The DTS DR Team and COT AIX teams recover all required application file systems for the application server for FileNet
- The DTS DR Team and COT/Windows VM teams recover all required application file systems for the application servers for:
    - FileNet-KHRIS ISRA Connector
    - WS_FTP
    - Business Warehouse Application
    - Confidential Data Share
    - Personnel Home Drives Share
    - SharePoint 2013 Web Application
    - SharePoint 2013 Web Application
    - File Shares
    - FileNet Print
    - Team Foundation Server
- DTS Technical staff and COT Storage Team will recover all required application file systems for the application servers supporting:
    - Big SQL
    - Small SQL Databases
    - Business Warehouse Database
    - SharePoint Database

Testing Technical

Once systems have been stood-up, the DTS Basis Team and Technical staff will:

- Validate system logs for any network, DB or application issues/dumps
- Validate RFC connectivity between systems in SM59
- Validate database functions by running catalog queries, usage queries and utility configurations in DB2 transaction
- Validate ADS functionality with Portal connection with FP_TEST program
- Validate BSI tax functionality from ECP
- Validate Redwood scheduling functionality from ECP
- Validate System Landscape Directory and Solution Manager interface between ECP/EPP and SLM
- Validate Business Warehouse running and RFCs to ECP
- Validate FileNet running and connection to FileNet-KHRIS ISRA Connector
- Validate FileNet-KHRIS/ISRA Connector running and RFCs to Image Connect
- Validate WS_FTP is running and connections to ECP
- Validate SharePoint Web Application is running and connections to Team Foundation Server and database
- Validate Team Foundation Server running and connections to SharePoint Application and database
- Validate File Shares are running

Testing Functional

Once DTS Basis Team and Technical staff have validated system checks they will handoff to DTS Functional staff for business process functional testing. Functional staff will:

- Confirm production client running by logging into SAP backend client, ECP400, using the disaster recovery user, DISRECOV
- Confirm BSI (BSP) production client running and communicating with ECP400 by Executing payroll for a single SM (semi-monthly) Payroll Area employee
- Confirming payroll results
- Posting payroll results
- Generating outbound files for eMARS and eMARS Reporting
- Generating outbound reports for SSCRB and BDVA
- Confirm production portal EPP, https://khris.ky.gov/irj/portal/, running
- In EPP log in as user DISRECOV
- Confirm HR Generalist running by starting Misc. PA action
- Confirm Worklist running and OM/PA action will render
- Confirm ADP server running by rendering Remuneration Statement for SM employee
- Confirm Non-Commonwealth Insurance Coordinator I & II running
- Confirm Biller Direct running and bill will render
- Confirm connection to KY Interactive's ePay
- Log in as EPP user DISRECOV and pay single line item payment for an insurance product, return positive confirmation code
- Confirm Redwood by initiating job ZPAI005_PRSNL_MASTER_EXTRACT, variant APA
- Confirm WS_FTP by confirm scripting moves file from AL11\KHRIS\INTF\APA to pers110\outbound\APA
- Confirm FileNet, ISRA Connector & FileNet Print by logging into the KHRIS portal using HRG test user, launch documents via Image Connect and by printing multiples to local printer
- Confirm File Shares by, as a Personnel user access, files on Pers502- Confidential Data Share, Pers522- Personnel Home Drives Share & Persnt25- File Shares
- Confirm SharePoint websites and Team Foundation Server:
- As a Personnel user, access the following pages:
    - https://extranet.personnel.ky.gov/Pages/default.aspx
    - https://personnel.ky.gov/Pages/default.aspx
    - https://hr.personnel.ky.gov/Pages/default.aspx
    - https://careers.ky.gov/Pages/default.aspx
    - https://livingwell.ky.gov/Pages/default.aspx
    - https://gsc.personnel.ky.gov/Pages/default.aspx
    - http://perstfs:9000/tfs/PersonnelCollection/Personnel%20Cabinet%20Support
        - Submit ticket via RMS webform
    - http://perstfs:9000/tfs/FROI/FROI
        - Submit ticket via First Report of Injury

COMMUNICATION PROCEDURES

Approval, maintenance, and testing of The Plan are critical for knowledge, acceptance and successful execution of The Plan. The DR/Business Continuity Coordinators will administer The Plan under the direction and review of the DTS Director's Office.

- When any or all of the identified systems are unavailable, the DTS CIO/Director's Office will communicate with Personnel Cabinet Executive Staff notifying them of the service interruption or outage and may communicate with the Division of Employee Management as well as the Department of Employee Insurance to, if possible, communicate to key staff in external agencies (e.g. HR Executives/Administrators and/or Insurance Coordinators/Billing Contacts)
- When DTS activates this plan or a portion of it, the DTS CIO/Director's Office will notify Personnel Cabinet Executive Staff with details of the issue, the response strategy, the timeline, and will provide additional periodic updates until full system functionality is restored
- The DTS CIO/Director's Office, DR/Business Continuity Coordinators and Business Owners will determine the need and method for further communication based upon the specific situation encountered

PLAN ADMINSTRATION

Approval, maintenance, and testing of The Plan are critical for knowledge, buy-in, and successful execution of The Plan. The DR Coordinators will administer the DR Plan under the direction and review of the DTS CIO/Director's Office.

Approval Procedures

Approvals and changes to The Plan are through the Personnel Cabinet Change Control Committee (CCC). The review process involves the following:

- Director's Office, Division of Technology Services
- Integration Managers (DR/Business Continuity Coordinators), Division of Technology Services
- Leadership Team, Division of Technology Services
- Secretary's Office, Personnel Cabinet
- Executive Director, Office of Administrative Services
- Commissioner, Department of Human Resources Administration
- Assistant Director, Division of Employee Management
- Commissioner, Department of Employee Insurance
- Deputy Commissioner, Department of Employee Insurance
- Director, Department of Employee Insurance, Division of Financial and Data Services
- Internal Audit, Office of Administrative Services

Distribution Procedures

The Plan will be stored with The Business Continuity Plan and its associated documentation. The Business Continuity Plan and this Disaster and Recovery Plan will be communicated to the DTS Leadership Team along with the following:

- Personnel Cabinet Secretary
- Executive Director, Office of Administrative Services
- Commissioner, Department of Human Resources Administration
- Director, Division of Employee Management
- Commissioner, Department of Employee Insurance
- Deputy Commissioner, Department of Employee Insurance
- Director, Department of Employee Insurance, Division of Financial and Data Services
- Internal Audit, Office of Administrative Services
- IT Audit Team, KY Auditor of Public Accounts

Maintenance Procedures

The Plan will be reviewed/updated annually. Changes identified outside of the annual review will be requested and approved via the DTS Change Control process as:

- Stand-alone request for change to The Plan; or
- Addendum to another request brought before the Cabinet's Change Control Committee whose solution will impact systems identified for DR or would make the system considered 'productive' and necessitate addition of that system to The Plan.

Change Log

This section should be used to identify all related documents and information needed to support The Plan and all related implementation procedures.

Description	Date	Version	CR	Contact Information
Initial Version	05/01/12	1.0	29109	Robbie S Perkins
Revised	06/08/12	1.1	29109	Robbie S Perkins
Revised	06/11/12	1.2	29109	Neil M Popplewell
Revised	06/12/12	1.3	29109	Jill P Anderson Robbie S Perkins Neil M Popplewell
Review	02/16/13	1.3	No Change	Robbie S Perkins
Review	09/15/13	1.3	No Change	Robbie S Perkins
Revised	02/19/14	2.0	13434	Robbie S Perkins
Revised	06/04/15	3.0	30944	Neil M Popplewell
Revised	05/04/16	4.0	44634	Neil M Popplewell
Revised	09/21/16	4.1	44634	Robbie S Perkins