Information Technology

OIC Incident Management

Escalation Guidelines

December 2016

Version 4.0

TABLE OF CONTENTS

Document Maintenance Schedule & Revision History

1. Annually review and update this document, including all procedures, and checklists. In addition update this plan for any of the following circumstances:
   1.1. Changes to management personnel identified in the document;
   1.2. Significant changes to activities related the OIC management of an incident.

2. Review Process:
   2.1. Request feedback on suggested improvements from:
      2.1.1. OIC Supervisors, IC Managers, Tech Team Managers and Service Desk Managers
   2.2. Make revisions and publish revised Guidelines

The following table contains the change history of this document:

Change	Version	Comments	Author(s)	Revision Date
0	1.0.0	Initial Document Release	Cindy, Collins, Alan Sowell, and Paul Urban	7/20/2010
1	1.1.0	2011 Review of current process, update current practice.	Frank Barker, Paul Swedeen, Alan Sowell, and Paul Urban	4/18/2011
2	1.2.0	2012 Review and update	David Barringer, Frank Benavides, David Henry, Janice Larsen, David Palmer, Paul Urban	5/1/2012
3	3.0	2013 Review and Update	David Knippelmier Michael Nevins David Henry Hubert Jarmon Janice Larsen Paul Urban	10/14/2013
4	4.0	2015 Review and Update	Janice Larsen	6/17/2015
5	4.0	Review and Update	Janice Larsen	12/19/2016

1. Introduction

The purpose of the IT Incident Management Guidelines (ITIMG) is to provide guidance and standardization for alert categorization and escalation procedures.

2. Incident Management Criteria

All incidents will have a classification of Yellow, Orange, or Red for the duration of the incident. (See chart to determine current alert level) During the life of an incident, its alert level may change depending on the incidents current impact to customers and/or business operations. All Yellow, Orange, and Red Alert issues are candidates for Incident Management. All incidents will be documented using the available Incident Management software by entering an Incident Ticket. All Orange and Red Alerts will be accompanied by an email notification to the appropriate distribution group in conjunction with phone/bridge information as needed. Yellow alert notifications are made at the discretion of the OIC Supervisor.

It is the responsibility of the team taking the initial call to make sure that both the Service Desk and OIC are notified of any Yellow, Orange, or Red Alert.

During this interim period, all issues identified above must be reported to one of the following:

Name	**Title**
Janice Larsen	Manager of Operations Support Services
Mark Tabak	Manager of Platform Services
Vicky Macha	Manager of Field Services
Daren Gutschow	Manager of Telephony Services
Richard Dodson	Manager of Network Security Services
Kim Lee	Manager of Workstation Services

* Underscore indicates Notification changes from a lower condition alert.

Alert Stages	Definition	Notification
Condition RED – Bridge	Mission critical system down, Tier 1 app, COMM site down, Major DL site down, outage impacting external customers, outage preventing commissioned officers from performing their duties. **All managers and appropriate staff should join the bridge.**	OIC, Assistant Director IT*, Deputy Assistant Directors IT, IT Managers, Service Desk, Server Team, Network Team, Application Team and/or Vendors as appropriate. --Use OIC Outage Notification Spreadsheet for Distro list
Condition RED – NO Bridge	Mission critical system down, Tier 1 app, COMM site down, Major DL site down, outage impacting external customers, outage preventing commissioned officers from performing their duties.	OIC, Assistant Director IT*, Deputy Assistant Directors IT, IT Managers, Service Desk, Server Team, Network Team, Application Team and/or Vendors as appropriate. --Use OIC Outage Notification Spreadsheet for Distro list
Condition Orange	Mission critical system with issues (not down), DL site not down with moderate external customer impact, system outage impacting specific departments, i.e. an accounting system or an HR system, system outage with impact to commissioned officers but not preventing officers from performing their duties	OIC, Deputy Assistant Directors IT*, IT Managers, Service Desk, Server Team, Network Team, Application Team and/or Vendors as appropriate. --Use OIC Outage Notification Spreadsheet for Distro list
Condition Yellow	Non mission critical systems, specific areas having problems but no outage, connectivity that is down but not currently in production	OIC, IT Managers, Service Desk* --Use OIC Outage Notification Spreadsheet for Distro list
Condition Green	Previously reported problem has been resolved/cleared	Sent to all group(s) **notified** of the incident. --Use OIC Outage Notification Spreadsheet for Distro list

NOTE: In cases requiring an intentional shutdown/startup of a system or application used by or affecting the Data Center (DC) operations or Customer Service operations, make applicable notifications 30 minutes in advance of the shutdown. Note these conditions may be handled differently if this is an offsite incident. The above Guidelines are implemented as deemed appropriate by the OIC Supervisor.

- Technical Team members are to respond to a notification within 15 minutes. If there is no response from the on-call staff, escalate to the next level in the chain of command for the Technical Team member.

A. Support Escalation Procedures

Escalation of the Support Level does not automatically escalate the Alert Level. Throughout the Support Escalation process the consideration should be given to escalating the Alert Level, as outlined in the **Alert Stages and Notifications** section.

Level One: Service Desk and OIC Process for Possible Outage Reported

1. HEAT Template (Quick Ticket): Outages
2. Customer: Enter in customer name/ACID. If unknown, put: oic
3. Site/Circuit: Enter site name, mnemonic, circuit
4. Summary: Describe the basic outage in the Summary Line. Example:
    a. Outage – DL604 Austin loss of connectivity
    b. Outage – DLS not responding
5. Description: Fill in all needed details
    a. Reason for call?
    b. Point of contact (direct phone number)?
    c. Alternate contact (cell number)?
    d. Number of people impacted?
    e. Is a work around in place or is business suspended?
    f. Circuit ID #
    g. AT&T Ticket#:
    h. List other pertinent information in the description box – including any direct error messages
6. Service: Outage
7. Category: Select appropriate
    a. APPS – DL
        - These are all apps used to support Driver License
        - AAMVA, ADLTS, Appointment Plus, DLS, Nemo-Q, OTC, Qless, Texas.Gov, TOK
    b. APPS – General
        - These are all apps used by all of DPS

  - Amber, EIS/ETA, Exchange, Finance, Finesse, HEAT, HR, Intranet, Orion, Other, Planview, Sharepoint, SPURS, USAS, VPN

c. APPS – LE (CID, ICT, Ranger, THP)

  - These are apps used by the actual law enforcement employees
  - Borderstar, CLERIS, CRIS, DMV, Drawbridge, InCar, Mobile CAD, NetMotion, Streets & Trips, TxMap

d. APPS – LES (Law Enforcement Support)

  - These are apps for all things that SUPPORT Law Enforcement
  - AFIS, CCH, LIMS, NCIC, NLETS, OMNIXX, TCIC, TLETS

e. APPS – RSD

  - These are all apps used to support Regulatory Services
  - CAP, CLIPS, LTC, PAT, RSA, Texas.Gov, VIC

f. Infrastructure

  - These are anything to do with power, circuits, internet, data, hardware (Basically, anything not applications)
  - ASA 5505, ASA 5555, Cisco Firewall, Data Center, F5, Infoblox, MPLS (WAN) Circuit, Phone Circuit, Proxy, Router, Secure Auth, Server, Switch, UPS, VPN Tunnel, VSAT, WAP

8. Subcategory: Select appropriate
9. Impact – Select appropriate

a. No Impact (Site that is not open, no user impacted, auto-workaround (example: UPS failed, but was able to plug directly to wall, VSAT down but VADB auto-connected)

b. High – Tier 1 apps, major site, many users impacted, safety or security issues

  - AAMVA, AFIS, CCH-internal, DLS, Drawbridge, FusionCore, InCar, LIMS, Omnixx Console and Force, RSA, TCIC, TLETS, TxMap

c. Medium – 2-4 Tier app or minor site, moderate number of users impacted

  - Bluezone, CAD, CCH-external, CHL, CJIS, Email/Outlook/Exchange, HOD, LTC, METALS, NCIC, PAT, SharePoint, Texas.Gov,

d. Low – Applications not required for production, minimal users impacted

  - ETA, SQL Server, TokOpen, Intranet, MSA, Web Venice, Test Software

e. ***SLAs are triggered off of this coding

10. Urgency (How fast the system needs to be up)

a. High – Work that cannot be completed and is highly time sensitive. Must resolve NOW.

b. Medium – Work does not directly impact immediate production, but could cause impact if not resolved within a limited time. Should resolve as soon as possible.

c. Low – Work that cannot be completed but is not time sensitive.

11. Source: Defaults to phone, but could also be Network Monitor or other listed area
12. Division: Select appropriate

a. Administration

   b. Criminal Investigations
   c. Director’s Staff
   d. Driver’s License
   e. Education, Training, and Research
   f. Emergency Management (this includes SOC)
   g. Finance
   h. Highway Patrol
   i. Information Technology
   j. Intelligence\Counter Terrorism
   k. Law Enforcement Support
   l. Multiple (Example: THP and DL office)
   m. Outside Entities
   n. Rangers
   o. Regulatory
13. Area Impacted: Select appropriate
    a. Headquarters
    b. Multiple Sites
    c. Regional
    d. Single Site
    e. Statewide
14. Exact Time of Outage Start: – Select DD/HH/MM of the start of the outage or the start of the reported outage.
    a. If a site goes down in Orion and stays down – it will be the time of down
    b. If an external site calls to say their site has been down for three days, it is the time first reported if no other monitors are available
15. Team: Should be assigned to OIC. OIC will change team if further escalation is needed
16. SAVE
17. OIC is contacted via phone to continue Incident Management of Outage
    a. Ticket information is provided to OIC
18. Front End Started - if necessary

Level Two: OIC Handling of Reported Outage / Supervisor Duties

1. Validate Potential Outage:
   a. Check current changes or other known issues
   b. Validate weather / Power
   c. Validate if impact is not a single user issue
   d. If NOT an outage – change the Service to appropriate service (not Outage) and proceed with normal escalation
   e. If indeed this is a validated outage, ensure Service = Outage and proceed to next step
2. Condition: Select appropriate

a. Red – Mission Critical – Priority 1
b. Yellow – Non Critical or Work around or temporary fix – Priority 2-5
c. Green – Outage has been resolved
d. Blue – Unmanaged

3. Exact Time of Outage Start – validate and correct as needed
4. Send out email notification of Outage
   a. Determine if additional support is necessary to resolve the issue and include needed escalation points on email notification.
      - Include specific resolvers or teams in the bcc of the email
   b. Distribution Group
      - Select appropriate group from Outage Notification Roster
      - Put distribution group in the bcc: of the email
   c. Subject Line: Include Condition - <<App or Site>> <<Brief Description>>
      - Condition Red – No Bridge
      - Condition Red – Bridge
      - Condition Yellow
      - Condition Green
      - Example: Condition Red: No Bridge – TxDMV/Vehicle registration down
   d. Body of Notification Email – Include all details of the outage including the HEAT Ticket number, escalation point, ETA, and any other pertinent information
   e. Signature Line:
      - Include: (OIC-<< initials of who sent email>> <<line number of distribution group>>
      - Example:

        Operations Information Center
        Information Technology
        Texas Department of Public Safety
        512-424-2139
        (OIC-jwl-86)

5. If issue is resolved:
   a. Support identifies a probable resolution
   b. Immediately change the condition from Red to Yellow
   c. Put in a Time Stamp for Exact Time of Service Restored (DD/HH/MM)
   d. Change Impact from High to Med or Low
   e. Send out a Condition Yellow email notification
   f. Continue to validate and verify that resolution
   g. If issue is resolved – proceed with steps below to Close Outage Ticket
6. If issue is not resolved and must be escalated – proceed to Level Three Support

Level Three Support: Escalation / Support / Emergency Change

1. If a Bridge is required, ensure that all needed dial-in information is included in the notification email.
2. Open Bridge by following the OIC Conference Bridge process
3. Contact directly any relevant staff, vendors, etc. to either escalate or join bridge call. Engage vendors as needed. Engage Change Management as needed.
4. Implement crisis management escalation procedures as outlined above
5. If OIC does not get a return call within 15 minutes for OnCall – escalate to next level up to and including manager, DAD and/or CIO.
6. If Emergency Change is required, the changes are to be done in accordance with the Change Management Procedures
7. All support teams and personnel remain involved until a successful resolution is established and there is verification that the resolution meets the client's expectations.
8. If issue is resolved:
    a. Support identifies a probable resolution
    b. Immediately change the condition from Red to Yellow
    c. Put in a Time Stamp for Exact Time of Service Restored (DD/HH/MM)
    d. Continue to validate and verify that resolution
    e. If issue is resolved – proceed with steps below to Close Outage Ticket
9. If Level Three Support cannot resolve the issue, escalate the issue to Level Four. This step to be initiated as soon as determined that there is vendor impact.

<u>Level Four Support: Vendor Support</u>

OIC or IT Resolver performs the following steps:

1. Coordinate with Management to acquire additional support, based on the criticality of the service or application. Additional support could include resources that are external to the Agency. (i.e. contract for services, other State Agencies).
2. Engage the vendor for support.
3. When the issue is resolved – proceed to Close Outage Ticket

<u>Close Outage Ticket</u>

1. If an emergency change is required, changes must be done in accordance with the Change Management Process
2. Send out Condition Green email notification to same distribution group used for Condition Red and Yellow.
3. Complete HEAT Ticket:
    a. Summary Line is complete
    b. Status: Resolved
    c. Exact Time of Service Restore DD/HH/MM (first instance at which the resolution established, even before actual verification)
    d. Resolution: Enter all resolution notes and include resolver findings and input

e. Outage Root Cause: Select appropriate

- 3rd Party (all non-DPS fixes)
- Change
- Configuration
- Database
- Hardware Failure – DPS Fix
- Power
- Proxy/Firewall
- Software Failure – DPS Fix
- Weather
- Unknown – must enter detailed notes in Resolution if this Root Cause is selected

4. Save Ticket

3. Incident Team Tasks and Responsibilities

Once an incident has been documented into the Incident Management system, additional tasks may need to be performed. Below is an overview of some of the possible tasks that need to be performed by different roles.

A. OIC Supervisor – Coordinator of Incident unless delegated to Incident Commander

Task	Description of Task
Assemble Incident Team	• Issue a **CONDITION ORANGE** or **RED** alert, based on the severity of the event. • Determine if it is appropriate to activate phone bridge(s) • Distribute email notification that the Incident Phone Bridge is opened and recorded. - In some cases the Incident Team may need to work at their workstations to troubleshoot and resolve the incident. The OIC Supervisor will make this decision. - If the Incident Team must work at their workstations, members will call into the Incident Phone Bridge
Document Events (Recording)	• The OIC Supervisor or shall record the event history in Conferencing Recording system and keep notes of the chronological time line of all tasks performed, as well as the time performed. The recording of bridge call and other notes to be captured using WebEx or other audio recording service. This recording to be saved to OIC Sharepoint at conclusion of call. WebEx: txdps.webex.com. • Include the following: • Track Date-Time of all incident activity, including start, escalation, bridge activation, and end time… Format: (mm-dd-yy hh:mm) • Business Unit(s) Impacted • Problem Description • Escalations – including who was contacted and the time • User Workarounds • Root Cause(s) • Steps taken to correct the problem (specify short or long term)
Manage Communications	• Perform escalation procedures • OIC Supervisor will determine if alternate escalations

Task	Description of Task
	are needed • Escalate to senior management when appropriate • Update senior management, and IT audience of current status of the incident • All notes taken by individuals during time of the incident will be consolidated and used to generate a Problem Management Ticket in Incident Management System. - Incident Ticket assignees are responsible for providing detailed troubleshooting steps required to initiate workaround, provide any corresponding information such as a Change number, and a detailed description of Root Cause/Permanent Fix - OIC will determine who should author the Problem Management ticket and assign that task.

B. Technical Team

Depending on the nature of the incident, one or many of the following on call staff will be involved: DBA, Developer, Server, Mainframe, Network Engineer, and/or Product Engineer.

- Technical Team members are to respond to a notification within 15 minutes. If there is no response from the on-call staff, escalate to the next level in the chain of command for the Technical Team member, then in 15 minutes increments until a return call is received.

Task	Description of Task
Determine Issue Scope	• Work with other members of the team to determine the scope of work needed to resolve issue.
Communicate With OIC Supervisor	• Communicate all issue updates back to the OIC Supervisor and provide ETA as to when issue will be resolved.
Resolve Issue or Escalate	• Resolve issue and communicate back to OIC Supervisor that the issue is resolved or escalate issue to next level of SMEs.
Complete Incident Management Ticket and Problem Management ticket as needed in the Incident Management System	Work with OIC Supervisor to document and complete the Incident Management Ticket in the Incident Management System, providing enough information that the OIC and/or Service Desk will have enough information to effectively troubleshoot and resolve should the incident occur again
System Available	• Send a System up and functional message to the Incident Coordinator to mark the time the incident is resolved. Facilitates the sending of the Condition Green.

NOTE: It is the ultimate responsibility of the OIC Supervisor to ensure that all details of the incident are captured in the Incident Management Ticket.

The data in the ticket should include:

- Summary (freeform text)
- Description (freeform text)
- Category (freeform text)
- Type (freeform text)
- Item (freeform text)
- Case Type
- Status
- Priority
- Login (requester information tab)
- Name (requester information tab)
- Source (requester information tab)
- Work Log (activity tab)
- Assigned Time: (mm-dd-yy hh:mm) (activity tab)

Problem Management Ticket Completion: Once the incident is resolved, all information should be included in the Problem Management Ticket that should be created by impacted service area.

C. Service Desk / OIC

Task	Description of Task
Manage Auto Answer Recording	• Change the message notification on the incoming auto answer recording to reflect the outage
Create Incident Ticket	• Incident Management System
User Status Update	• Call back to customers who have reported issues to ensure that the system(s) are up and functional with no residual effects – This should be clarified to read something like: • After a Code Orange or Red Incident has been resolved, the customer initiating the incident should be contacted within 12 hours of resolution to determine if any issues are still occurring but have not been reported
Manage Auto Answer Recording	• Change the message notification on the incoming auto answer recording to reflect the revised status
Statewide / Nationwide Broadcast	• OIC to send TLETS Administrative AP and/or APB messages as needed for CCH / DL /TCIC / DMV / TLETS or other identified system.

4. Incident Management Guidelines Checklist

Incident Management Guidelines Checklist

This checklist provides guidelines to manage the incident.

Start	Assemble Incident Team	✓
15 minutes after problem/outage start time	OIC to Determine alert level (**Yellow, Orange, Red,) depending on impact** Issue appropriate alert Open Incident Management System or refer to initial Ticket OIC Supervisor will designate an individual to keep detailed notes	
30 minutes after problem/outage start time	OIC to Update alert as needed Establish conference bridge – if necessary Contact SMEs or On-Call personnel	
1 hour after problem/outage start time	OIC Supervisor will Determine if incident meets impact guidelines for escalation to Red Alert. As applicable: Contact executive management team Contact vendor SMEs Contact TDPS OIC Initiate hourly notifications and updates, including t when the next update will be sent, and continue notifications throughout the duration of the incident.	
Resolution of problem/outage	Issue Green Alert Collect all relevant documents Ticket assignee to Update Incident Management System with enough information that the OIC and/or Service Desk can effectively troubleshoot and resolve should the incident occur again.	

NOTE: In cases requiring an intentional shutdown/startup of a system or application used by or affecting critical DPS operational functions, make appropriate notifications at least 30 minutes prior to shutdown.

5. Notification Guidelines

Applies to: System outages, unplanned reboots, other high visibility incidents requiring notifications

Service Desk procedure:

- Call arrives at Service Desk
- Technician verifies system failure by
  a. Multiple reports of the same outage
  b. Verifying system failure through troubleshooting steps
- Technician enters Incident Management Ticket
- Technician contacts OIC by telephone to advise of outage
  - 512-424-2139 – OIC
  - Technician follows up the call with the submission of the Incident Management ticket

OIC procedure

- OIC sends notifications as required to impacted users, including AP and APB administrative messages via TLETS to national law enforcement or law enforcement in Texas, depending upon the nature of the problem.
- Utilize the OIC Outage Notification spreadsheet located on OIC SharePoint Essentials
  - Subject line of email to start with color condition, Bridge or No Bridge and brief description
    - Example: Condition Red (No Bridge) US Passport Verification (AAMVA)
    - Example: Condition Red – Bridge Open – Major power outage at DPS HDQ
  - Use appropropriate distribution group
    - Place the distro group **in the bcc**: portion of the outgoing email notification
    - On the signature section of the email notification – include the row number of the distribution group included in the bcc: above
    - Include sender initials
      - Example: OIC – JL - 87
- Perform standard User and Management notification for the system or service outage based on Notification Guidelines for the specific system/service.

6. Glossary of terms

(This list will provide a full understanding of the terms used in this process)

Term	Definition
DL	Driver License
OIC Supervisor	Person responsible for escalating and coordinating the response to the Incident
Incident Commander	Person responsible for management and execution of condition alert activities
Technical Team	Staff with technical expertise related to the equipment or application
Incident Management System	Software to track an event/problem. A Case (aka ticket) is issued when an event/problem is reported or identified. Current software in use by DPS is BMC's Service Desk Express
SME	Subject Matter Expert
ETA	Estimated Time of Arrival – i.e. estimated time the problem will be resolved with the system/service and it is functioning at an acceptable level.
ETR	Estimated Time for Recovery
MTTI	Mean time to Implement
MTTR	Mean time to resolve
PMT	Problem Management Ticket in Incident Management System
RTO	Recovery Time Objective

6. Mission Critical Applications

The Mission Critical Application prioritization is based on the Business Impact Analysis (BIA) conducted in June 2010. Applications are in alphabetical order by recovery Tier, by Recovery Time Objective. The following list does **not** include IT infrastructure that is required to recover the applications. (e.g. Internet, Firewalls, DMZ, DNS, etc.)

Tier	Recovery Time Objective
Tier 1	0 to < 4 hours
Tier 2	4 Hours to < 72 Hours
Tier 3	3 Days to < 14 Days
Tier 4	14 Days and Greater

Application	Tier	RTO
AAMVA	Tier 1	< 1 Hour
AFIS	Tier 1	< 1 Hour
BorderStar	Tier 1	< 1 Hour
CCH - Computerized Criminal History (Required for TCIC - Texas Crime Information Center)	Tier 1	<1 Hour
DLS – Driver License System Applications - for Law Enforcement	Tier 1	<1 Hour
DrawBridge	Tier 1	< 1 Hour
FusionCore	Tier 1	<1 Hour
InCar	Tier 1	<1 Hour
JSI (J Tone Systems wire tap intercepts)	Tier 1	<1 Hour
LIMS	Tier 1	<1 Hour
Omnixx - Console (ASP)	Tier 1	<1 Hour
Omnixx - Force (Java)	Tier 1	<1 Hour
PenLink	Tier 1	<1 Hour
RSA	Tier 1	<1 Hour
TCIC - Texas Crime Information Center (Outstanding Warrants, Protective Orders, etc.)	Tier 1	<1 Hour

Comment [T1]: This list changes from time to time. Instead of listing all the Tier 1, 2, 3 and 4 systems, it would be better to insert a hyperlink, or refer to applicable document in Sharepoint

Application	Tier	RTO
TLETS	Tier 1	<1 Hour
TLETS Admin Message - Administrative message management application (COM)	Tier 1	<1 Hour
TLETS: Omnixx Database Servers	Tier 1	<1 Hour
TXMap	Tier 1	< 1 Hour
AIS DSS (Crystal Reports)	Tier 2	24 Hours
Black and White	Tier 2	24 Hours
BlackBerry Email	Tier 2	24 Hours
Bluezone	Tier 2	24 Hours
CAD - Computer Aided Dispatch (COM Office)	Tier 2	24 Hours
CCH-Criminal History SOR Secure and Public	Tier 2	24 Hours
CHL Database	Tier 2	24 Hours
CLERIS, CLE and BIA investigative reports from April 1999 to date	Tier 2	24 Hours
CJIS	Tier 2	24 Hours
Email/Outlook/Exchange	Tier 2	24 Hours
Emergency Alert System (EAS)	Tier 2	24 Hours
Host On-Demand (HOD)	Tier 2	24 Hours
HP-6 / 3 Citation and Warning Data Collection for Highway Patrol	Tier 2	24 Hours
IDENT - Department of Homeland Security AFIS database.	Tier 2	24 Hours
Image Verification System	Tier 2	24 Hours
In Car CAD	Tier 2	24 Hours
In Car Mobile Message - In-car / communications message management application	Tier 2	24 Hours
In Car THP-6 / 3 Motorist Assist, Citations, Warnings data collection	Tier 2	24 Hours
LTC	Tier 2	24 Hours

Application	**Tier**	**RTO**
METALS	Tier 2	24 Hours
MPCH Web	Tier 2	24 Hours
MVD - Texas Vehicle Title and Registration Records Search	Tier 2	24 Hours
NCIC	Tier 2	24 Hours
PAT	Tier 2	24 Hours
Radiant (Inventory System)	Tier 2	24 Hours
Record data base	Tier 2	24 Hours
SharePoint	Tier 2	24 Hours
SPURS	Tier 2	24 Hours
TCIC - License To Carry	Tier 2	24 Hours
TCIC - MPCH	Tier 2	24 Hours
TDEX	Tier 2	24 Hours
Texas.Gov	Tier 2	24 Hours
FORTIS	Tier 3	72 Hours
HQ-35 - Highway Patrol interdiction and seizures	Tier 3	72 Hours
INT-8 service requests	Tier 3	72 Hours
S2	Tier 3	72 Hours
SAFER/CVIEW	Tier 3	72 Hours
TCIC - SexOffender	Tier 3	72 Hours
TCIC - Trip	Tier 3	72 Hours
TXIC Daily Log (Fusion)	Tier 3	72 Hours
Workflow Management Tool (Sharepoint)	Tier 3	72 Hours
Alias DL Trap	Tier 3	7 Days
CCR - Central Cash Receiving System	Tier 2	24 Hours
FORAY ADAMS	Tier 3	7 Days
Hazard Materials (HAZMAT) - Tracks all transported Hazard Materials	Tier 3	7 Days
LAN Based (Shared Drive) Spreadsheets, Databases, Etc.	Tier 3	7 Days

Application	Tier	RTO
Lotus Notes (ALR Lotus Notes)	Tier 3	7 Days
Motor Vehicle Theft (MVT) off line search	Tier 3	7 Days
Narcotics Service Report (NSR)	Tier 3	7 Days
Omnixx - Trainer	Tier 3	7 Days
Procurement DB	Tier 3	7 Days
Rangers TR-1 and intranet	Tier 3	7 Days
SQL Server	Tier 3	7 Days
TCIC - Motor Vehicle Theft	Tier 3	7 Days
TCIC - Heat	Tier 3	7 Days
Tokopen	Tier 3	7 Days
TXGANG: TEXGANG - Website for entering / searching TX Gangs and/members	Tier 3	7 Days
AIS DSS (Query Builder)	Tier 4	>14 Days
Applicant data base	Tier 4	>14 Days
Applicant Tracking software	Tier 4	>14 Days
Big Blue	Tier 4	>14 Days
Big Blue Reporting	Tier 4	>14 Days
CAD - Computer Aided Design	Tier 4	>14 Days
CLIPS	Tier 4	>14 Days
Fleet Database	Tier 4	>14 Days
Gatekeeper	Tier 4	>14 Days
General Manual	Tier 4	>14 Days
Internet - TxFS	Tier 4	>14 Days
Intranet Access (DPSNET)	Tier 4	>14 Days
Macintosh Software	Tier 4	>14 Days
Motorola Gold Elite	Tier 4	>14 Days
MSA - Finance	Tier 4	>14 Days

Application	**Tier**	**RTO**
MSAS - HR database	Tier 4	>14 Days
MyCOOP	Tier 4	>14 Days
PE-32 (HR)	Tier 4	>14 Days
Polaroid SQL data base	Tier 4	>14 Days
Quick Key and Quick Web	Tier 4	>14 Days
SendSuite	Tier 4	>14 Days
SharePoint - OGC	Tier 4	>14 Days
SPA	Tier 4	>14 Days
Specialized Equip	Tier 4	>14 Days
TAVIS, Vehicle Inspection	Tier 4	>14 Days
Testing Software	Tier 4	>14 Days
Web Venice	Tier 4	>14 Days