

CTS Disaster Recovery Processes Updated February 21, 2014

Prepared by Jason Beers and CTS Service Owners in response to an inquiry from the Office of the State Treasurer.

Telephone –

The DR plan for the phone systems vary by site and thus recovery windows range from 0-120 hours.

The system is distributed across 3 host processors in 3 different buildings in the Olympia campus area. All 3 of these hosts have redundancy built in but do not provide redundancy for the other hosts (if a processor in one of the hosts fails, a redundant processor in that host will allow functionality to continue). If a host totally fails, some gateways have standalone capability (the ability to make and receive calls but other functionality, i.e. voicemail lights, is limited). Other gateways would have to be re-homed to the remaining processors or staff would have to be moved to locations that still have service. CTS and Avaya maintain crash kits with most system components locally.

State Government Network –

The SGN is designed to re-route traffic in the event of a single node site failure. The failure of two or more node sites will produce unpredictable routing.

Customer sites with connectivity to the SGN through only one node site will lose access to the SGN if that node site fails. Some agencies have consequently secured connections to more than one node site (redundancy).

Loss of the Olympia node site (currently in OB2) will result in the unavailability of Firewalls. Recovery from the loss of OB2 is a manual process. The transition to the SDC has resulted in changes to our rebuild process. An effort is currently underway to identify these changes with results expected in the next six weeks.

Secure File Transfer –

Infrastructure has been placed in Spokane to support SFT after an event. System configuration data is replicated to the Spokane infrastructure on a daily basis. The failover process is manual, and estimated to take up to 8 hours. Files that were sent prior to the event, but not yet retrieved, will need to be re-sent by the customer.

Business Continuity (TierPoint) –

TierPoint was provisioned as a site for customers to place their business continuity infrastructure. There is no DR in place for TierPoint as it is the DR solution. An event

that disrupts TierPoint (in Eastern WA) is unlikely to simultaneously disrupt production systems (in Western WA) and vice versa.

IBM 390 Mainframe –

The MPLS network has been extended to the hot-site in PA where our mainframe recovery infrastructure resides. In the event of a disaster, once the mainframe has been recovered by CTS staff (RTO is 72 hours); customers will be able to access the mainframe using Host-on-Demand (HOD) just as they do our production mainframe.

Connection of the recovered mainframe to the SFT service (both production and DR infrastructure) has been tested successfully during our semi-annual mainframe DR exercises.

Secure Access WA –

SAW functionality is now present with the October 2013 addition of the 1.5M+ user repository in Spokane. The customer proxy mappings are still a manual task and will take up to 24 hours to recover.

The Spokane SAW infrastructure will be available for use at all times; it will just require a different URL to access it. In the event of a disaster, CTS will make a DNS change to point the production URL to the Spokane IP address. Customers who require immediate access to SAW in the event of a disaster will be able to use the Spokane URL directly until the DNS change is made.

VPN –

Infrastructure to support VPN has been installed in Spokane, and failover is automatic. However, usability of that infrastructure is dependent on administrative changes made by both CTS and individual agency security personnel.

Choice of which server to connect to is done at the VPN client level; however, customers must create a new connection entry for the Spokane server.

DNS changes, performed by CTS staff, would be required for access through Citrix and Juniper remote access front-end solutions.

Shared Service Email –

SSE is configured in a redundant 3-node structure. The Olympia site is a two-node highly-available configuration. The third node is in Spokane for disaster recovery purposes. In the event of a declared disaster, a site recovery would be performed at the Spokane node. A site recovery may take up to 8 hours. Exchange, OWA, and ActiveSync would be available once the site recovery is complete.

Infrastructure for WaSERV data has been installed in Spokane, and data is replicated there. Since access to archival data has not been identified as a 'critical service', no infrastructure has been installed to host the software to access that data. After an event, equipment would be acquired and installed, the software would be installed, and the indexes to the data would be rebuilt. RTO for WaSERV is established at 30 days.