Tiering

Tiering of IT services is based upon the Recovery Time Objective (RTO). The below chart represents ***guidelines*** and ***suggested*** DR strategies for IT systems based on Tiering. To determine the DR Strategy of your IT system, please contact your Technical Application Manager or Bernie Conlu [1].

Recovery Time Objective (RTO): The maximum tolerable length of time that a computer, system, application can be down before major impacts occur.

Recovery Point Objective (RPO): The maximum targeted period of time in which data might be loss from an IT service due to a major incident.

RTO	Tier Name	Tier Definition	DR Strategy	Short Technology Description
Up to 15 minutes	0	Core technology infrastructure that requires multiple data centers to be able to serve production without manual intervention. Includes services related to: • Network Services (Switch, Router, Firewall, Load Balancer, Internet, WAN) • Storage Services (EMC, IBM SANs, EMC DPA, IBM SVC) • Platform & Virtualization Services (VMWare, vCenter, AIX) • Domain Services (AD, DNS, DHCP, ACS)	Geographically clustered (Active-Active)	Real time data replication between data centers (Active Directory, DNS, DHCP).

RTO	Tier Name	Tier Definition	DR Strategy	Short Technology Description
Up to 6 hours	1	Systems are critical to patient health and safety for immediate clinical decision making or patient diagnostic and documentation. Failure to function for even a short period of time could have a severe impact on patient treatment. Manual downtime procedures are planned, but cannot be sustained for a long period of time. Includes services related to: • Core Communication Infrastructure • Core Patient Care Delivery • Patient Monitoring Systems	Hot/Warm Standby	Dedicated DR environment at alternate data center. Servers are racked, configured, tested, and ready to use at alternate data center. Asynchronous replication of business data and system states to available hardware.
Up to 24 hours	2	Systems are required in order to perform critical hospital and business operations, but can allow for manual processes for up to 1 day as a reasonable workaround.	Warm Standby	Servers are provisioned and configured at alternate site. Replicated snapshots throughout day to available hardware.
Up to 5 days	3	Systems are necessary to UCSF, but short-term interruption or unavailability of 1 to 5 days is acceptable.	Cold Standby	Hardware and servers are reserved or allocated at an alternate data center. Backup restoration to hardware with horizontal scaling and ship on-demand hardware.

RTO	Tier Name	Tier Definition	DR Strategy	Short Technology Description
Up to 30 days	4	The functions affected do not jeopardize health, safety or security of patients, faculty, students or employees and manual procedures could be used until system is available.	ATOD (At Time of Disaster)	Quick ship agreements may be possible with preferred vendors for delivery at time of disaster. No hardware in place at alternate site.
Not Applicable	N/A	When an IT system or service is not managed by UCSFIT or hosted in a UCSFIT Data Center. UC tiering standards do not apply.	N/A	N/A

Information Technology
UCSF Main Site

Links
[1] mailto:Bernie.Conlu@ucsf.edu