Last updated March 30, 2010

Server Justification and Disaster Recovery (DR) Plan FAQ

1. Do I have to submit a letter and plan for every server I'm running?

A letter of justification is required for every server, or collection of servers, providing a "service" to a department. The services generally fall into the area of e-mail, file server, or Web/application server. For every authorized server that provides a service in support of a critical line of service, a written Disaster Recovery Plan is required.

2. My department is a separate institute or auxiliary. Do I need to file letter(s) of justification and DR plans?

Yes. Unless your unit reports to an external organization such as the Law School, the Ag Center, the LSU Foundation, or LSU Alumni Association, you should file letters and DR plans.

3. What can ITS do to help me with meeting the Disaster Recovery Plan requirements?

Moving a server to a virtual image in the data center with an accompanying support contract with University Networking and Infrastructure (UNI) group may simplify the preparation of a DR plan for a departmental server. However, the justification letter and plan would still be required.

4. All of my servers and services are outsourced off campus. Do I need to submit the letters and plans?

Outsourced e-mail and application services are not exempt from the justification letter and DR plan requirements. However, documentation from your hosted provider may make it easier to prepare your DR plan.

5. What should the justification letter contain?

Letters of justification should identify,

- the name of the server or "service" being justified
- the rationale for running a separate service
- a description of its function and capabilities including the level of resources (storage, memory, etc)
- how patch management of the operating system and software is handled
- the lifecycle replacement schedule for the server(s)
- how public records requests (PRR) are received and handled, and by whom
- for email servers, how identity management is handled if accounts are being issued and the strategic plan outlining the future of e-mail support within the department

6. To whom should the letter of justification be addressed? To whom should DR plans be sent?

The letter should be addressed to Brian Voss, the Vice Chancellor for IT. The DR plans should be sent to the Frey Computing Center to the attention of "Emergency Operations Center".

7. What should the disaster recovery (DR) plan contain?

The disaster recovery plan should address the following; time and resources required to return the service to operation in the case of a loss and the measures currently being taken to preserve institutional data (backups/redundancy measures).

A workshop was presented on March 17 discussing design parameters of Disaster Recovery plans. The PowerPoint slides are available on the "Disaster Recovery" page of the ITS Security & Policy web site, http://itsweb.lsu.edu/ITS_Security/Data_Management/Disaster_Recovery/item815.html.

8. Can I just move my physical server into the data center to avoid submitting the letter and plan?

Moving a physical server into the data center will not satisfy the requirements of the auditors and is not possible at this time due to resource constraints. It may be possible to acquire a virtual server instance from existing infrastructure housed in the data center. To discuss the availability of virtual servers resources at ITS, submit a request through the UNI Web site, http://newservicerequest.lsu.edu and an analyst will contact you.

9. If I eliminate my e-mail server and move my e-mail accounts into one of the central e-mail systems can I avoid submitting the letter and plan for my e-mail server?

Yes. To discuss migrating your e-mail accounts into the central e-mail service at ITS, submit a request through the UNI Web site, http://newservicerequest.lsu.edu and an analyst will contact you.

Additions as of 03/30/2010

10. Who will be evaluating justification letters?

The letters will be reviewed by the Chief IT Security Officer (John Borne) and his security staff in the Office of the Vice Chancellor for IT and ITS; the Chief IT Security Officer will forward letters with his recommendations to the Vice Chancellor for IT (Brian Voss), who will make decisions regarding outcomes. The Vice Chancellor may wish to speak with a given College Dean, departmental Director, or Vice Chancellor before reaching a final decision on a case-by-case basis.

11. What is adequate justification?

There are no set criteria for ensuring approval of a justification. The most effective strategy for justifying a server or service is to clearly and honestly delineate the reasons for operating and supporting it. The individuals reviewing the justifications are all qualified for the task with long experience supporting servers and services at the University.

12. Should justification letters be focused on “services” or “servers”?

A department can take either approach or both. A service may be supported by several servers. For instance, there may be several file servers in a department for which the justifications would be identical. In such a case, one letter, or section of a letter, would suffice addressing the “service” that simply identifies the servers involved. A similar example might be an application “service” might have several servers as part of its architecture. Again, that would be one letter, or section in your letter. Alternatively, a department can simply name a server and speak to its purpose and critical nature.

13. Do I need to submit a justification letter for a print server?

Probably not. In many cases creative ways can be found to provide services if they are lost or destroyed. If the server is not required for your department to operate, then it is not critical. However, if a print server is an essential part of a large computer lab you are operating, then perhaps you might want to include it.

14. What if no justification is provided?

If no justification and DR plan is submitted for a server critical to the operation of the University, then we may be forced to terminate its connection to the network.

15. Is the audit document a public record?

Yes, the audit document is a public record. We have chosen not to post it to our website because it describes possible vulnerabilities of the University and contains findings that specifically name certain Colleges and Departments. If you wish to see the final audit document, contact the Chief IT Security Officer (John Borne).

16. Why do I need a Disaster Recovery Plan?

It is reasonable and prudent to have a documented plan to recover critical services needed for your department to continue to perform its lines of service. It is also required by both the State of Louisiana via the Office of Information Technology, and by the LSU System per PM-36.
http://itsweb.lsu.edu/ITS_Security/IT_Policies/LSU/item614.html

17. What qualifies as "a server"?

While there are many possible definitions, in general, a server is a single instance of an operating system. A service is an application or function that runs across one or more servers.

18. Is a Disaster Recovery Plan for a service, or for a server?

Ultimately, it is for the service, but depending on how your technology is architected, it may make more sense to approach things from a server perspective.

19. Must every server have a written Disaster Recovery Plan?

No, just the ones you would ever need to restore. Let us suppose the building housing your servers were to burn to the ground. Any servers that you would not need to restore, ever, don't require a written recovery plan. It may still be a good idea to mention them in a plan to acknowledge their existence and the fact that they are not required for your unit's basic operations.

20. How should a Disaster Recovery Plan address a server running multiple applications that have different recovery parameters?

There are two approaches to this. The simplest is to treat the server and all its applications as a single unit and restore the whole thing to match the most strict recovery parameters. The other approach is to restore the applications and their associated data files individually, though this tends to make for a more complicated recovery scenario.

21. How are Disaster Recovery plan timeframes supposed to account for outside dependencies, such as facilities availability, network infrastructure and/or financial resources?

It is a good idea to list assumptions and dependencies in the preamble to a DR plan. Your plan should indicate that any time requirements are relative to the listed assumptions and dependencies. Most departmental plans would be designed to recover from the "100 ft" event, that is, an event confined to a small area perhaps no bigger than a single building. In such a case, it would be acceptable to list as an assumption that the recovery facility located in a different building and the existing network connections for that building would be available. If expenditures would be required to implement the plan in the event of a disaster, estimates of the amounts should be included in the plan. It would be advisable to seek the guidance of the departmental budget authority for your unit if your plan contains such emergency funding assumptions.

22. What are guidelines for storing backup data off-site?

Data to be used in a recovery should be stored beyond the "blast zone" (radius of the event). The security responsibilities you have for the data travels with all copies of the data. Thus, in addition to it being an appropriate environment for the physical media (i.e., clean, safe from the elements, etc), it should be a secure environment as well. This applies to data while in transit as well as the storage destination. Sensitive or protected data should be encrypted in storage and during transmission.

23. Who will evaluate our Disaster Recovery Plan?

It is up to each department to determine if their plans are adequate to meet their needs. The Emergency Operations Center (EOC) requires every department to submit a copy of their DR plan and has the authority to review and make recommendations as deemed necessary.

24. Can we see an example IT Disaster Recovery Plan?

There is a checklist of recommended elements for a Disaster Recovery Plan. There is also a sample plan documented using the checklist and based on an actual plan that a department has agreed to share. These are found on the LSU ITS Disaster Recovery web page,
http://itsweb.lsu.edu/ITS_Security/Data_Management/Disaster_Recovery/item815.html