(Please submit to Patrick Stewart, Director of Data Center Services, C-1631, Mail-Stop 10020)

The purpose of this form is to gather information required for a new server build. Please complete all fields. If you need assistance filling in the form please contact Infrastructure Services in the Information Technology department.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Requesters Information** | | | | | |
| Name: | | | | | Date: |
| Department: | | | Title: | | |
| Building/Room: | Phone: | | | | Service Desk Request #: |
| Email Address: | | | | | |
| Manager/Supervisor: | | Supervisors Phone: | | | |
| **Server Information** | | | | | | |
| Type of server (check all that apply):  Linux  Application Server  Database Server  File Share Server  Print Server  Web Server  Other:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | |
| Environment (check only one): Production Development  Does this system need to be available during Disaster Recovery: Yes No | | | | | | |
| Will this server house Personally Identifiable Information (PII): No Yes | | | | | | |
| Server Owner:  Name (Last, First) \_\_\_\_ \_Stewart, Patrick\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Server Administrator:  Name (Last, First) \_\_\_\_\_\_ Bowers, Susie \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Security Administrator:  Name (Last, First) \_\_\_\_\_\_\_Bowers, Susie\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | |
| Application Administrator (individual or department responsible for maintaining the application software):  Name: \_\_\_\_\_Susie Bowers\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone: \_\_\_409-880-2261\_\_\_\_\_\_\_\_\_\_\_\_\_  Will remote desktop or SSH access be required: No Yes, List the IP of users system: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | |
| **System Requirements** | | | | | | |
| Check one: Virtual Machine Physical Server | | | | | | |
| Server Name: \_  Operating System: Windows 2012 R2\_Datacenter \_\_\_\_\_\_\_\_\_\_  Nbr of CPU’s: \_2\_\_\_\_\_\_\_  Processor: \_3 Ghz\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Memory: \_\_16 Gb \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Storage requirements for application/data**:\_Active Directory \_\_**  Application Software:\_\_Microsoft Windows 2012 R2 DataCenter \_\_\_\_\_\_ | | | | Will backups be required: No Yes  Note: Standard backup policy – Full backups are ran once a week and retained for 1 month. Cumulative incrementals are ran daily and retained for 2 weeks. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Authorization** | | | |
| All requests for servers must be approved by the appropriate Dean or Department Head. By signing below the department head certifies the server is required | | | |
| Print Name: | Date: | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature of Dean or Department Head | | | |
| **Infrastructure Service Authorization** | | | |
| All requests for servers must be coordinated with and signed by the Director of Infrastructure Service or the designated representative. | | | |
| Print Name: | Date: | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Director IT Computing Infrastructure | | | |
| **To be completed by Infrastructure Services System Administrator** | | | |
| Service Tag/Serial Nbr: | LU Tag Nbr: | |
| **Networking Information** | | | |
| Private IP: | VLAN: | | |
| Public IP: | DRAC IP: | | |
| Standard Management Software/agents installed:  Netbackup Client software  Nagios Client software  OMSA configured | | | |
| Printed Name: | | Date: | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature Designated System Administrator | | | |

**Lamar University Server Policy**

1. Information resources, including servers, are provided for the purpose of accomplishing tasks related to the university’s mission.
2. Any server that is connected to the university network must comply with this policy, related policies, established standards and procedures.
3. Specific personnel will be identified for each of the following roles:
   1. Server Owner
   2. Server Administrator
   3. Security Administrator
   4. Application Owner
4. Server owners must register their server with the Lamar University Information Technology Services Division and provide yearly verification of all necessary information required in the registration process. Changes to server registration information will be promptly reported to the Information Technology Division.
5. Public services will be disabled for any server that does not meet yearly registration requirements. Server owners and server administrators will participate in and/or conduct a yearly risk assessment of their designated servers based on server registration information.
6. The server owner is responsible for the management, operation, and security of the server. Server administration functions may be designated; however, the server owner retains ultimate responsibility for the server. The server owner will, at a minimum:
   1. Register the server with ITS
   2. Designate a server administrator
   3. Designate a security administrator
   4. Provide fiscal resources required to maintain server policy compliance
   5. Include server management compliance in fiscal planning, business/academic continuity planning,   
      and personnel resource planning.
   6. Ensure proper training for server administrators and security administrators
   7. Respond to any vulnerability scan notifications from ITS
   8. Participate in yearly risk assessments
   9. Ensure that risk mitigation activities identified are resolved within 90 days of risk assessment   
      completion.
   10. With coordination through ITS, respond to audit requests made by TSUS, state or federal audit  
       agencies.
7. Prior to the purchase of any server, the server owner should contact ITS to evaluate the capabilities required to maintain server compliance and review alternative solutions where applicable.
8. ITS will be notified in advance when the purpose, location, management, or disposition of the server changes.
9. ITS will publish server management guidelines for use by server administrators.
10. ITS will conduct routine scans of the university server environment. Vulnerabilities will be communicated to the server owner and server administrator for resolution. The Server owner must respond with an acknowledgement within 3 days. Vulnerabilities that remain unresolved for 30 or more days are subject to disconnect. Servers that pose an immediate threat to network operations, performance, or security may be disconnected or quarantined until the threat is removed.
11. Incident management procedures will be executed by ITS when appropriate.

Definitions

Server Management – Functions that enable the server to operate within acceptable parameters of performance, security, availability, and business continuity.

Server Owner – The department head charged with overall responsibility for the server asset in the university’s inventory records.

Server Administrator – An individual designated by the server owner as principally responsible for performing server management functions, including the installation, configuration, security, monitoring, maintenance, registration, and assessment of the server.

Security Administrator – An individual designated by the server owner as principally responsible for performing security management functions, including provisioning, review and monitoring of server accounts.

Application Owner – The individual responsible for installing, updating and maintaining the application software on the server.