Information Services Hosting Arrangements

Purpose

The purpose of this service is to provide secure, supported, and reasonably accessible computing environments for departments at DePaul that need server-based technologies.

Server Hosting Services Provided

DePaul's Information Services data center provides a secure, 7x24 environment with electrical power, HVAC, UPS, servers, and network connections. Information Services will provide facilities for data backup and system administration services for supported OS, including system patching, maintenance, and monitoring.

Servers

Information Services will provide the servers and other computer and operating-system software to operate and support the application. Unless it is determined that a physical server is a requirement, the server provisioned by Information Services will be a virtual server and will be provisioned to meet the resource requirements of the application.

Information Services will configure the server, and Campus Partner (or authorized designee) will load and/or configure any applications necessary onto the server computer(s) as needed for their business requirements. After the server is loaded, set up with the Campus Partner application, and is fully operational, Campus Partner will be responsible for all application management. Information Services will work with Campus Partner on backup arrangements.

Storage, backup, and networking

Information Services will provide connection of the Server to the campus network and Internet if required, including all networking equipment and connections for the server to provide access on a 24-hour-a-day, 7-day-a-week basis, allowing for scheduled maintenance downtimes. When initially configured, your server cannot communicate with any other systems over the network. All communications required for both access to the server, and any functionality provided by the server, will have to be explicitly requested by the campus partner. Information Services will discuss with the campus partner what will be required, and the campus partner may have to provide documentation about your requirements at a port/protocol level.

Information Services will provide storage and backup as agreed to prior to the deployment of the hosted server. Information Services currently provides a standard backup policy retention of 90 daily backups. In the event of an issue where the system needs to be restored from backup, upon request Information Services will recover backed-up data from an agreed-upon date/time. Should storage, backup, or networking requirements change, Information Services should be notified with appropriate advance notice to plan for any necessary changes.

Necessary maintenance, patching, and monitoring

Information Services employs a regular maintenance window for Windows and Linux Server Patching. Windows Server patches are evaluated after each "Patch Tuesday" with an expectation of deployment to dev/test environments on the Sunday morning following "Patch Tuesday". Production Windows systems will receive Windows Server patches on the following Sunday, one week later. Linux system patches are generally applied quarterly with test environments receiving patches before production systems. Periodic Network and Security device patching is also performed as needed. Information Services will use its best efforts to provide uninterrupted server and network availability, except for scheduled maintenance downtime and any interruption beyond our control (e.g., acts of nature, equipment or transmission failures, security breaches, etc.).

Information Services will perform maintenance services as we determine reasonably necessary to maintain the continuous, secure operation of the Server. Information Services will provide prior notice of any maintenance downtimes that fall outside of regularly scheduled maintenance windows, except when circumstances beyond our control limit our ability to do so.

Campus Partners will be given access to monitoring systems that provide service availability information and may receive alerts directly at their discretion for immediate notification of service degradation.

Other Considerations

Information Services will install anti-virus and vulnerability assessment software and keep this software up to date. In the situation where this may cause problems with the normal usage of the application, exemptions can be discussed with appropriate documentation from the application vendor.

Information Services can provide a database in our Oracle, SQL, or MySQL farms and will cover the licensing required. Database configuration details, including storage, backup, and account requirements will need to be provided by the campus partner. These details will be discussed and agreed to prior to the deployment of the hosted server.

Additionally, Information Services can provide load balancing, a downtime/maintenance sorry page, and DNS services.

Campus Partner Responsibilities

The goal of Information Services Server hosting is to provide the highest possible level of quality, security, and uptime. To ensure that required service levels can be maintained, it is crucial that Information Services has standardized on a core set of minimum configurations and that essential coordination and planning are adhered to. Information Services and the campus partner will jointly establish a team with responsibilities to coordinate server hosting planning, operations, and maintenance.

To support this goal, the Campus Partner will be responsible for and manage the following:

- Identify and provide contact information for personnel who will serve as the primary technical liaisons who will be capable of addressing technical issues related to your server/application.

Should these resources change, campus partner agrees to notify Information Services via the Information Services Systems Team email account systems@depaul.edu.

- Provide and maintain contact information for a functional owner who can make decisions regarding your system's functionality and availability, communicating with any user community, and taking overall responsibility for this system at DePaul.
- Only use your server for the purpose or application it was initially set up for. If you need to install another piece of software, please ask for another server, or check with IS to see if it will be ok to install additionally on your existing server.
- Acknowledge, follow-up, and close-out any query that Information Services forwards to campus partner for resolution.
- Provide Information Services with timely notice of any disruption of services and/or changes in the campus partner's technical and/or server environments.
- Provide contacts that will be available to assist Information Services with tasks that may require "after hours" or emergency completion.
- Evaluate and communicate any problems or concerns with services to the Information Services Systems Team email account systems@depaul.edu , or to the Infrastructure Associate Director (Ryan Johnston, ryan.johnston@depaul.edu, 312-362-7789) directly.
- Administration of all non-OS software (i.e. 3rd party software, applications, etc.) hosted on the server. This includes user account management, as well as any licensing requirements necessary for non-OS software.
- Campus partner is responsible for testing service and application operation after OS patches have been installed (to ensure/verify that patches have not had an adverse effect.)
- Campus partner application(s) will run on standard, supported operating systems. Information Services supports current Windows and Oracle Linux Server versions that have available mainstream support from the vendor. Information Services will provide at least 6 months advance notice if an OS/version will be dropped from support and will work with the campus partner to migrate servers to newer, supported OS versions. If an unsupported version of Operating System is required, campus partner must work with Information Services to resolve.
- Provide adequate advance notification of any required changes to the server, or applications running on the server, including upgrades of applications, migrations or upgrades to new OS versions, new or additional components, frameworks, or supporting system requirements, etc. Questions about desired changes should be made to the Information Services Systems Team at systems@depaul.edu . Requests for changes should be filled out via a direct Systems team Helpdesk request form. If required changes turn out to require significant resource commitments, these changes may necessitate the creation of a formal Information Services project request, subject to scheduling and approval in accordance with normal Information Services project procedures.
- Other
    - Follow all established DePaul policies
    - Participate in audits and security assessments as necessary
    - Maintain vendor support contracts

- Conform to application security best practices

Issue Reporting

If there is a non-critical issue or request that the customer needs to report to Information Services, there are two preferred methods of notification. The preferred method is to utilize DePaul's ServiceNow Helpdesk ticket system to notify Information Services of any issue. You may also call (312) 362-8765 to reach an IS Helpdesk agent. The Helpdesk serves as the front-line for all technology related questions or problems and will log and communicate issues to the Information Services Systems team.

Support Response Time

Information Services maintains systems to monitor servers and data center infrastructure components in order to maximize system availability. These monitoring systems notify Information Services team members and application administrators when critical failures or problems arise.

Emergency Cases

During an emergency, Information Services on-call personnel will respond to the situation within 2 hours during business hours (defined as 6am – 10pm) and within 4 hours outside of those times. After initial response, IS personnel will address issues as quickly as possible. The following are defined as Emergency categories: Critical server down; Storage offline; Network or connectivity issues for critical systems.

Non-Emergency Cases

Information Services personnel will respond within a minimum of 2 business days and will address these issues as soon as possible. This includes issues related to application functionality, system errors, account problems, etc.

Emergency Notification

In an emergency, a campus partner should contact the on-call systems team engineer via phone at 312-362-0042. This method should only be used for critical issues and outages of DePaul Infrastructure.

Change Management

Notifications of desired changes should be made to the Information Services Systems Team via a Helpdesk Systems Team request form. This includes requests for upgrades to new versions of applications or OS, migrations to new servers, new or additional components, frameworks, or supporting system requirements, new account creation or account changes, etc. If required changes turn out to require significant resource commitments, these changes may necessitate the creation of a formal Information Services project request, subject to scheduling and approval in accordance with normal Information Services project procedures. Please note that any change to system networking or communication requirements may require updates to firewall configurations, subject to review by the Information Services Systems and Security teams.

Server Access

Information Services provides standard methods of server access as described below. Exceptions to these standard access methods should be discussed in advance and agreed on by Information Services and campus partner.

Admin Access

Standard procedures allow admin access to the application owner(s) and technical owner(s) via RDP (Remote Desktop Protocol) and SSH\SFTP through the data center VPN. Vendor access for remote management and troubleshooting can also be configured however, that access is coordinated with Information Services Security and is done on an as needed basis. If remote access for the vendor is only needed temporarily it is recommended to be removed as soon as the necessary work they are performing is complete.

User Access

If user access via RDP and/or SSH/SFTP is required, campus partner should communicate and discuss with the Information Services Systems Team.

Physical Access

If in-person physical access is required for equipment owned by the campus partner that access can be coordinated with the Systems team. Campus partners should put in a request with the team indicated the time and date the access is needed. Access is given via an IS employee escort who may, at their discretion, accompany the campus partner/vendor for the duration of their work.