Website Hosting Services
Service Level Agreement
University of Hawaii, Information Technology Services
D R A F T v 1 – 0 1

Service Level Agreements (SLAs) ensure that two parties have a common understanding of what services are being offered, and under what conditions these offers exist so that there are no misunderstandings and so that the desired level of service is achieved.

Purpose

This SLA describes the ITS Service for Website Hosting Services and the roles are responsibilities of all involved parties.

Parties

Service Provider: UH, Information and Technology Services

Executive Sponsor:

Name: _____

Office Location: _____

Department/Staff Office: _____

Validity Period

This SLA is effective for the entire life cycle of the hosted website; from planning through implementation in production and until the hosted website is removed from the ITS Data Center. ITS involvement during the planning stage is critical to ensuring that adequate resources are available to successfully host the website.

Scope

1. **Planning**
   During the planning stage ITS will review proposal for a hosted website and ensure that adequate hardware and network resources are available. The availability of resources, including ITS staff resources will influence the time lines for implementation.
2. **Website Hosting Requirements**
   - The website must be relevant to the University's mission.
   - The website must adequately protect information that is not appropriate to make public, such as personal identity information.
   - The website must not present a security risk.
   - The website must be supported by a dedicated technically knowledgeable website administrator.
3. **Management requirements**
   ITS can only host websites supported by a dedicated Website Administrator. The Website Administrator is responsible for taking all trouble calls related to the website. The Website Administrator must notify ITS immediately of any changes to the following information:

   Primary Contact Information

   Name: _____

Office Location: _____

Office Phone Number: _____

Pager or Cell Number: _____

Email: _____

Secondary Contact Information

Name: _____

Office Location: _____

Office Phone Number: _____

Pager or Cell Number: _____

Email: _____

Additional Contact Instructions: _____

_____

_____

_____

4. ITS Data Center Infrastructure

The ITS Data Center is designed to support the availability requirements of UH for its servers and applications. By design the ITS Data Center is a 24x7 facility and includes tools and practices that provides for rapid detection of and escalation for problems as they arise. While ITS has taken precautions to ensure high availability of servers and services, continuous availability cannot be guarantied due to the need for periodic maintenance, infrastructure improvements, construction, etc.

ITS Data Center features:

- Uninterrupted Power Supply
- Redundantly powered equipment racks
- Redundant air conditioning units
- Air temperature monitors
- Network monitoring
- Server and services monitoring
- Video surveillance
- Fire suppression system
- Fire detection sensors and alarms

- Automated tape backups
- Robotic tape librarian

5. **Network Security**
   All production servers are protected by a network firewall. ITS staff must work with a knowledgeable System Administrator in order to determine the appropriate policies for allowing internet connections between the Equipment and the Internet. By default the firewall is configured extremely conservatively and this may prevent some intended services from functioning properly if the appropriate policies are not in place.
6. **Physical Security**
   There is an official list of who may enter the ITS Data Center. Access to the Equipment in the ITS Data Center is limited only to System Administrators that are officially listed. There will be no exceptions, if a System Administrator is not listed, entry will not be permitted. Additionally, System Administrators must have a UH staff or student ID, or a State or Federal government issued picture ID available for verifying identity to ITS Data Center staff. Note that video surveillance is enforced. Any System Administrator found in the wrong areas or engaged in inappropriate activities may be immediately escorted from the ITS Data Center and barred from ever returning.
7. **Monitoring**
   Servers and Services are monitored 24x7, except for State holidays. In order for Services to be monitored the System Administrator will need to work with ITS staff to identify services to be monitored. In the event of a problem, ITS staff will follow the escalation instructions provided. These instructions must be unambiguous. Typically, such instructions indicate who to contact, how to contact them, and any restrictions on the hours of contact. Additionally, instructions can include up to two additional individuals to be included in the escalation instructions. Please note that ITS staff will usually wait about 10 minutes for a return call before moving on to the next person in the list of emergency contacts.
8. **Disaster Recovery**
   In the event of catastrophic system failure, ITS staff will provide the System Administrator with access to backup tapes. Full backups are done weekly with incremental backups done daily after normal working hours. While ITS has well established practices and procedures to ensure the reliability of backups, ITS can assume no liability for any problems with restoring from backups.

Infractions

1. Websites that become dysfunctional, due for example to neglect to keep up with changes to PHP, etc may be disabled in the Test and Production environments.
2. Websites that present a security risk may be disabled in the Test and Production environments.
3. Websites that provide inappropriate content may be disabled in the Test and Production environments.
4. Websites that provide access to information that is not appropriate to be made public, such as personal identity information, may be disabled in the Test and Production environments.

Optional services

None at present.