University of Hawai‘i Hosted Website Service Service Level Agreement

(DRAFT 2018)

This Service Level Agreement (SLA) ensures 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.

Table of Contents

Purpose

This SLA describes the Information Technology Services (ITS) Service for the University of Hawai‘i (UH) Website Hosting Services and the roles are responsibilities of all involved parties.

Parties

Service Provider

University of Hawai‘i, 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 timelines 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 personally identifiable information (PII). Information on institutional data classification categories is available through the UH Systemwide Policies and Procedures Information System (PPIS) under Executive Policy E2.214 (http://www.hawaii.edu/policy/e2.214). 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

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 guaranteed 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.

9. General Commitment to Accessibility

By University policy, all web content should be in compliance with federal Section 508 Standards and should also meet the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA as outlined in EP2.210 (http://www.hawaii.edu/policy/e2.210). This includes any theme used if using a CMS (e.g. Drupal, WordPress). Existing content should be checked for compliance, and remediated on a prioritized basis in accordance with time and resource availability. Any legal mandate may obligate remediation on a specified timeline.

Please refer to the UH Guidelines for Accessible Technology and Digital Media at http://www.hawaii.edu/access/uhguidelines.html and to Information on Website Accessibility at http://www.hawaii.edu/access/webaccess.html, for more information on how to make your web content accessible.

10. Unscheduled Downtimes

ITS endeavors to minimize unscheduled downtimes. However, these may occur for a variety of reasons including hardware or software failure, human error, or emergency security upgrades.

Interruptions in service and their resolutions are posted to the ITS Alerts page at http://www.hawaii.edu/its/alerts.

Infractions

- Websites that become dysfunctional due to neglect keeping up with changes to PHP may be disabled.
- Websites that present a security risk may be disabled.
- Websites that are not properly maintained or patched, especially content management systems (e.g. Drupal, WordPress), may be disabled.
- Websites that provide inappropriate content may be disabled.
- Websites that provide access to information that is not appropriate to be made public, such as personally identifiable information, may be disabled.

ITS will be running frequent scans for any vulnerabilities existing on our hosting service. Any breach to this Service Level Agreement will involve:

- Upon the first violation, a written warning will be given.
- A second violation will result in a 6-month ban from the UH Hosted Website Service.
- A third violation will result in a permanent ban from the UH Hosted Website Service.

Optional services

None at present.