TAMUSA Standard 29.01.03.O0.01.S3: IT Standards for University Public Web Sites

PURPOSE OF THESE STANDARDS

The university's public websites are its public face and as such present special risks to the institution. The purpose of these standards is to mitigate those risks.

Because they do not authenticate users, the university's public websites are more likely to be attacked and compromised. The university's brand is diluted when there isn't a consistent look and feel. The university's reputation is damaged by messages which contradict the university's vision or fail to meet minimal editorial standards. Websites that do not comply with relevant law and policy harm our users and increase the risk of litigation and reputational damage.

DEFINITIONS

Public website is a website that does not require users to authenticate before accessing. Websites that require users to authenticate (e.g. Blackboard, Jagwire) are not public websites.

University public website or **UPW** is any public website where at least one of the following conditions is true:

1. The domain of the website is owned by the university, e.g. tamusa.edu, jaguar.tamu.edu;
2. The university is contractually obligated to maintain the website;
3. The university pays for any costs associated with the website (e.g. development, hosting, management, etc.) regardless of the source of funds, or;
4. A reasonable person would conclude that the website is owned or operated by the university, or that the website speaks on behalf of the university.

UPW-related resources are the information resources used in the creation and management of UPWs. Examples include domain names and web hosting services.

POLICIES

1. Governance
    a. The university's webmaster (webmaster@tamusa.edu) shall:
        i. Be selected by the university's Chief Information Officer;
        ii. Review all proposed UPW-related acquisitions and renewals and have the authority to deny any such that does not comply with relevant law or policy;
        iii. Have the authority to disable, in whole or in part, any non-compliant UPW or related information resources;

iv. Have the authority to require a UPW to be managed within a specific environment (e.g. web hosting environment, content management system).
v. Have the authority to scan websites for compliance checking;
vi. Have the authority to issue binding guidelines **tamusa.edu/upwguidelines** regarding UPW content and management. Such guidelines must be approved by the Director of Marketing and Communications to become official.

b. The Director of Marketing and Communications shall have the authority to:
   i. Review all proposed UPW-related acquisitions and renewals and have the authority to deny any such that does not comply with relevant law or policy;
   ii. Direct the webmaster to disable, in whole or in part, any UPW or related resources.

2. Compliance
   a. UPWs are state websites and thus must comply with Texas Administrative Code §206 "State Websites".
   b. UPWs must comply with the university's binding UPW Guidelines found at **tamusa.edu/upwguidelines**.
   c. UPWs and UPW-related resources are university information resources and must comply with all law and policy applicable to information resources, including the university's IT Standards for All Users and IT Standards for Owners and Custodians.
3. Exceptions
   a. To request an exception to any policy regarding UPWs and UPW-related resources, please email webmaster@tamusa.edu.