1.0 Purpose

Montclair State University's web presence is essential to its mission of teaching, learning, and public service. However, any information published to a web server can potentially be viewed, copied, and redistributed by anyone who can access it via a web browser. Thus, the University's Web Publishing policy seeks to establish standards and guidelines that will:

- Support the vision, mission, goals, and traditional academic values of the University.
- Assist web publishers in developing sites that comply with university policies, rules, and regulations, and all applicable local, State, and Federal laws.
- Facilitate the official business of the University and appropriate online transactions while maintaining the necessary level of security and privacy.
- Outline mechanisms for maintaining the integrity and security of confidential/sensitive information that for legitimate business or pedagogical reasons must be stored on or accessed via a campus web server.
- Define web account creation policies to ensure that only those individuals with proper authorization can publish content to web servers in the montclair.edu domain.

This Web Publishing policy document is not intended as a style guide for the look and feel of web pages, nor does it address areas of web page design or branding. Please refer to the Division of University Advancement's Web Services page for guidelines pertaining to Montclair State's standards for web page design and branding.

Specific requirements for the proper protection and handling of sensitive and confidential information in any medium by members of the Montclair State University community are described in the University's Safeguarding Sensitive and Confidential Information policy document.

2.0 Scope

This policy document applies to:
• Montclair State University's official web site, http://www.montclair.edu
• All web pages located on servers within the montclair.edu domain.
• University-affiliated sites outside of the montclair.edu domain using approved MSU trademarked or copyrighted materials, images, logos, etc.
• Web pages of Application Service Providers (ASPs) or vendors that have contracted with the University to deliver online services. Examples include, but are not limited to, online learning management systems and vendor “portals” for procurement of equipment, services, and supplies.
• Faculty, staff, and student pages located on any server or device connected to the Campus network that is capable of delivering web content.
• Individuals who have been assigned custodial rights to a departmental web publishing account.

3.0 Policy

Web publishers are responsible for the content of the pages they publish and are expected to abide by the highest standards of quality and responsibility. These responsibilities apply to all publishers, whether they are colleges, departments, student or employee organizations, or individuals.

• All web content must conform to the University's Safeguarding Sensitive and Confidential Information policy document. Among other things, this means that sensitive University information including, but not limited to, student records, financial records, or any other confidential or private information may not be displayed on publicly-accessible web pages or stored on a web server in unencrypted form.

• Web pages may only be published to a server on the campus network using an IT-authorized user account. Examples of authorized user accounts include MSU NetIDs and any departmental or application-specific logins created by OIT for the purposes of web content publishing.

• All accounts used for web publishing shall conform to the University's Account Management and Password Management policies.

• Any web site or online form that requests a username and password for authentication must do so over a secure (SSL/TLS) connection for both the username/password entry and the actual form submission process. See Section 3.4 for more details.

• A web site's home page should clearly identify the person or unit responsible for its creation and maintenance. It is recommended that any sub-pages linked from the site's home page should contain similar information.
3.1 College and Departmental Web Pages

Non-OIT web servers that are maintained and operated by a college or department are subject to all University policies regarding server configuration, security, account management, and content as defined in the following policy documents:

- Network Connectivity Policy
- Account Management Policy
- Password Management Policy
- Safeguarding Sensitive and Confidential Information Policy
- Web Application Development Policy

At the University's discretion, College and Departmental web server may be included in the University's overall search engine indexing and web site statistics gathering processes.

3.2 Personal Web Pages

There are numerous services available on the campus community that facilitate the publishing of personal web pages. Some examples include:

- MSUWeb “public_html” folders available to all faculty, staff, and students with an active MSU NetID.
- Faculty/staff cover pages on the main University web site.
- The Blackboard learning management system (course content, student portfolios, discussion groups.)
- Various college and departmental web servers that allow personal web pages.
- Personal computers with web server software installed (note: access to these web servers is restricted by the University's firewall to on-campus traffic only.)

Individuals who utilize one or more of the above services to publish web content are subject to all of the policies herein, as well as all other University computing policies, and state, federal, and local laws.

3.3 Copyright

All web publishers are required to respect the intellectual and creative property rights of others and abide by all applicable policies and guidelines for fair use of copyrighted materials.

3.4 Online forms and Transactional Web Pages

Various colleges, departments, and Administrative units have a legitimate need to collect and process information using online forms and transactional web pages. Some examples include WESS online registration, applications for Financial Aid, Graduate School applications, event/seminar registration, and surveys. The following rules apply
to any online form or transactional web page, whether it is hosted on an OIT-operated web server, college or departmental web server, or an individual's web server.

- Individual (personal) web pages may NOT be used to gather personally identifiable information such as MSU NetIDs and passwords, Social Security numbers, home address, or any other personal identity information as defined by applicable state, federal, and local laws.

- Colleges, departments, and Administrative units needing to gather personal identity information may only do so using web forms or transaction systems that have been provided by OIT for this purpose, or have been evaluated by OIT for security and privacy compliance.

- Any online form or transactional web site must clearly state on the site what will be done with the information collected, and provide a link to the University's privacy policy.

- All transactional websites must comply with University policies regarding server configuration, security, account management, and content as defined in Section 3.1 above.

- Online forms and transactional web sites should only collect the minimum amount of information that is required to complete the form or transaction.

- Where possible, give users the option of not identifying themselves.

- Clearly state who is collecting the information and provide context so that users are aware why it is being collected.

- Use and disclose personal information only for the primary purpose for which it was collected, and in accordance with the University's Safeguarding Sensitive and Confidential Information policy.

4.0 Related Policies and Links

- Network Connectivity Policy
- Account Management Policy
- Password Management Policy
- Safeguarding Sensitive and Confidential Information Policy
- Web Application Development Policy
- Secure LDAP Authentication