UNM Digital Signage Standards
DRAFT (May 19, 2014)

Responsible Office: UNM CIO Office

Summary of Standard

The UNM community has a need for a central, enterprise-level digital signage solution to communicate to the community. This standard documents the roles and responsibilities of the University’s digital signage platform. The platform will be made available to all departments and campuses, and implemented in a way that is financially feasible for the University and its constituents. With this system the University can maintain consistent, updated content with a standard look and feel that enhances safety, facilitates way-finding, promotes events, bolsters the University’s reputation, and improves the campus experience. All members of the UNM community must follow this standard and associated UNM policies and procedures.

Who is affected by the Standard?

This standard applies to any UNM organizational entity (i.e. college, school, department, business unit, or other UNM affiliated organization), hereinafter referred to as a “department”, that intends to implement, or has implemented digital signage.

For new installations, departments must adopt the enterprise system. Departmental content will remain under the control of the individual units. Requirements outlined in this standard will automatically be available to each unit.

Departments that have existing digital signage systems will not be required to adopt the enterprise digital signage system. At time of renewal, departments should consider the following:

1) Costs
2) Support
3) Consistency of Institutional Messages
4) Scalability
5) Functionality

Existing systems must meet the content standards outlined in this standard.

If departments choose to adopt the enterprise system, migration assistance, licensing, and ongoing support will be provided by UNM IT. Departmental content will remain under the control of the individual units. If departments choose to retain/renew their existing system, they must show that their system satisfies all of the specifications and UNM policies noted below; or that the cost of their selection is equal to or significantly less than the University of New Mexico Enterprise Digital Signage solution; or that a core function within their unit can only be satisfied by their current system.
Why we have this Standard?

The Digital Signage Standard (DSS) enables the development of effective, scalable, secure and manageable signage deployments. This will enable campus wide communication and way-finding, and reduce total cost of ownership for individual departments.

Given the distributed nature of digital signage and the potential for wide use by the campus community, the purpose of this standard is to assure continuity, reliability, and sustainability of both services and resources.

- Be well-supported as an enterprise system
- Be accessible and affordable to all departments using existing purchasing mechanisms
- Feature updated content
- Be a safety communication tool for the entire UNM community
- Convey information about the University
- Provide current affairs and events to the University community
- Offer an opportunity for interaction that integrates with digital messaging (interactive displays, kiosks)
- Provide way-finding solutions for campus locations (main and branch campuses)
- Showcase student, faculty and staff achievements
- Provide sponsorship opportunities for internal constituents of the University
- Integrate with existing UNM systems for institutional information
- Maintain consistent branding

Responsibilities

1. Digital Signage Steering Committee (DSSC) - transition of UNM DS committee
   The DSSC works to improve communication and cooperation among the various University entities using digital signage. With broad representation from several units of the University, the DSSC is charged with:
   - maintaining the integrity of the University's digital signage
   - creating and recommending policies pertaining to digital signage
   - overseeing compliance with and reviewing requests for exceptions to the required elements of the Digital Signage Standards
   - provide guidance and support for policy and standard implementation
   - assisting campus entities in interpreting and adhering to standards
   - assisting with migration of existing systems
   - development of a digital signage template
   - shared infrastructure (such as content originating from other UNM and HSC enterprise data systems or other campus wide content)
   - working with UNM EOD to develop training resources

2. Functional Owner: Participating Colleges, Schools, Departments, and Units
   - must trigger and display all official emergency notifications issued by the University emergency system
   - help to implement the DSSC's decisions
   - submit all exceptions requests to the DSSC
   - see section above regarding compliance of system
- create, maintain, and approve departmental content
  - content currency
  - content accuracy
  - content appropriateness
- assign departmental access to the system
  - managing access
  - assigning training through EOD as needed
- if a digital display is not working, contact the Helpdesk to report the problem. Service will be prioritized according to the impact level.
- all functional owners will comply with all the following University policies:
  - Policy 1010 ("University External Graphic Identification Standards")
  - Policy 2500 ("Acceptable Computer Use Policy")
  - Policy 2520 ("Computer Security Controls and Access to Sensitive and Protected Information")
  - Policy 2550 ("Information Security")

3. Technical owner: UNM-IT
   - advises the DSSC on the tools and infrastructure appropriate to support the University's digital signage efforts and may also provide that infrastructure
   - advises the DSSC on security and confidentiality issues related to digital signage content
   - ensures connectivity to UNM data sources
   - assists in migration of existing systems
   - if on-premises, maintains digital signage system and ensures uptime response
   - responsible for maintaining the infrastructure and operation of the digital signage system.
   - responsible for incident management
   - managing user access for functional owners

4. Training: UNM Employee Organizational Development (EOD)
   - develop and conduct training resources on creating content
   - develop and conduct training on workflow/approval processes

Specifications

1. Campus Emergency Alert System
   a. Must have an Emergency Alert Override function
   b. Tie into UNM Emergency system
   c. Support Common Alerting Protocol (CAP) compliance
2. ADA Compliancy regarding digital signage
3. UNM Brand Identity Consistency
4. Individual targeting of displays as well as administrative override for all University displays
5. Integration with multiple institution data sources (see list of UNM data sources in appendix)
6. Support for Interactivity (e.g. way-finding)
7. Web-based Content Management
8. Reporting
   a. Frequency of Content Playback
   b. Date/Time Grouping
   c. Access Lists
   d. Library Catalog
   e. Error Messaging
   f. Audit History
   g. Workflow Approval, Status
   h. System Usage
   i. Standard Reports

9. User Management and Restrictions
   a. If the digital signage system requires distributed management, integration into UNM Active Directory Services / LDAP
   b. All interaction with the proposed solution must be managed through individual user accounts with authenticated access

Procedures

- Procedures are described in the UNM Digital Signage Service Level Agreement

Exceptions

The Digital Signage Steering Committee (DSSC) evaluates and makes recommendations on requests for exceptions to this standard.

Website for this Standard

http://cio.unm.edu/standards/

Related Documents and References

A. UNM Digital Signage Committee Report
B. UNM Data Sources
C. UNM Digital Signage Service Level Agreement
D. UNM Planning & Campus Development Way-finding and Signage Guidelines
E. Policy 1010 ("University External Graphic Identification Standards")
F. Policy 2500 ("Acceptable Computer Use Policy")
G. Policy 2520 ("Computer Security Controls and Access to Sensitive and Protected Information")
H. Policy 2550 ("Information Security")