UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	System Banner Standards
Standards Number:	107
Effective Date:	05-01-18
Revised Date:	07-24-18
Responsible Authority:	Information Security Office
Pages:	4

ACCOUNTABILITY/APPLICABILITY:

System banners should be implemented on any UCF system. This standard is for system administrators and owners responsible for the implementation and maintenance of UCF systems. The standard outlines different banners for end user systems versus systems that perform administrative or critical functions that are not end-user in nature.

STANDARDS STATEMENT:

System banners are critical to inform potential users of a system of the terms, advisories, and consents under which they agree to use the system. These can include university policies and regulations as well as state and national laws. Further, it indicates their consent to monitoring of their usage. Finally, they outline possible consequences to violations and other unacceptable use. The UCF Information Security Office has developed the following statements to meet this need.

STANDARDS:

1. All banners must be placed such that users must read and agree before access to the system is granted.

2. The following banner text must be used for end-user systems:

UCF System User Agreement

> This UCF system is for authorized users only. Anyone using this system expressly agrees and adheres to the university's policies (including Acceptable Use Policies and information security policies), regulations, and all other applicable laws, including but not limited to Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA). Be advised, that your usage of this system implies consent to possible monitoring and auditing of activities on this system. If such monitoring reveals possible evidence of criminal activity, system administrators may be obligated to provide the evidence of such monitoring to University Administration or law enforcement agencies. Any violation may result in immediate loss of network and computer access privileges, seizure of equipment, or removal of inappropriate information posted on university-owned computers or university-supported Internet sites. In addition to these corrective actions, failure to comply with these policies and procedures may result in disciplinary action up to and including termination.
>
> For further information on the laws and policies referenced, please visit:
> https://policies.ucf.edu
> https://ed.gov/policy/gen/guid/fpco/ferpa/index.html
> https://www.hhs.gov/hipaa

3. The following banner text must be used for systems that perform administrative or otherwise critical functions that are not end-user in nature.

> WARNING! THIS SYSTEM IS THE PROPERTY OF UCF. AUTHORIZED USERS ONLY.
>
> This UCF system is for authorized users only. Authorized users of this system expressly agree to and adhere to the university's policies (including Acceptable Use Policies and information security policies), regulations and all other applicable laws. Be advised, that your usage of this system implies consent to monitoring and auditing of activities on this system. If such monitoring reveals possible evidence of unauthorized use, violation of policy, or criminal activity, system administrators may be obligated to provide the evidence of such monitoring to University Administration or law enforcement agencies. Any violation, failure to comply with these policies or procedures, or unauthorized use of any kind may result in immediate loss of network and computer access privileges, seizure of equipment, and may result in disciplinary action up to and including termination.
>
> For further information on the laws and policies referenced, please visit https://policies.ucf.edu.

DEFINITIONS:

Authentication: The process of establishing confidence in user identities electronically presented to an information system.

Information system: A collection of hardware and software components and interconnections, as well as the information contained with them.

System Banner: A message to inform users of an information system of information they need to know before use of the system can begin.

RELATED DOCUMENTS:

- 4-008.1 *Data Classification and Protection* policy
- NIST 800-53 Rev4: Control AC8 – System Use Notification
    - https://nvd.nist.gov/800-53/Rev4/control/AC-8

CONTACTS:

Information Security Office
https://infosec.ucf.edu
infosec@ucf.edu

UCF IT Support Center
(407) 823-5117
https://ucf.service-now.com/ucfit
itsupport@ucf.edu

Identity Access Management (IAM)
https://infosec.ucf.edu/iam
iam@ucf.edu

Security Incident Response Team (SIRT)
https://infosec.ucf.edu/incident-response/
sirt@ucf.edu

Revision Date	Summary of Change
06-28-18	Formatting
07-24-18	Added secure link to policies.ucf.edu page

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *107*

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv Digitally signed by chrisv
Date: 2018.07.31 10:15:11 -04'00' Date: ____________