

# UCSC Password Policy

## Vice Chancellor, Information Technology (Policy IT-0002)

### I. Purpose/Scope

The purpose of this policy is to establish the applicability of, and specific responsibilities relating to, the *UCSC Password Strength and Security Standards*<sup>1</sup> (Password Standards).

### II. Detailed Policy Statement: Applicability and Responsibility

#### APPLICABILITY

- A. The UCSC Password Standards become requirements for passwords that provide access to University restricted data<sup>2</sup>, or where otherwise required by law, UC or campus policy, or contract.
- B. The Password Standards are also recommended for passwords that provide access to other types of confidential information.
- C. Passwords that do not provide access to confidential information, and do not share an Authentication System with ones that do, are not required to comply with the Password Standards.

#### RESPONSIBILITY

System Stewards<sup>2</sup>, in consultation with Subject Matter Experts<sup>2</sup>, where appropriate, are responsible for determining the applicability of the Password Standards to systems or data for which they are responsible based on the above criteria<sup>3</sup>. In situations where it is not clear whether the Password Standards apply to a certain type of data or system, the System Steward shall err on the side of more secure password requirements. System Stewards are also responsible for ensuring implementation and enforcement of the Password Standards where they are applicable. This includes informing users of password requirements.

System Stewards of Authentication Systems (e.g. systems, such as an identity management system, that allow the same username/password to be used for access to multiple services) are responsible for including in their service definition the minimum level of protection required for passwords provided by their system(s), and for communicating this information to other System Stewards.

All individuals are responsible for following the Password Standards where required. This includes not using passwords that provide access to confidential information with other systems or applications that do not adhere to the Password Standards.

---

<sup>1</sup> See Attachment

<sup>2</sup> See Definitions

<sup>3</sup> If a System Steward relies on an Authentication System, e.g. an identity management system, it is the responsibility of the System Steward to include password protection requirements of the Authentication System in this assessment.

### III. Authority

The campus Vice Chancellor, Information Technology on behalf of the Office of the Chancellor and the Office of the Campus Provost and Executive Vice Chancellor (CP/EVC) is the campus authority for the *UCSC Password Policy*. This policy was initially reviewed and approved by the CP/EVC on 2/11/2007. Next review date is 2/11/2009.

### IV. Getting Help

For questions or feedback about this policy, contact the ITS Service Manager for Community and Compliance at [itpolicy@ucsc.edu](mailto:itpolicy@ucsc.edu) or (831) 459-2779.

### V. Definitions

The following terms used in this policy are defined in the online *Glossary of selected terms in UCSC IT-related policies, procedures and guidelines*, available at <http://security.ucsc.edu/policies/glossary.shtml>.

Confidential Information  
Restricted Data  
Subject Matter Expert  
System Steward

### VI. Related Policies/References for More Information

#### References

*UC Business and Finance Bulletins - Information Systems (IS) Series:*  
<http://www.ucop.edu/ucophome/policies/bfb/bfbis.html>.

#### Related Legislation and Policies

*Federal Privacy Act of 1974 - Public Law 93-579 (5 U.S.C. 552a)*  
<http://www.usdoj.gov/oip/privstat.htm>

*State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)*  
[http://www.oispp.ca.gov/consumer\\_privacy/laws/code/ipa.asp](http://www.oispp.ca.gov/consumer_privacy/laws/code/ipa.asp)

*State of California Public Records Act (Gov. Code Section 6250 et seq.)*  
[http://www.oispp.ca.gov/consumer\\_privacy/laws/code/pra.asp](http://www.oispp.ca.gov/consumer_privacy/laws/code/pra.asp)

*UC Business and Finance Bulletins - Records Management and Privacy (RMP) Series:*  
<http://www.ucop.edu/ucophome/policies/bfb/bfbrmp.html>

### VII. Attachments

UCSC Password Strength and Security Standards:  
<http://security.ucsc.edu/policies/password.shtml>