

Identity Management Security Policy/Practice Questions, Decisions and Feedback
IT Security Committee
August 17, 2005

<i>Policy/Practice</i>	<i>Recommendation</i>	<i>IT Security Committee 6/29/05 Decision</i>	<i>Feedback</i>	<i>Recommendation to Committee 8/17/05</i>
PASSWORDS Required strength: What minimum standards should we require for passwords?	Require a password with a minimum length, mixed case characters and non-alphabetic characters. Require non-dictionary words, non-inclusion of user name and other similar restrictions. Exact mix of characters TBD working with Security team, Audit and any other appropriate staff.	Start with recommendation as stated and work toward more flexible password strength checker with recommendations as guidelines.	None	Final approval of 6/29/05 decision for current implementation. Recommend future update on more flexible password strength checker.
PASSWORDS Password Expiration: Should we require passwords to expire after a certain amount of time? (And what amount of time)	Do not require expiration at this time. Once we've worked out how to deal with expirations we can do an expiration process at that time, if desired.	Passwords don't expire unless there is a legal requirement.	None	Final approval of 6/29/05 decision.
ACCOUNT ACTIVATION This is the process of delivering the initial account information to the user. Especially relevant for accounts created automatically (e.g., from data in AIS or PPS).	Recommendation varies slightly based on audience. Can be summarized as: Either deliver password directly to user, or require user to enter information unique to them and known to IdM. E.g., account name, an ID (Student ID, Employee ID, etc.), combined with name, DoB, SSN or other known data elements.	Accept recommendations for people in source systems only. No use of SSN.	Recommended a large activation window, especially for applicants, as applicants may not need to activate their account for months after it is created.	Final approval of 6/29/05 decision with clarification of a large activation window for applicants.

<i>Policy/Practice</i>	<i>Recommendation</i>	<i>IT Security Committee 6/29/05 Decision</i>	<i>Feedback</i>	<i>Recommendation to Committee 8/17/05</i>
<p>PASSWORD RESET The "I forgot my password" process.</p>	<p>When account is initially activated, prompt user to provide answers to a number of specific security questions (exact questions to be developed) and to provide a third party (non-@ucsc.edu) email address that will be used ONLY for password recovery purposes. If the user wishes to opt out of the online password reset process, they can opt to not answer these questions.</p> <p>When a user wishes to reset a password, require entry of some identity data (if available – we may not have this information for guests); e.g. EID, DoB, etc. Also challenge the user to answer one or more security questions (initially seeded above). Finally, in email to the third party (non-@ucsc.edu) email address with information that is required to complete the process. Require the user to provide all of these pieces of information (identity data, security questions, and data from the email) at the same time. If all are correctly answered, allow the user to change the password. Send notice of the password change to both their UCSC email address (if one exists) and their 3rd party address.</p>	<p>Use three security questions that users have provided answers to previously. (Provide 4-5 total questions). Faculty and Staff are not permitted to use this process, and would require an “in-person” reset. Recommend identifying delegated staff who are also allowed to do resets for faculty and staff (e.g., IT field support staff).</p>	<p>From IdM Steering:</p> <ul style="list-style-type: none"> • Not using a 3rd party email account as part of the process reduces the security threshold • Concerns that a student will remember the exact answers to 3 questions. If too difficult this could mean the automation is less effective. • The requirement that faculty and staff must contact an individual means greater delays for these individuals, even if the number of people able to perform password resets is increased. <p>From AIS: For password resets, it would be best to use automation as much as possible. Nearly 98% of our applicants and students have an external email address. When a student forgets their password, they should be queried for authentication and on a match, the new password is emailed to them at their non-UCSC email. This would eliminate help desk intervention and provide a secure method for sharing the password.</p> <p>The method we do not support is one that immediately shows the person the password on the screen or allows them to immediately reset it without using their email account. This method could be compromised, particularly by parents. By sending it to an email address, it provides another layer of security. Allowing the student to define their own questions (rather than using preset questions) would give a student the opportunity to choose more secure questions, but the security is still less predictable than using the students personal email address.</p> <p>Others: As the password being reset allows access to more systems, increasing the number of people with access to reset passwords is a potential security concern.</p> <p>Implementation Note: complex changes may not be possible to implement before fall 2005.</p>	<p>Final approval of 6/29/05 decision for current implementation.</p> <p>Recommend future update on proposals to address concerns about security and automation.</p>

<i>Policy/Practice</i>	<i>Recommendation</i>	<i>IT Security Committee 6/29/05 Decision</i>	<i>Feedback</i>	<i>Recommendation to Committee 8/17/05</i>
<p>SESSION TIMEOUTS This addresses how long a user who is logged in but is idle should be allowed to maintain their login session.</p>	<p>Ideally we will allow "role based" session policies, where we can limit your access based on whether or not you are a student, faculty, etc. However, at this point we are still investigating the capabilities of the product, and cannot say for sure whether this will be feasible.</p>	<p>Issue was raised, but no decision was made at this point.</p>	<p>None</p>	<p>Recommend proposals when capabilities of product are known.</p>