MINUTES
IT Advisory Committee Meeting
May 28, 2009
8:30-10:00 AM

Present: Dr. Stephen Balfour, Andy Bland, Dr. Becky Carr, John Chivvis, Dr. Fred Fisher, Steven Conway, Jim Culver, David Sweeney, Dave Jennings, Ron Szabo, Dr. Henrik Schmiediche, Khalid Sarwar Warraich, Lacey Baze, Willis Marti, Allison Oslund, Jeff McCabe

Item 1: IT Training Update
A. Becky Carr updated the committee on the IT vendor selections.
   • Becky’s committee heard the vendor presentations last week and has narrowed it down to
two: Global Knowledge (Houston) and St. Edwards (Austin).
   • The vendors have agreed to reach out to the campus to find out the training needs. They will
also tell the campus about upcoming training opportunities.
   • The vendors will only need a conference room with electricity to conduct training and will
provide the other materials (laptops, connections, etc.).

Item 2: Authentication Changes Update
A. Identity Management
   • CIS is working to provide an identity management system to gain control over the handling
of user IDs and passwords. This will centralize password storage into one repository that is
not recoverable. Announcements and policies are being drafted to decrease the number of
places where NetIDs and passwords can be stored.
   • Users of CAS3 will have to identify themselves so that CIS can check their system’s
soundness. Screen scraping will not be allowed. CIS will provide local options such as
passwords.
   • The system is needed because a lot of systems scrape credentials and use them to
authenticate in another system. It is insecure to have recoverable copies of these credentials
floating around.
   • CAS3 doesn’t work well with Active Directory.
   • This change will take place within the next year, but not before September.
   • Guest access will be granted in a timely fashion once approved by the appropriate authorities.
There will be an option to grant year-long access, but it will have to be revisited each year.
   • Guest wireless access accounts should be created within 15-20 minutes before the end of the
summer.
   • The ability to do reverse lookups has yet to be decided. The user may not be able to do it
manually, but should be able to contact someone else to do this
B. LDAP vs. Shibboleth
   • LDAP is the underlying data storage.
   • Shibboleth is a mechanism to request information and is designed to be federated between
separate trust organizations. Currently software.tamu.edu uses it.
   • LDAP and CAS use the same directories, but LDAP is the authoritative source.
   • Willis was asked to create a picture of how all of these systems work.
   • An identity management workshop will be held this June for 24 people across campus to get
an idea of the problem from a policy/procedural prospective (not technical). More workshops
will follow.

Item 3: Survey
A. Survey Observations
• We still need to get the survey results for the questions “What is confidential data?” and “How do you protect confidential data?”
• Encryption should be the standard we measure against.
• Willis supports any further surveying, and the committee thinks this would be appropriate after some education/SAPs have been into place.
• The committee stills sees a problem with the ability to encrypt confidential data. Their Identity Finder scans revealed confidential data, but they have no software to encrypt it.
• The State will not allow us to have our own definition of confidential data, but we can give examples.
• Ron Szabo had his department fill out and sign a form about what data they have and where they are storing it before he ran his scan.
• A lot of faculty store confidential data on personal desktops.
• Any SAP that prohibits storage of confidential data on personal devices will not work.
• Change text of scanning form to “Request for exception to maintain Social Security Numbers” and explain that the request must be approved.
• Department heads will eventually have to sign a form about the scan. Willis will resend the form reminding them that they have to scan.

B. Survey Report
• An executive summary should appear at the front at the report.
• The problem should be defined as well as the scope of our report.
• Recommendations for how to solve the problem are still needed.
• Focus on the data, not what device. Don’t exclude desktops.
• Create a list of examples of confidential data.
• Educate entire campus about confidential data and provide tools/training for them to protect it. Don’t focus on portable devices.
• Announce SAP to department heads. Recommend departments follow best practices that are already in place for data storage on desktops at work.
• Mandatory training for how to protect confidential data.
• Review current SAP and define the position of what the university already has in place.
• Create best practices for data storage on portable devices.
• Willis: Requirements for working with confidential data, protection mechanisms, and time and place restrictions.