Comments - Security Related Documents

Comment #1
I was trained to be an ISO9000 lead auditor about ten years ago, and I have found that training to be very useful in many areas of my life even though I only worked with it for a few months. I continue to have an interest in quality standards, and like to contribute if I can.

I remember reading through some records retention standards while I was at DAS-Personnel. They might be useful to look at in creating the NITC Data Classification Standard, since they have already classified many types of information in them.

Thanks,

Brad Finch
IT Business Systems Analyst
NDOR - Materials and Research

Comment #2
In the password standard document, point 1.1 states...
Must not repeat any character sequentially more than 2 times.

RACF can't enforce it without an exit, which I prefer to avoid coding.
Besides that, I believe the statement is ambiguous, e.g., AAbbCC22 might be viewed as invalid, as could AAAbcde1. My recommendation would be to remove that requirement.

Fred Lupher
Enterprise Computing Services
Office of the CIO
State of NE

Comment #3
We are in complete support of the strong password/frequent password reset policy for granting access to State network resources. Where I began to get uncomfortable with the proposal is when I realized that it's intended to also apply to applications that reside outside the State firewall (in an appropriately designed dmz).

I am confident our internal customers will have significant concerns with this, and I don't believe addressing them through the NITC exceptions policy is the correct method of handling them. Generally, the NITC exceptions tend to be for legacy systems, and granted until such time as a revision or replacement to the system occurs. In a couple of instances in our environment, I'd expect our customer requirements in the event of a rewrite to include less stringent password policies. In both cases, the end users is accessing only resources that reside in a dmz - and thus has no direct access to the State network. Here's some examples;

Our UIConnect application is used by employers to pay Unemployment Insurance taxes, file associated reports, and set up new accounts. We purposely use a pin, which is refreshed and sent to the employer each quarter, for access. During the initial design of the system we had extensive debate regarding authentication, including a review of risk. The conclusion, there is little risk - few people will try to pay taxes they don't owe, and the repair to incorrect information in the system is inexpensive and doesn't have long term impact. The advantages of having a simple authentication are large in terms of employer support, and in terms of reduced cost of government. I know our business unit has a goal of having essentially all taxes filed through this

self-service application in the future. A strong password on a 90 day refresh would significantly hamper their ability to achieve that goal...

Our Nebraska JobLink Application is used by job seekers to search and apply for jobs, and to post resume's for employer review, as well as used by Employers to search for applicants and post jobs available. Again, this application provides an important service, reduces the cost of delivering government services, and we believe would see a reduction in usage with a strong password - frequent reset policy.

Both applications sit in a dmz - the purpose of which is to protect network resources. I'm wondering if applying the strong password requirements to services of this type is a case of requiring both belt and suspenders....

Thanks for your consideration - please let me know if you have questions.

Robert Shanahan, Executive Director
Office of Information Technology
Nebraska Workforce Development - Department of Labor
402-471-2518

Comment #4
1. Password policy
(http://nitc.ne.gov/standards/comment/Password_Standard_20070814_comment.pdf)
While having strong passwords can be an inconvenience to our staff, it is important to remember the kind of data that these passwords help safeguard... Nebraskan's social security numbers, personal information, and in some instances systems that access their bank accounts or credit card numbers. Good passwords are an important step in doing our due diligence in protecting that data.
One thing that may help users is to use passphrases, as opposed to passwords. Some users are under the impression that a strong password must resemble the cryptic form of /#*aKj8$, which forces them to write it on a nearby paper. A passphrase such as MyN@me15T1b0r (my name is tibor) are just as secure and much easier to remember.

2. Information Security Policy
(http://nitc.ne.gov/standards/comment/ITS_Security_Policy_2007_20070814_comment.pdf)
I like the open-ness of the document. It is a very nicely written and all-encompassing, dealing with many areas that security-minded sysadmins are aware of, but unfortunately many of our peers may not be. This document brings important information to all IT personnel and points out the things we should all be paying attention to.

None of us would like to see our name on the top half of the newspaper one morning and having to explain to media how we lost personal data on 50000 Nebraskans and businesses, and these 2 documents , as well as the data classification one go a long way towards protecting all of us.

Tibor Moldovan

Infrastructure Support Analyst
NDE Vocational Rehabilitation Services
402.471.1201

Comments from Informational Meetings

Comment #5
Information Security Policy

1. Remove the word 'Broad' in the 3rd paragraph on pg. 4 Change the phrase "must be used for state business only" to read "must be used for official business only". (pg. 7
2. Sharing Information Outside of the Agency.
    a. Add " within the control of the agency. Now reads" For information (that lays within the control of the Agency) to be released…"
    b. Strike "Sensitive or Confidential" and replace with "Non-public" – confusion on the multiple uses of the word confidential
3. Agency Accountability (pg. 8-9)
    a. Replace 'Sensitivity' of that information to read "classification' of that data
    b. Strike Backup plans (bottom of page 7) and replace with Disaster Recovery (DR) and Business Continuity Plans (BCP)
    c. Strike backup of critical data, to read "Preservation of critical data
4. User Training – Delete developed from the first line.
5. Monitoring Pg. 10 – Rework
    a. Old: Only qualified agency staff or third party individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use 'sniffers' or similar technology on the network to monitor operational data and security events on the State network.
    b. NEW: Only individuals with proper authorization from the Office of the Chief Information Officer will be permitted to use 'sniffers' or similar technology on the network to monitor operational data and security events on the State network.
6. Equipment Security: Strike "… in accordance with DAS fixed asset guidelines"

DEQ

Comment #6
Information Security Policy

User Authentication for External Connections (Remote Access Control) – Pg. 14
What about Windows Update services? Java updates? Adobe? Are these covered under this section?

NIS CNC

Comment #7
Information Security Policy

Section 3: Agency accountability – Pg. 14; "Add a reference that recovery plans should be tested on a regular basis, and those tests documented."
Section 6 – Delete "when classifying data…
Section 9 – Change Control Management – Needs a standard to Guideline spell this out in detail.

Password Standard

Applications that are available only once you have authenticated to the state's network (e.g. - a domain or LAN) should be allowed to use non-expiring passwords as allowed in 1.2

Randy Cecrle – WCC

Comment #8
Information Security Policy

Section 6 –
Spell out GLB, HIPAA, FERPA

Janette Lee – Banking

Comment #9
Data Security Standard

Check court rulings on the use of “Data Owner” and “Data Custodian”

Mike Overton – Crime Commission

Comment #10
Information Security Policy

Pg. 10 Monitoring - The Legislature will likely have some uneasiness over the privacy of their stored data.

Change data owner to data owner(s) throughout the document

Addendum A
Data Owner definition uses the term “data owner”

Old: An individual or group of individuals designated by the agency will serve as or represent data owners for the data and tools they use.

Proposed: An individual or group of individuals designated by the agency by an agency who will represent the agency concerning the data the agency owns and tools the agency uses on the data.

Gary Wieman - Legislature