STATE OF INDIANA

Mitchell E. Daniels Jr., Governor

OFFICE OF TECHNOLOGY
Gerry Weaver
Chief Information Officer

Indiana Government Center North
100 N. Senate Ave., Room N551
Indianapolis, IN 46204
(317) 232 - 3171

TO: State IT Directors

FROM: Tad Stahl, State Chief Information Security Officer

RE: Increasing Password Security

DATE: February 6, 2007

I write to inform you of our move to increase password security across IT in state government, which will affect our businesses partners—the end users—early next year.

Today, the State has multiple IT systems with different user names and passwords for the same user, different intervals for password change, and varying levels of minimum password complexity. This is primarily due to the formerly decentralized nature of IT management in state government before this administration. Our IT consolidation, however, has positioned us to correct this, and over the course of this year we have audited and analyzed state IT security. Increasing password security is a fundamental step to increasing the security of state data.

During this quarter we will move to "complex" passwords (requiring numbers and special characters) at a 90 day interval. (This is up from the 30 day interval used on some systems.) There are good reasons for this move, including:

- A 90-day interval *with* complex passwords combine for a significant security improvement because the period is long enough for people to memorize their password and complex enough not to be easily hacked. This move puts the State in the company of private and public sector entities, such as the FBI, using this same standard practice.
- We are working to integrate usernames and passwords of multiple systems, including Active Directory (*i.e.*, your computer login) and PeopleSoft. (A requirement for this is a consistent password change interval.) Such integration will improve security through easier user password management.
- The increased interval from 30 to 90 days will result in fewer password reset requests to our Customer Service Desk. (In November, IOT took 15,000 calls for password resets.) Lowering the number of reset requests, frees resources for higher value work.

To ensure a smooth transition, we will roll this out in coordination with you and your staff. Please let me (tstahl@iot.in.gov) know if you have any questions or concerns.

For more information about password management, please visit the IOT Security website.