PURDUE UNIVERSITY

USER CREDENTIALS STANDARDS
Developed to support the implementation of the Authentication and Authorization Policy (VII.B.1)

.

Issued October 13, 2008 (rev. June 30, 2011) from the Identity and Access Management Office.
Questions about these standards can be addressed to iamo@purdue.edu.

I. Introduction:

Purdue University will assign a Purdue University Identifier (PUID) and User Credentials for Identification and Authentication purposes to each individual that has a business, research, or educational need to access University IT Resources. All users of Purdue University IT Resources are responsible for taking appropriate steps, as outlined herein, to select and secure their User Credentials.

II. Passwords

Passwords are a User Credential that represents an important aspect of IT Resource security. They are often the first level of protection for University IT Resources. A poorly chosen password may result in the compromise of University IT Resources, University data, and user data.

Password Requirements:

Passwords may be used only by the authorized user. Passwords or accounts should never be shared with anyone, including trusted friends or family members. Account owners will be held responsible for any actions performed using their accounts. Purdue University IT staff will never ask users to disclose their passwords in any manner.

Passwords for University IT Resources must comply with the following standards:

- Passwords must contain at least 1 letter.
- Passwords must contain at least 1 number or punctuation mark.
- Passwords must be between 8 and 16 characters long.
- Passwords must contain more than 4 unique characters.
- Passwords must not contain easily guessed words (e.g. Purdue, itap, boiler).
- Passwords must not contain your name or parts of your name (e.g., Bill, Julie, Bob, or Susan).
- New passwords must be different than the previous password (re-use of the same password will not be allowed for one (1) year).

In addition, passwords must not be inserted into e-mail messages or other forms of electronic communication without the use of encryption.

Passwords should never be written down and left in plain sight, or stored in plain text online. If a password must be written down, it should be stored in a secured location.

The use of group accounts for administrative purposes and shared passwords for those accounts should be minimized where technically feasible. In situations where group accounts for administrative purposes and shared passwords for those accounts is required (e.g. "Root" or "Administrator" accounts), the passwords used must follow the standards stated in this document and must be changed every thirty (30) days and immediately upon any personnel change within the group.

Password Expiration:

All University IT Resource passwords must be changed at least every 365 days. Except for student-employees, as indicated below, all students must change their passwords at least every 365 days.

All faculty, staff, student-employees, and other affiliates having any privilege other than those base roles designated below in either the OnePurdue/SAP or the myPurdue/Banner system will be assigned a 90-day password expiration cycle in both the OnePurdue/SAP and the myPurdue/Banner systems:

System Name	OnePurdue/SAP Portal	myPurdue/Banner
Base Roles	• R3:COMMON_ALL_USERS • FI900_000_END_USER_GENERAL • TV200_000_TRAVELER • HR280_000_EMPLOYE_SELF_SERVICE • SM200_000_REQUISITIONER • SM235_000_COMMON • SM800_000_REPORTING • HR285_000_MANAGER_SELF_SERVICE	• Student • FacultyPU

Entire University academic or business departments may also implement a 90-day password expiration requirement if there are special departmental circumstances that require a shorter password expiration cycle.

III. Two-Factor Authentication

Two-factor authentication (TFA) offers inherently greater security than reusable passwords. TFA utilizes a "something you have and something you know" method of authenticating users. The "something you have" is a hardware device such as a token or smart card, and the "something you know" is a PIN (personal identification number, or alphanumeric code). The combination of the hardware device and the PIN authenticates users to systems.

Two-Factor Authentication PIN requirements:

A PIN used for University IT Resources must be at least 4 characters long.

A PIN used for University IT Resources should be created with the following best practices in mind:

- A PIN should avoid easily guessed sequences such as "1234" or "abcd."
- If the PIN is numeric, it should not contain information identifying you such as Social Security Number (SSN), PUID, or other information publicly obtainable about you.
- If the PIN is alphanumeric, it should contain both characters and numbers.
    - If alphanumeric, a PIN should not contain easily guessed words.
    - If alphanumeric, a PIN should not contain your name or parts of your name, or information publicly obtainable about you (e.g., address, phone number, office number).
- A changed PIN should be substantially different from the previous PIN.
- A PIN should not be the same as your University voicemail PIN.
- A PIN should be memorized.
- A PIN should not be reused within one year.

In addition, TFA devices of all kinds (tokens, smart cards, etc.) should be safeguarded and kept with you at all times. If your TFA device has been lost or stolen, report it to your supervisor immediately.

PIN Expiration:
There is currently no requirement to change the PIN on a TFA device. However, the longer a PIN remains unchanged, the greater the risk of certain types of attacks. The IAMO recommends that PINS be changed at least yearly.

IV. Compliance with User Credentials Requirements

Users of University IT Resources must comply with this standard, related standards, and expiry periods issued by the University in support of this standard and the Authentication and Authorization Policy.

Additionally, users are responsible for safe handling and storage of all University passwords and TFA devices, such as tokens, ID cards, and smartcards. The use of a "password vault" or other similar software application is considered an acceptable secure storage mechanism for passwords and PINs.

If you suspect that one of your Purdue University User Credentials has been compromised, it should be changed immediately. The unauthorized use of computer accounts is a violation of University policy and it may also be a violation of Indiana law. If you know or suspect that someone else was or is using your account, you should complete the information on the SecurePurdue Incident page at:
http://www.purdue.edu/securePurdue/incidentReportForm.cfm

Centralized and departmental authentication services will be used to automatically check, where technically possible, user credentials used for authentication to University IT Resources based on the standards for creating strong user credentials at the time a user changes their user credential. Expiration periods will also be automatically enforced where technically feasible. If, in the opinion of authorized staff, a user credential in violation of current standards is detected or the user credential is in use beyond its expiration period, the user will be required to change it.

V. Related References

- Authentication and Authorization policy (VII.B.1), available at: http://www.purdue.edu/policies/information-technology/viib1.html

- University IT Policies are available at: http://www.purdue.edu/policies/information-technology.html

- Standards supporting the implementation of this and other University IT Policies are available at: http://www.purdue.edu/securepurdue/bestPractices/

- Purdue University Data Classification and Handling Requirements, available at: www.purdue.edu/securepurdue/bestPractices/dataClass.cfm

Issued October 13, 2008 (revised June 30, 2011) from the Identity and Access Management Office (IAMO). Questions about these standards can be addressed to iamo@purdue.edu.

Revised June 30, 2011 to include an additional role in the list of base roles for password expiration.

Revised November 21, 2011 to update URLs.

Revised November 8, 2013 to update password expiration.

Revised December 9, 2014 to update password requirements.