

## **ACCESS CONTROL STANDARDS**

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

### I. Introduction:

Identification, Authentication, and Authorization are controls that facilitate access to University Information Technology (IT) Resources. Purdue University uses access controls and other security measures to protect the confidentiality, integrity, and availability of University data maintained in University IT Resources. Each IT Resource owner is responsible for ensuring that access control standards are followed for their respective IT Resource(s).

### II. Access Control Standards:

To the maximum extent possible and where technically feasible, authentication, authorization and access control practices for University IT Resources must address the following standards.

#### Identification Standards

The Purdue University Identifier (PUID) number is a ten-digit identification number and is assigned to each person based on his or her unique relationship with the University. A person's PUID identifies the person to Purdue University's computer-based, service-provider application programs. A PUID will be assigned to each individual that has a business or educational need to access University IT Resources, but a PUID alone is not sufficient to access University IT Resources.

- A PUID will be assigned to all prospective students at the time of application to the University.
- A PUID will be assigned to all employees of the University at the time of employment.
- All contractors, consultants, or other non-employees, who must be granted User Credentials in order to fulfill a business, education, and/or research obligation to or on behalf of Purdue University, must follow the "Request for Privileges" process. A PUID will be assigned once that process is complete.

A PUID is not the same as a Purdue Career Account. A Purdue Career Account gives an individual electronic access to a number of services at Purdue University, including services for email, instructional, ResNet, research, and departmental use. All Purdue students, faculty, and staff receive a base set of Purdue Career Accounts and such base access may include different services depending upon a person's affiliation with the University.

- A Purdue Career Account will automatically be assigned to all faculty and staff at the beginning of their employment period, and to students upon offer of admission to the University.
- A Purdue Career Account may be assigned to an individual that has a business, educational, or research need to access University IT Resources, but is not a faculty, staff, or student at the University. This access is subject to quarterly review through Human Resource Services.

## Authentication Standards

- Departments and units are strongly encouraged to use the Purdue Career Account for authentication purposes for all non-public IT Resources.
- Authentication credentials for Purdue IT Resources will not be coded into programs or queries unless they are encrypted, and only when no other reasonable options exist, and must follow the User Credentials Standard for password expiry. A security policy exception request is required in order to code authentication credentials into programs or queries if unencrypted.
- The PUID must be used with appropriate authentication credentials. By itself, the PUID must not be used to gain access to any private information or non-public IT Resource.

## Authorization Standards

- IT Resource owners must establish specific authorization privileges in accordance with University Policy for IT resource access.
- Only the minimum privileges necessary to complete required tasks shall be assigned to an individual.
- Privileges assigned to each individual must be reviewed on a regular basis, and modified or revoked upon a change in status with the University. When the privileges assigned to each individual change (e.g. due to a change in role or responsibilities), access to University IT resources must be adjusted accordingly.
- Privileges must be established such that system users are not able to modify production data in an unrestricted manner. System users may only modify production data in predefined ways that preserve or enhance its integrity. In other words, system users must be permitted to modify production data only when employing a controlled process/system approved by management.

## Access Controls, General

- Access controls will be accompanied by mechanisms to detect, record, and generate alerts about repeated failed attempts at access to University IT Resources in accordance with the University's IT Resource Logging Policy.
- Access controls must include account lockout capabilities, including a maximum number of login attempts and a lockout time duration.
- Access control permissions for all non-public Purdue University IT Resources must default to no access, which blocks access by unauthorized users.
- IT Resources should be designed to default to no access (denial of privileges to end-users) in the event of a malfunction.
- Access to IT Resources must use password-protected screensavers whenever and wherever possible; access to such resources should time-out after a 15 minute or less period of inactivity.
- Testing or attempting to compromise internal controls, when outside of the scope of an individual's employment duties with Purdue University, is prohibited unless specifically approved in advance and in writing by the Office of the Vice President for Information Technology.
- All contractors, consultants, or other non-employees must only be given access privileges to IT Resources when the IT Resource owner, or his or her designee, determines that they have a

legitimate business need. These privileges must be enabled only for the time period required to accomplish approved tasks and then promptly disabled upon completion of the approved tasks.

Access Controls, Remote Access

Secure remote access to University IT Resources must be strictly controlled in accordance with the University's Remote Access to IT Resources Policy.

III. Terminating Access to IT Resources

To the maximum extent possible Terminating Access to University IT Resources must address the following standards:

Access Removal:

The University reserves the right to remove any user's access to University IT Resources at any time and under any circumstances.

Privileged Access:

- All privileged access to University IT Resources must be immediately terminated at any time that an employee separates with Purdue University.
- IT Resource owners, or his or her designee, are responsible for maintaining a record of users who have privileged access to such IT Resources so that privileged access may be expediently revoked on short notice.

General Access:

The Identity and Access Management Office (IAMO) will define procedures and schedules for the termination of non-privileged access to University IT Resources.

IV. Compliance

Centralized and departmental IT units and IT Resource owners or other designated individuals are responsible for ensuring appropriate compliance with this standard on University IT Resources within their areas of responsibility. The IAMO at Purdue University offers a number of identification, authentication, and authorization services to departments and academic units. For information about these services contact: [iamo@purdue.edu](mailto:iamo@purdue.edu).

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

The University maintains the authority to restrict or revoke any user's privileges at any time; and to take any other steps deemed necessary to manage and protect its IT Resources. This authority may be exercised with or without notice to the involved users.

V. Related References

- Authentication and Authorization policy (VII.B.1), available at:  
<http://www.purdue.edu/policies/information-technology/viib1.html>
- IT Resource Acceptable Use Policy (VII.A.2), available at:  
<http://www.purdue.edu/policies/information-technology/viia2.html>
- Data Security and Access (C-34), available at:  
[http://www.purdue.edu/policies/pages/information\\_technology/c\\_34.html](http://www.purdue.edu/policies/pages/information_technology/c_34.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/>
- Information regarding Purdue Career Account is available at:  
[https://www.purdue.edu/apps/account/IAMO/Purdue\\_CareerAccount.jsp](https://www.purdue.edu/apps/account/IAMO/Purdue_CareerAccount.jsp)
- The Request for Privileges form is available at: <https://www.purdue.edu/apps/account/r4p>
- Information regarding the Request for Privileges process is available at:  
[http://www.purdue.edu/hr/HR\\_Operations/resources/requestForPrivilegesDoc.html](http://www.purdue.edu/hr/HR_Operations/resources/requestForPrivilegesDoc.html)

Issued February 1, 2008 from the Identity and Access Management Office (IAMO), updated December 7, 2011. Questions about these standards can be addressed to [i amo@purdue.edu](mailto:iamo@purdue.edu).