PURDUE UNIVERSITY

BIOMETRIC TECHNOLOGIES IMPLEMENTATION STANDARD

Issued December 21, 2009 from the Purdue University Security Officer's Group, University Data Stewards, and IT Networks and Security (ITNS). Questions about these guidelines can be addressed to itap-securityhelp@purdue.edu.

I. Introduction:

"Biometrics" refers generally to the science of measuring, recording, and analyzing the unique physical attributes of a person. In information technology, biometrics typically refers to those technologies using a person's unique physical attributes for identification and/or authentication purposes. Unique physical attributes, also called "biometric data," can include, but are not limited to, fingerprints, hand geometry, retina and iris patterns, voice waves, signatures, and facial patterns.

Due to each person's uniqueness, the use of biometric technologies can be used to greatly enhance information security. However, due to the immutable nature of biometric data, ensuring the security of such data and protecting the privacy of persons required to use biometric technologies is of the utmost importance.

II. Biometric Technologies Implementation Requirements

Due to the unique and immutable nature of biometric data, any deployment of technologies using biometric data for identification and/or authentication purposes must be specifically approved by the University's Chief Information Security Officer, using the *Request to Use Biometric Data* form.

In addition to the information required on the *Request to Use Biometric Data* form, all departments and units within Purdue University or any entity using Purdue University IT Resources must comply with the following requirements when deploying any technology or service using biometric data (called "biometric technologies" in this document):

- No storing of biometric images.
- Biometric data must be encrypted via the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning to that biometric data without use of a confidential process or key.
- Biometric hashes are considered restricted data under the Purdue University data classification schema and must be handled accordingly under the Purdue University data handling requirements.
- Biometrics shall be used for identification of an individual, not authentication. If authentication is needed, an additional factor is required, such as a PIN, password, or other user credential. No information may be returned to a user other than public information provided in the Purdue Directory without the provision of an additional factor, such as a PIN, password, or other user credential.

Use of Student Biometric Data: "Biometric Record" is defined as personally identifiable information under the Family Educational Rights and Privacy Act of 1974 (FERPA). Departments and units considering biometrics implementations involving student biometric data must consult with the Purdue Office of the Registrar FERPA consultant.

In addition to the requirements stated above, departments and units wishing to deploy technologies using biometric data are encouraged to be familiar with emerging standards on the secure use of biometric data. The National Institute of Standards and Technology (NIST) provides numerous resources related to biometrics use.

Approval for the use of biometric technologies at the University takes into account many factors, including but not limited to, reason for the biometric technology deployment, security needs, type of biometric data used, planned protection measures, placement of biometric technologies, and the technical specifications of the planned technologies. Departments, units, or individuals requesting to use biometric data are expected to work with IT Networks and Security (ITNS) to ensure that such factors are appropriately addressed in light of the facts and circumstances of a particular installation.

Note Regarding Research of Biometrics: This standard is not intended to apply to those departments and/or personnel conducting research of biometric technologies for academic purposes. Departments conducting research of biometrics technologies, data, and similar implementations are strongly encouraged to adopt appropriate security measures to protect the biometric data used in this type of research.

III. Compliance

University departments and units, University IT Resource owners, departmental IT units, or other designated individuals are responsible for implementing this standard on any biometric technologies at Purdue University under their control.

The University maintains the authority to restrict or revoke any user's privileges on University IT Resources, and to take any other steps deemed necessary to manage and protect University IT Resources and data, including referral to appropriate external authorities. This authority may be exercised with or without notice to the involved users.

IV. Related References

- *Request to Use Biometric Data* Form available on the SecurePurdue webpage.
- University IT Policies are available at: http://www.purdue.edu/policies/information-technology.html
- Standards and guidelines supporting the implementation of University IT Policies are available at: http://www.purdue.edu/securepurdue/bestPractices/

- Purdue University Office of the Registrar (for FERPA information), available at: http://www.purdue.edu/Registrar/

- National Institute of Standards and Technology (NIST) resources related to biometrics use are available at: http://csrc.nist.gov/publications/PubsTC.html (Scroll to "Biometrics" section for applicable references. *See for example*, NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices and NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; SP 800-77, Guide to IPsec VPNs; or SP 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.)

Revised November 21, 2011 to update URLs.