Subject: Personal Credentials for Enterprise Electronic Services

1. Purpose

This policy instructs individuals affiliated with Virginia Tech and providers of Virginia Tech electronic services on the use of personal electronic credentials within the electronic enterprise systems of the university. The policy promotes security, accountability, and appropriate levels of confidentiality in the assignment and use of these personal credentials.

2. Policy

Virginia Tech uses a personal identifier (PID) to represent students, faculty, staff, alumni, business partners and other affiliates of the university. The PID and associated credentials provide electronic access to services. The PID is also basic identifying information and is considered directory information consistent with Federal policy. The PID positions both centrally and locally managed services to authenticate individuals reliably and accurately.

One and only one PID is provided to an individual at the time the individual initially assumes or resumes a relationship with the university for which PIDs are provided. The PID remains the property of Virginia Tech and Virginia Tech reserves the right to change, delete, or add PIDs. Having a PID is a prerequisite for accessing centrally provided electronic services, and is associated with credentials used to authenticate the individual.

Having a PID is not, however, sufficient to authorize individuals to use those services. Each service defines the criteria for service provisioning, and authorizes the individual according to those criteria.

Having a PID is a prerequisite to acquiring other central login credentials.

2.1 Scope of Policy

This policy applies to the PID as the primary credential for authentication to university electronic services. The character string that constitutes the PID may take on other uses and properties than authentication credentials. This policy applies only to the uses of the character string as an authentication credential.

2.2 PID Data Administrators

The ***data trustee*** for the PID is the Vice President for Information Technology. The primary ***data steward*** for the PID is the director of Identity Management Services.

Standards for creating and suspending PIDs will be established in consultation with the data trustees with primary responsibility for the relationships between an individual and the university; namely:

- Students and former students: Vice President and Dean for Undergraduate Education
- Alumni and friends: Vice President for Alumni Relations and Vice President for Development and University Relations
- Employees and retirees: Associate Vice President for Human Resources
- Other affiliates: Unit head responsible for requesting the PID(s).

2.3 PID Lifecycle

2.3.1 Creating PIDs

The PID will be created when an individual initially assumes or resumes a relationship with Virginia Tech that entitles that person to a PID. These relationships are defined in the ***PID Procedures*** document.

2.3.2 Changing PIDs

Because a PID is a credential that does not require that large numbers of individuals know the PID, the string of characters composing the PID will not normally be changed.

2.3.3 Suspending PIDs

The PID may be suspended when an individual relinquishes all relationships with Virginia Tech that could entitle that person to a PID. These relationships are defined in the ***PID Procedures*** document.

In addition, the university reserves the right to require a renewal process. Renewal criteria may be based upon the elapsed time since a student's last enrollment or a retiree's last employment, the elapsed time since the PID was used for authentication in the Information Technology-provided authentication system, actuarial expectations, and/or additional criteria as determined by the Vice President for Information Technology.

2.3.4 Other Actions to PID Accounts

The university reserves the right to take other actions that result in a PID not being usable.

2.4 Character Strings and Namespace

By using central IT-provided authentication, a university electronic service may use the PID and its associated password in a secure and accurate manner.

When it is not feasible for a service to use central IT-provided authentication, other authentication services should consider using the same character string as the PID.

If a service requires more than one electronic ID for a given individual, conflict with PIDs can be avoided by making application to IMS to reserve the character string of the additional electronic IDs in the PID namespace.

2.5 Passwords

A minimum credential for logging into electronic services is a password. The University Information Technology Security Officer establishes the password standards.

Password changes will be done by the user through a process that does not expose the password to being physically read by other individuals, either during the change or after.

If a password must be administratively reset, then the individual must provide additional information to verify his or her identity. Administrative resetting of passwords will result in a temporary password that must be changed again by the user before it can be used.

By extension from the Acceptable Use and Administration of Computer and Communication Systems (Policy 7000) and its associated standard, users must guard their own information associated with password resetting carefully, and not use anyone else's password reset information without permission.

Passwords for PIDs will NOT be shared with any entity outside the university.

Additional electronic credentials may be associated with the PID.

3. Procedures

Detailed implementation of PID lifecycle and PID uses is outlined in the associated document, ***PID Procedures***.

4. Definitions

Electronic credentials: Electronic credentials provide a means to link an asserted identity in the electronic medium to evidence used to verify a person's identity. Electronic credentials may be something you know (for example, PID plus password, or a challenge question and answer pair), something you have (for example, a smart card or a physical token), or something you are (including biometric measures).

E-mail address: Virginia Tech provides basic e-mail service to many of its affiliated groups. Individuals with e-mail service will have an e-mail account named after their PID, and PID/password credentials will be used to authenticate to the basic e-mail system. However, e-mail account holders are encouraged to set a ***preferred e-mail address***—another character string—that is the e-mail address used by others to communicate with them.

Employees: Employees include those individuals who are currently employed and paid by Virginia Tech, as well as those who have been designated as employees but not paid by Virginia Tech. Employees must be present in the enterprise human resources information system.

IMS: Identity Management Services is the office responsible for provisioning access credentials to university online resources.

Other affiliates: Other affiliates of the university are designated by agreements with other entities.

Principal name: An identifier used by an individual or other entity to identify itself to an authentication system. At Virginia Tech, this is the PID.

Retirees: Retirees are those individuals who have officially retired from the university, and whose information is present in the enterprise human resources information system**.**

Students, former students, and alumni: These terms broadly defines a student, former student, or alumnus as a person who has enrolled in credit-bearing courses at Virginia Tech, and who has an entry in the enterprise student information system.

Suspended PIDs: A suspended PID is a PID that is not usable by the account holder.

5. References

Administrative Data Management and Access Policy—University Policy 7100

Acceptable Use and Administration of Computer and Communication Systems—University Policy 7000

Acceptable Use Standard

6. Approval and Revisions

Approved March 30, 2005 by the Vice President for Information Technology, Earving L. Blythe.

September 7, 2006: Technical revisions – (1) policy renumbered to Information Technology Policy 7040 from former General University Policy 2040; (2) "Personnel Services" updated to "Human Resources;" (3) references updated.

- Revision 1

  April 1, 2008: Updates to position titles and/or responsibilities due to university reorganization.

- Revision 2

  August 24, 2009: Updates to (1) reflect unit name change from Information Resource Management (IRM) to Identity Management Services (IMS); (2) reflect name change from "Acceptable Use Guidelines" to "Acceptable Use Standard"; (3) add requirements to the treatment of PID passwords; and (4) add reference to PID Procedures.