Contents:

1. Preface
2. Policy
3. Audit and Compliance

Section 1. Preface

A. Name. The formal name of this policy is the Account Creation and Deletion Policy.

B. Status of This Policy

2. Public Review and Comment Period. 4/15/2013 to 5/15/2013
4. Working Group Review and Comment. 7/17/2013
5. Accepted. 7/17/2013

C. Scope and purpose

This policy establishes the timing and process around creating and deleting accounts by which members of the community are authenticated and authorized to use Haverford’s information technology resources. This policy addresses:

- Who has the authority to approve the creation of accounts
- What steps must be taken before accounts are created
- Who has the authority to request the disabling of accounts
- What steps must be taken before accounts are disabled
- Standard intervals between separation, account disabling and the final deleting of accounts and data associated therewith
- Who has the authority to override standard intervals between separation, account disabling and final deleting of accounts and data associated therewith
- How IITS shall address appeals of the above decisions and/or dates

This policy addresses all systems administered by IITS to which access is typically granted through the use of an account with one or more authentication factors (usernames and passwords, RFID, RSA or other random or sequential token generator, etc.).
Strictly speaking, this document does not address access to systems that are not administered by IITS. However it may impact availability of any such system that uses IITS-operated central authentication or authorization technologies.

D. Spirit and Intent

The underlying intent of this document is to support IITS in developing business practices to:

- Protect the integrity of college-owned systems.
- Maximize the security around any data:
  - To which the College has a legal or contractual obligation to control access.
  - To which limited access is in the best interests of the College or members of the Haverford Community.
- Maintain an overall high level of security and user accountability while also:
  - Providing for common-sense access to resources during the orderly transition of a community member’s affiliation with the College.
  - Providing for managers’/department heads’ access to college-owned resources previously stewarded by a community member whose affiliation with the college is changing.
- Maintain a high level of understanding broadly among the Haverford College community about what happens to account access and data when the nature of a community member’s affiliation with the college changes.

Section 2. Policy.

A. Account Creation.

1. The Dean of Admissions, or those he or she may designate, shall have the authority to cause records for new Haverford College students to be entered into the College’s authoritative systems of record.

2. The Dean of the College, or those he or she may designate, shall have the authority and responsibility to enter or modify records for Haverford College students as necessary in the College’s authoritative systems of record.

3. The Executive Secretary of the Committee on Student Standing (CSSP) shall have the authority and responsibility to modify existing students’ records as necessary in the College’s authoritative systems of record for the purposes of changing students’ access pursuant to CSSP actions (for example, restoring access to a student who has returned from a leave mandated by CSSP).

4. The Director of Human Resources, or those he or she may designate, shall have the authority and responsibility to enter records for new or returning non-student Haverford
College affiliates such as faculty, staff, volunteers, contractors and others into the College’s authoritative systems of record.

5. The Chief of Staff and Board Secretary, or those he or she may designate, shall have the authority and responsibility to mark records for members of the Board of Managers. As a matter of workflow, this responsibility may be delegated to the Director of Human Resources but only as directed by the Chief of Staff and Board Secretary.

6. It is the general policy of the College that individuals receive accounts from only their institution of record. In cases where an individual is employed to work, or enrolled to study, at more than one among Haverford College, Bryn Mawr College and Swarthmore College, the individual shall receive accounts only from their primary institution.
   i. This policy may be overridden on a case-by-case basis when a Haverford College account is necessary to facilitate access to necessary services not available through a home institution account.
   ii. In the case of students the test for primary institution is the institution into which the student is matriculated or primarily affiliated. For example, a student majoring at Bryn Mawr College but matriculated at Haverford College shall, for the purposes of this policy, be considered a Haverford College student.
   iii. In the case of non-students, the test for primary institution is the institution that issues pay and benefits, regardless of the source of funding for such pay. For example, an employee who works half time at Haverford College and half time at Bryn Mawr College, but is paid for all Bi-College work by Haverford College shall, for the purposes of this policy, be considered a Haverford College employee. This holds true regardless of whether Bryn Mawr College reimburses Haverford College for a portion of wages and benefits.

7. IITS shall have the authority and responsibility to:
   i. Create, manually or through established automated systems, accounts used to authenticate the identity of community members properly entered into the College’s authoritative systems of record.
   ii. Deliver account usernames and passwords (account credentials) directly to users.

8. IITS shall not create accounts or provide account credentials for individuals not yet entered into the College’s authoritative systems of record.

9. No individual except an appropriate member of the IITS staff shall deliver account credentials to users.

10. No individual may receive account credentials except the individual for whom the credentials were created.

B. Routine Account Suspension. The business practice of IITS shall be to proceed as if separations are on good terms using standard intervals between suspension and deletion, unless
notified otherwise. The Routine Account Suspension policy applies when one of the following conditions exist:

- **Non-Students.** The Director of Human Resources, or his or her designate, together in consultation with a separating community member’s supervisor or organizational member of the Senior Staff of the College, shall determine whether such separation is on good terms. Factors to be considered include whether a separation is voluntary or involuntary and whether the employee separating is in good standing with the College.

- **Students.** The Dean of the College, or his or her designate, shall determine whether a student’s separation is on good terms. Factors to be considered include whether a separation is involuntary, whether the student is in good standing with the College, etc.

- The Dean of the College, or those he or she may designate, shall have the authority and responsibility to mark records for separating Haverford College students in the College’s authoritative systems of record.

- The Executive Secretary of the Committee on Student Standing (CSSP) shall have the authority and responsibility to modify existing students’ records as necessary in the College’s authoritative systems of record for the purposes of changing students’ access pursuant to CSSP actions (for example, suspending access to a student as mandated by CSSP).

- The Director of Human Resources, or those he or she may designate, shall have the authority and responsibility to mark records for non-student affiliates of Haverford College such as faculty, staff, volunteers, contractors and other non-student affiliates into the College’s authoritative systems of record.

- The Chief of Staff and Board Secretary, or those he or she may designate, shall have the authority and responsibility to mark records for members of the Board of Managers.

### C. Emergency Account Suspension.

IITS shall have the authority to suspend an account in cases where there is, in the opinion of the Chief Information Officer or his or her designate, sufficient evidence to indicate that one of the following conditions exists:

- The account’s security has been breached.
- The account’s use presents a clear and present threat to the College, account holder, community or our IT resources.
- The account is being used to violate College policy, or local, state or federal law.
The account is assigned to a member of the community who is separating and such separation does not meet the tests established in Section 2.C of this policy.

The President of the College and members of the President’s Senior Staff (including Provost, Dean of the College, Vice Presidents, Chief of Staff), and the Director of Human Resources, shall have the authority to cause IITS to suspend an account assigned to a person under their direction or charge when they deem that such suspension is necessary in the best interest of the College.

IITS shall make every reasonable attempt to notify a user that his or her account has been suspended and of all related suspension and deletion policy as close to the time of suspension as possible, unless such notice is not in the best interest of the College or Community.

D. Automation of account creation, suspension and deletion
   a. IITS shall be responsible for developing and maintaining systems that create, suspend and delete accounts automatically based on entries in the College’s authoritative systems of record as described in sections 2.A and 2.B of this policy.
   b. Where automation is not possible or practical, IITS shall be responsible for manually creating, suspending and deleting accounts on systems operated by IITS based on entries in the College’s authoritative systems of record as described in sections 2.A and 2.B of this policy, or as provided for in section 2.C of this policy.
   c. IITS offers mechanisms for central authentication and authorization into College-owned systems. System administrators who opt to not use these mechanisms to control access to locally managed systems are responsible to monitor the affiliation status of their users and manage their own authentication and authorization.
   d. IITS shall not be responsible for authentication and authorization into systems not operated by IITS where the system administrator is unwilling or unable to use IITS central authentication and authorization mechanisms.
   e. IITS shall not be responsible to maintain lists of local systems or system administrators, nor notify them upon the separation or status change of a community member.

IITS shall be responsible for communicating implications of account creation, suspension and deletion to account holders.

E. Preparation for separation and security of College IT resources.
   When possible, supervisors should do the following as near to the separation of a non-student as possible.
Secure or limit access to the user’s desktop computer. IITS can assist by removing power and Ethernet connectivity to desktop computers if necessary.

At the request of Human Resources, IITS will gather any data that may be required for legal or records-retention reasons.

Gather all portable college-owned devices (cellular telephones and smartphones, laptop computers, external hard discs and portable storage, etc.).

Ensure that the user’s identification card is returned to Human Resources. ID cards contain electronically stored data on magnetic strips and special microchips that can be used to gain both physical and electronic access to resources and, in the case of Pharos printing, incur departmental charges. Retrieving and returning this card to HR helps prevent unauthorized access following a separation.

Be sure to also notify Security (to cancel physical access to campus buildings) and the Business Office (to change voicemail passwords). IITS does not administer physical access to campus buildings or voicemail.

In planning for the routine, voluntary separation of an employee in good standing (as in the case of retirement or a career change beyond the College) supervisors should refer to the IITS website for guidance on best practices in working with an employee to transfer data to another employee.

F. Supervisor access to non-student data upon suspension of an account.

1. IITS shall attempt to facilitate access to college-owned data for supervisors upon the separation of a non-student for a period sufficient to allow for transfer of data to another account holder.

2. IITS will, at the request of a supervisor, setup of an out-of office message. Such messages should include:

   ▪ Greeting and an indication that the user’s affiliation with the college has changed.
   ▪ Information on where to send future college-related communication.
   ▪ A notice that e-mails have been forwarded to that address, if applicable.
   ▪ Information on where to send future personal communication.
   ▪ Additional contact information or details as directed by the departmental supervisor.
   ▪ Transfer any data linked to or owned by the departing non-student to another account holder.

G. Account Deletions.

1. An account holder’s primary record in the College’s authoritative systems of record shall not be deleted.
2. Usernames, once issued to an individual person, shall not be reissued for use by another person and recorded in the account holder’s primary record in the College’s authoritative system or record.

3. IITS shall, in cooperation with the Dean of the College and the Director of Human Resources, establish and publish a practice setting a period of time, not shorter than 90 days for students and 30 days for non-students from the time of account suspension, before which accounts and associated data are deleted from College-owned systems.

Section 3. Audit and Compliance

A. Audit. Enterprise systems shall establish an audit process with an interval no less than annually to ensure that business process and practice are in compliance with this policy.

B. Enforcement. The CIO and IITS Directors shall have the authority to enforce this policy through establishing and implementing business practices consistent with the policy.

C. Risk of Non Compliance. Failure to comply with this policy may have the following implications for the college and community.

- This policy creates a framework for uniform treatment of accounts consistent with the spirit and intent. Violating the policy or business practices originating therefrom could set precedents that make further enforcement difficult.
- This policy creates a framework for securing access to College-owned data upon separation of a community member. Violating the policy or business practices originating therefrom may create a risk of data loss.
- This policy creates a framework for securing access to data protected under federal, state or local laws. Violating the policy or business practices originating therefrom may expose the College or members of the community to legal sanction.

D. Penalties for Non Compliance. A community member’s attempt to override or circumvent this policy or business practices originating therefrom subjects the community member to sanctions as determined by IITS, the Office of Human Resources together with the Senior Staff member under whose purview an employee falls, the Office of the Dean of the College or the Office of the Provost, as appropriate. These sanctions include but are not limited to loss of account or data access, review by Honor Council, and/or disciplinary action through the Office of Human Resources.