HAVERFORD
COLLEGE

Account Creation and Deletion Policy

Introduction

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.

The procedures for creating, suspending and deleting accounts vary by category and role of each user and the differences and time frames are described within the policy. Procedures for handling individual separations from the College vary based on whether or not the separation is routine.

Scope

The 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 (e.g. usernames and passwords).

While this policy does not address access to systems that are not administered by IITS, it may impact availability of any such system that uses IITS-operated central authentication or authorization technologies.

The underlying intent of this policy is to protect the integrity and security of College-owned systems and data, and to provide for appropriate provisioning and deprovisioning of access to community members throughout the life of their affiliation with the College.

Policy

All Haverford College community members in good standing will be provided access to ~~a~~ Haverford systems account in order to access systems necessary for their role at the College. The specific systems to which access is provided and the level of permissions within those systems will be dependent on the individual's specific role and position requirements. Each category of community member – student, staff, faculty, emeritus, contingent – will be given a base level of access for their role when their account is created. If additional access beyond the base level is required the individual's Dean or Supervisor will work with IITS to determine and execute the necessary changes to their account permissions.

Upon separation from the College, for any reason, account access will be suspended, and eventually deleted. Depending on the category of community member and reason for separation, there may be a grace period provided following separation but before suspension, as well as a grace period following suspension before deletion. Current grace periods are specified in Appendix I.

Extensions to the length of a grace period are, in general, not approved. However, if a separating community member believes they require an extension to their grace period for extenuating circumstances, their supervisor or dean may petition IITS for the extension which will be considered on a case-by-case basis.

Procedures

A. Account Creation -- Students

1. The Vice President and Dean of Admission, or those they may designate, shall have the authority to authorize records for new Haverford College students to be entered into the College's authoritative systems of record.
2. The Dean of the College or the Registrar, or those they may designate, has the authority and responsibility to enter or modify records for Haverford College students as necessary in the College's authoritative systems of record.
3. IITS has the authority and responsibility to establish automated systems (known as Identity Management Systems) or when necessary, manually, to authenticate the identity of community members properly entered into the College's authoritative systems of record and to deliver account usernames and passwords (account credentials) directly to users.
4. Only the College's identity management system or an appropriate member of the IITS staff shall deliver account credentials to users.
5. Individuals may not receive, or use, account credentials that are not theirs.

B. Account Creation – Employees and Affiliates

1. Human Resources, or those they may designate, has the authority and responsibility to enter records for new or returning employees or affiliates of the College such as faculty, staff, board members, volunteers, contractors, and others into the College's authoritative systems of record.
2. Faculty, staff, and contingent workers (all other non-students) each follow defined and different practices regarding what systems they are given access to and policies regarding suspension of their accounts (see below).
3. Contingent workers (everyone other than students, staff, or faculty) will be given the least access necessary to accomplish their responsibilities as indicated by their manager/sponsor. The baseline access for these individuals will be access to the College's network and wifi.

4. The Chief of Staff or their designee, has the authority and responsibility to identify members of the Board of Managers who require accounts.   IITS has the authority and responsibility to enter records for Board Members into the College's authoritative systems of record.

C. Account Creation – Trico Community Members

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.

1. 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.
2. 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.
3. 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.

D. Routine Account Suspension

IITS standard procedure is to proceed as if separations are on good terms using standard intervals between suspension and deletion, unless notified otherwise. The routine account suspension process applies when one of the following conditions exist:

1. Non-Students. The AVP or Director of Human Resources, or their designee, together in consultation with a separating community member's supervisor or divisional member of Senior Staff, 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. The Director of Human Resources, or those they may designate, shall have the authority and responsibility to mark records for non-student employees or affiliates of Haverford College such as faculty, staff, or contingent workers, into the College's authoritative systems of record.

2. Students. The Dean of the College or the Registrar, or their designee, in consultation with the Committee on Student Standing (CSSP) if appropriate, shall determine whether a student's separation is on good terms. Factors to be considered include whether a separation is involuntary and whether the student is in good standing with the College. The Registrar, or those they may designate, shall have the authority and responsibility to mark records for separating Haverford College students in the College's authoritative systems of record.
3. The Chief of Staff and Board Secretary, or their designee, shall have the authority and responsibility to notify IITS to mark records for members of the Board of Managers to be suspended.

E. Emergency Account Suspension.

IITS has the authority to suspend an account immediately when deemed necessary for the best interest of the College in the following instances:

1. The President of the College may authorize IITS to suspend any account at the college.
2. The Director of Human Resources may authorize IITS to suspend any non-student account.
3. The Dean of the College or Registrar may authorize IITS to suspend any student account.
4. Senior Staff may authorize IITS to suspend any employee or contingent worker account in their division.
5. The CIO or their designee may authorize suspension of any account if there is sufficient evidence that one of the following conditions exists:

    a. The account's security has been breached.
    b. The account's use presents a clear and present threat to the College, account holder, community, or other IT resources.
    c. The account is being used to violate College policy, or local, state or federal law.

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

F. Automation of account creation, suspension and deletion

1. IITS is 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 A through E of this policy.

2. Where automation is not possible or practical, IITS is 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 A through E of this policy.
3. IITS offers mechanisms for central authentication and authorization into College-owned systems and all system administrators at the College are encouraged to use these mechanisms when possible. 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 in accordance with College policies.
4. IITS is not responsible for authentication and authorization into systems not operated by IITS or where the system administrator is unwilling or unable to use IITS central authentication and authorization mechanisms.
5. IITS will not maintain lists of local systems or system administrators, nor notify local system administrators upon the separation or status change of a community member.

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

G. Preparation for Separation and Security of College IT Resources.

When possible, supervisors should do the following as near to the separation of a faculty, staff, or contingent worker as possible.

1. Secure or limit access to the user's desktop computer.
2. At the request of Human Resources or the Senior Vice President for Administration and Finance, IITS will gather any data that may be required for legal or records-retention reasons.
3. Gather all portable college-owned devices (cellular telephones and smartphones, laptop computers, external hard discs and portable storage, etc.).
4. Ensure that the user's identification card is returned to Human Resources.
5. 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.
6. If needed, supervisor may ask IITS 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. This access will only be available following the end of the non-student's grace period and will end once the data has been deleted per Appendix I.
7. If desired, supervisor may ask IITS to set up an out-of-office message for the separated employee.

At the request of Human Resources or the Senior Vice President for Administration and Finance, IITS will gather any data that may be required for legal reasons.

H. Account Deletions

An account holder's primary historical record in the College's authoritative systems of record shall be retained for historical purposes. However, the account holder's record in subsidiary systems, including email and data associated with the email account, will be deleted according to the schedule outlined in Appendix 1.

IITS shall, in cooperation with the Provost, the Dean of the College and the AVP of Human Resources, establish and publish a table outlining for each category of account holder, the periods of time at which their accounts will be first suspended and later deleted following their separation from the College.

Definitions

Authentication: The process of confirming a user's identity, usually through provision of a username, password, and Duo prompt.

Authorization: The process of confirming what systems an authenticated user is authorized to access.

Authoritative System of Record: The core system in which new users are created and which carries the most up-to-date information about the user's account.

Contingent Worker: A person with some relationship to the college, other than as a student, employee, or emeriti, that requires some level of systems access through an account.

Identity Management System: An automated system which manages and processes the authentication and authorization of an organization's users.

Permissions: Indicators on a user's record of which systems and functions within a system a given user is enabled to use.

References, Related Resources, or Appendices

Appendix I

Account Holder	**Systems Affected**	**Days After Which Account is Suspended**	**Days After Which Account is Deleted**
Graduated Students	All	90 days	180 days
Students on College Leave	All	28 days	Never
Students Withdrawn	All	90 days	180 days
Student Workers*	All	14 days	104 days
Faculty – Separated	Peoplesoft	30 days	Never
	Moodle	30 days	Never
	Network	180 days	270 days
	Google	180 days	270 days
	Duo	180 days	Never
Faculty – Emeritus	Peoplesoft	30 days	Never
	Moodle	30 days	Never
	Duo	180 days	Never
	Network	Never	Never
	Google	Never	Never
Staff – Separated	All	30 days	120 days
Contingent - Separated	All	0 days	90 days

*Note: Student Policy Takes Precedence over Student Worker Policy

First approved/Last revised November 12, 2020

Effective date November 12, 2020

Next review required by November 12, 2025

Sponsor: Spencer Golden, Associate CIO
Contact the IITS Office with any questions.