Policy Number:	IT01-04
Approved by	The Leadership team
Date Approved by:	01/06/2012
Date Effective:	Immediately
Date of Next Review:	01/06/2014
Related Policies:	IT00-01: Information Systems Acceptable Use Policy
Contact:	ITS Director

1.0 Purpose

The Network Account Policy defines policies and procedures for the creation and maintenance of network accounts and associated services of The American University of Paris (hereinafter "University") network users.

2.0 Scope

This policy applies to all users (both internal and external) requiring network accounts in order to access computer systems belonging to the American University of Paris (hereinafter “University” or “AUP”).

3.0 Network Account Policy

Information Technology Services (ITS) is responsible for creating and maintaining network accounts and for ensuring the security of the network account infrastructure. ITS collaborates with other departments to define policies governing access to technology services and resources.

3.1 Account Request and Support Procedure

All account-related requests and queries must be submitted to ITS via the AUP Helpdesk system.

3.2 Employee Accounts

All University employees receive an individual network account and associated services (including but not limited to an e-mail account, access to individual and departmental file storage spaces, membership in security and distribution groups (e.g. faculty, staff and departmental groups), the ability to use campus computers, and the ability to use the University’s wireless network).

Human Resources (HR) is normally responsible for submitting all employee account activation requests to ITS, irrespective of employee category. However, in the specific case of faculty accounts, Human Resources may delegate this responsibility to Academic Affairs (AA).

3.2.1 Account Validity

Employee accounts are normally valid from the first day of the employee's contract to the last day of the contract. For administrative reasons, HR or AA (as appropriate) may request that an employee's account be activated before the start of the employee's contract, and/or that deactivation of an employee's account be delayed by *up to ONE month* following the official end of the employee's contract.

3.2.2 Change Notifications

When a permanent employee leaves the university, or when a short-term employee's contract term changes, HR or AA (as appropriate) are responsible for informing Information Technology Services, who will take the appropriate action.

When an employee's departmental affiliation changes, HR or AA (as appropriate) are responsible for informing Information Technology Services.

3.2.3 Account Deactivation and Deletion

Once an employee account reaches the end of its validity period, the account is deactivated. Six months later, the account and all associated data are permanently deleted.

3.3 Student Accounts

3.3.1 Scope

This section applies to the following categories of users: applicants to the University, registered students, former students and alumni.

3.3.2 Student Account Creation

As soon as an applicant is admitted to the University, a network account is created for the user.

If the applicant chooses to attend the University, the account remains active throughout the student's studies (and after the student leaves the University, if he or she chooses to retain the account).

If the applicant defers admission, the account remains active until one of the cases outlined immediately below occurs.

If the applicant declines admission to the University, the account is deactivated and six months later is deleted.

If an applicant does not respond, the account is deactivated once the expected entrance term for that applicant has passed. The account is deleted six months later.

3.3.3 Student Account Validity

Student accounts are not deactivated as long as they are used (with the exception of applicant accounts, for which the rules are described in 3.3.2 above).

A student account is considered to be “in use” if the user changes the password at least every six months. Otherwise, the following procedure applies:

1. Passwords automatically expire six months after the last modification.

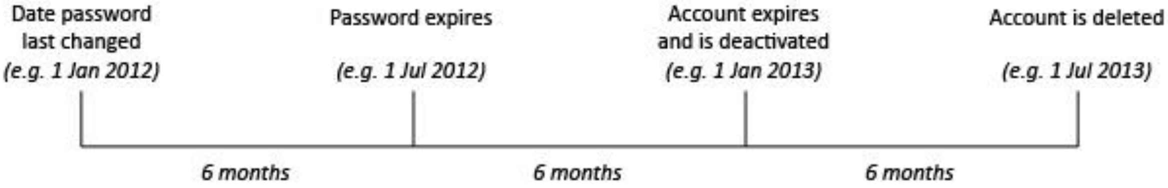
2. During the six months following password expiry, users can regain access to their accounts by changing the account password.

3. At the end of the six months following password expiry, if the user has not yet changed the password, the account expires and is deactivated.

4. During the six months following account deactivation, the user may request reactivation by contacting the AUP Helpdesk. It may be possible for IT Services to restore some or all of the user’s account data (such as e-mail messages and stored files), though this is *not* guaranteed.

5. At the end of the six months following account deactivation, the account and all associated data are permanently deleted.

6. Once the account has been deleted, former students and alumni may request a new account by contacting the Alumni Office.



The preceding provisions notwithstanding, as stipulated in other policies, ITS reserves the right to temporarily or permanently suspend access to network accounts and related services in response to abuse, or where a security risk requires such action.

3.4 Guest and Special Accounts

3.4.1 Guest Accounts
ITS may create guest network accounts on request, for specific purposes, such as for external consultants, guest lecturers or conferences attendees.

Guest accounts are normally activated only for a limited period, which should be specified by the requester.

ITS is responsible for ensuring that guest accounts do not allow unjustified access to sensitive data or threaten the security of University systems. Therefore, ITS reserves the right to refuse creation of guest accounts, or to significantly limit the privileges of such accounts if a risk is identified.

3.4.2 Emeritus Faculty Accounts
Emeritus Faculty may request a network account granting access to an individual e-mail mailbox, individual file storage, and campus computers in the Computer Labs, Lounges and in the Library. These services are provided in order to facilitate Emeritus Faculty members' participation in scholarly life at and beyond the American University of Paris. Commercial and for-profit uses of these services are not considered Acceptable Use.

3.4.3 Trustee Accounts
The Office of the President may request creation of network accounts for Trustees of the University. The Office of the President is also responsible for requesting termination of Trustee accounts as appropriate.

3.4.4 Visiting Scholar Accounts
Visiting Scholars are persons officially invited to participate in the scholarly life of the University for a particular purpose and period of time. To this end, they may access certain University resources and services. However, they are not University employees.

Academic Affairs may request the creation of individual network accounts for visiting scholars. These are limited accounts that grant users access to campus computers and the University's wireless network. There is no e-mail account or file storage associated with Visiting Scholar accounts.

3.5 Sharing of Network Accounts

Individual network accounts are strictly personal and sharing passwords is not tolerated. Where necessary (for example, where an assistant needs to access to a manager's mailbox or calendar), ITS will provide technical solutions allowing shared access to individual accounts without sharing passwords.

4.0 Password Policy

Passwords are an essential aspect of computer security. They are the front line of protection for user accounts, and ultimately for the University's computer systems. Poor choice and handling of passwords may compromise the security and integrity of University systems and result in unauthorized access to confidential data. All users of University systems are therefore responsible for maintaining strong passwords according to the standards outlined below.

Where technically feasible, these standards will be enforced using system-based rules.

4.1 General Password Standards

All users of University systems are expected to respect the following password standards:

- Passwords should be at least six characters long.
- Passwords should contain a mixture of lower and upper case letters, digits, and punctuation marks.
- When selecting a new password, it should not be the same as the previous password.
- Passwords should not contain elements that are easy to guess (such as dictionary words or family members' names).
- Passwords should be treated as confidential information and should never be shared with anyone.

4.1.1 Password Expiry

Changing passwords regularly is an important security measure. Network account passwords are configured to expire six months after they were last changed. Users are thus required to change their passwords at least every six months, to avoid losing access to their accounts.

Users receive notifications prior to password expiry.

4.2 Password Standards for Administrators and for Users of Enterprise Systems

Additional password standards apply to users with administrator privileges (such as Domain Administrators and campus-wide machine Local Administrators), and to users whose accounts grant them back-end or administrative access to Enterprise Systems (including but not limited to the University's Student Information System and the Accounting, Finance and Human Resources systems).

In addition to the standards outlined in section 4.1, the following standards apply to this category of users.

- Passwords should be at least eight characters long.
- When selecting a new password, it should not be the same as the previous three passwords.

4.2.1 Password Expiry

Passwords for this category of users are configured to expire three months after they were last changed.

5.0 Definitions

Term	**Definition**
AUP	The American University of Paris
Disabled Accounts	Upon notification by the appropriate body, the account expiration date is set to the exit date to prevent any further login activities.

6.0 Revision History

Date:	Authority:	Details:
22 August 2012	**E. Ritt**	**Corrections, enhancements to formatting.**
8 October 2012	**E. Ritt**	**Enhancements to text.**