Policy Number:	IT01-01
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 purpose of this policy is to establish a framework for management and administration of the security of The American University of Paris's (hereinafter "University") data network.

2.0 Scope
This policy applies to all existing and future connections to the university data network by all users of those networks, whether internal or external.

3.0 Policy
Information Technology Services protects the integrity of the university network by mitigating the risks and losses associated with technical security threats to the university network and information systems.

3.1   Information Technology Services is charged with:

    3.1.1   Providing a reliable network and Internet connection (in coordination with appropriate third parties) to conduct the university's business

    3.1.2   Granting only authorized access to institutional, research or personal data and information on the university network, in accordance with the University's policies on access to administrative systems and data.

    3.1.3   Protecting computer system and network integrity at University and specifically:
        A. Protecting computing and network resources from unauthorized access.
        B. Protecting university information from unintended and/or unauthorized disclosure.
        C. Monitoring the university network for devices and users in violation of this policy.

3.2   To accomplish these charges:

    3.2.1   Information Technology Services develops and maintains guidelines for network connections and for configuration of network-connected devices.

    3.2.2   Information Technology Services has the authority to enforce adherence to its network security guidelines.

3.2.3   Information Technology Services will proactively scan for security weaknesses in the network or any equipment connected to the network and will provide an audit report to the equipment owner after the scan/audit is completed.

3.2.4   The Information Security Officer in Information Technology Services is responsible for the interpretation, administration, and enforcement of this policy.

Information Technology Services has the authority to disconnect from the network any device which may impair or disable the network, compromise the integrity of other network-connected devices, threaten the security of university data stored on the network, or be used for activities which violate university policies.

Additionally, a violation of this policy may be regarded as a violation of other university policies in place for governing the conduct of university community members (faculty, staff, and students), and may therefore result in sanctions and disciplinary actions under the provisions of those policies.

See policies:
IT00-01: Information Systems Acceptable Use
IT01-01: Network Security Policy
IT01-02: Use of Computing and Network Resources – Applicants, Students and Alumni
IT01-03: Use of Computing and Network Resources – Faculty and Staff
IT01-04: Network Account Policy
IT02-01: Access to Administrative Systems and Data

4   **Definitions**

Term	**Definition**
AUP	the American University of Paris

5.0 Revision History

Date:	Authority:	Details:
24 August 2012	**E. Ritt**	**Enhancements to wording, formatting.**
8 October 2012	**E. Ritt**	**With feedback from** Tracy Mitrano, Director of the IT Policy and Institute for Computer Policy and Law in Cornell University.