الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

AASTMT Acceptable Use Policy

Classification	Information Security
Version	1.0
Status	Not Active
Prepared Department	Computer Networks and Data Center
Approved Authority	AASTMT Presidency
Release Date	19/4/2015
Effective Date	19/4/2015

Overview

AASTMT intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to AASTMT established culture of openness, trust and integrity. AASTMT is committed to protecting AASTMT employees, students and the academy from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every AASTMT employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer and network equipments at AASTMT. These rules are in place to protect the employee and AASTMT. Inappropriate use exposes AASTMT to risks including virus attacks, compromise of network systems and services, and legal issues. AASTMT reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Scope

This policy applies to employees, students, staff, temporaries, visitors and other workers at all AASTMT branches. This policy applies to all equipment that is owned or leased by AASTMT.

Policy

General Use and Ownership

1. Internet/Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of AASTMT. These systems are to be used for business purposes in serving the interests of the company, and of our staff and students in the course of normal operations.

2. While AASTMT computer networks and data center desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of AASTMT.

3. For security and network maintenance purposes, authorized individuals within AASTMT may monitor or maintain equipments/services (Racks, Routers, Switches, Firewalls, Internet, etc.), systems and network traffic at any time.

4. AASTMTMT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5. AASTMT recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on encrypting email and documents, for information saving sensitive information please revise AASTMT computer Networks and data center.

General guidelines

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every three months, for more info about passwords refers to password policy.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised to save information
4. Postings by employees from an AASTMT email address to newsgroups or social networking should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of AASTMT, unless posting is in the course of business duties.
5. All hosts used by the employee that are connected to the AASTMT Internet/Intranet, whether owned by the employee or AASTMT, shall be continually executing approved virus-scanning software with a current virus database.

Unacceptable Use

The following activities are in general prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems/network administration staff may have a need to disable the network access of a host if that host is disrupting network services).

Under no circumstances is an employee of AASTMT authorized to engage in any activity that is illegal under local or international law while utilizing AASTMT-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

1. Exporting work related information, software, technical information, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
2. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
3. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done from home.
4. Using AASTMT network resources in activities involving sexual harassment or any offensive activities in violation to law.
5. Altering any network information or adding any device to AASTMT network, this includes but not limited to: IP address, network card, cables, DSL routers, access points, connecting new devices .
6. Adding any network service without prior permission, this includes but not limited to: DNS, DHCP, HTTP, FTP, etc.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to(network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Port scanning or security scanning is expressly prohibited unless prior notification to AASTMT network department is made.
9. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
10. Posting information related to AASTMT in any blog or website without permission is prohibited.
11. Playing games during work time.

Enforcement

Beyond this security policy you should make sure you have a solid understanding of other AASTMT security policies and roles. Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Null.

Related Policies

✓ AASTMT Email Use Policy.
✓ AASTMT Internet Use Policy.
✓ AASTMT User ID and Password Policy.
✓ AASTMT VPN Policy.
✓ AASTMT Wireless Policy.

Definitions

Term	***Definition***
Spam	Unauthorized and/or unsolicited electronic mass mailings.