الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

AASTMT VPN Access 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

A Virtual Private Network (VPN) is a secured private network connection built on top of a public network, such as the Internet. A VPN provides a secure encrypted connection or tunnel over the Internet between an AASTMT network and other networ . Use of a VPN allows approved members of the AASTMT to securely access the network resources from anywhere outside.

Purpose

The purpose of this policy is to specify the security standards required for VPN access, ensuring the integrity of data transmitted and received, and securing the remote access VPN pathways into AASTMT network so that confidential information remains private over non-trusted networks. AASTMT reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Scope

This policy covers everyone who works for or on behalf of AASTMT and uses any of Remote Access Virtual Private Network (VPN) connections to AASTMT corporate networks.

Policy

- ✓ Approved AASTMT employees may utilize the benefits of VPN as a "user managed" service. This means that Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any associated service issue. VPN services work best over broadband connections (as DSL).
- ✓ Authenticated credentials used for accessing AASTMT VPN services must be encrypted during transit over non-trusted networks.
- ✓ Do not select a short, trivial login password. Passwords must meet complexity requirements. For more information, kindly check AASTMT user ID and password policy.
- ✓ It is the responsibility of approved AASTMT employees to ensure that unauthorized users are not allowed to share AASTMT VPN services.
- ✓ All computers connected to AASTMT corporate networks via VPN must use the most up-to-date anti-virus software and up-to-date operating system security patches.
- ✓ All persons authorized to connect a computer device to AASTMT network via VPN services must prevent other unauthorized persons from getting their password or physically accessing and using the computer while the VPN connection is active.
- ✓ Only approved VPN client software may be used to establish VPN connections to AASTMT VPN services.
- ✓ Approved VPN users will be automatically disconnected after a well defined period of inactivity.
- ✓ Users of computers that are not AASTMT owned equipment must configure the equipment to comply with this VPN policy and other and Network security policies.
- ✓ All persons approved to connect client computer devices to AASTMT VPN services may be subject to restricted network resource access per their specified business requirements.

Monitoring

For your safety and the safety of AASTMT network and information, all VPN connections to AASTMT corporate network is automatically audited and monitored by administrative privileges and by many levels. AASTMT has the capability and reserves the right to check, access, and limit or disconnect any sessions for any purpose. AASTMT may disconnect VPN sessions without prior notice. AASTMT is not obliged to monitor VPN sessions.

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

Revision History

Null.

Related Policies

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