Remote Access
Effective as of: 01.01.2022

American University of Armenia
Policy for Publication
Policy Number: ICTS20220001

Remote Access

The purpose of this policy is to define requirements for connecting AUA's network from any remote location. This policy is intended to provide direction on University security practices designed to ensure the confidentiality, integrity and availability of campus information. This policy is designed to minimize the potential exposure to AUA from damages, which may result from unauthorized use of AUA resources. Damages may include the loss of sensitive or confidential data, intellectual property, damage of reputation, or damage to critical internal systems and services.

General

1. Remote access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate business need.
2. All remote access to University applications, systems and hardware shell be authorized and approved through ICTS.
3. Approved AUA employees and authorized third parties may utilize VPN service to establish connection to the campus network.
4. Students, alumni and work studies are NOT eligible to use VPN

All employees can use VPN service with their AUA usernames / passwords. VPN user profiles for third parties will be created at the department's request.

Requirements

By using VPN technology, users must understand that their devices (computers, smartphones, etc.) are considered an extension of the AUA network, and as such are subject to the same policies and regulations that apply when connected directly to the campus AUA network.

1. Users of VPN service are responsible for procurement and costs associated with acquiring Internet connectivity and any associated service VPN services work more reliable over broadband connections
2. All computers connected to AUA campus network via VPN must have up-to-date antivirus This antivirus definition file must not be older than seven days. Additionally, all relevant software and security patches must be installed.
3. It is the responsibility of the ICTS Department to ensure that unauthorized users are not allowed access to AUA campus networks.
4. VPN access must be strictly controlled. Control and access will be enforced using access control methodologies.
5. Employees and third parties with remote access privileges must understand that their AUA-owned or personal device, which is remotely connected to AUA's internal network, shall not connect to any other network at the same time. There are no exceptions.

VPN Restrictions and Enforcement

1. AUA VPN services are to be used solely for AUA business and/or academic support All users are subject to auditing of VPN usage as per the Computer and Network Use Policy.
2. When actively connected to the AUA campus network, by default the VPN service will force all traffic to and from the remote location through the VPN
3. All VPN gateways on the campus network will be set up and managed by AUA ICTS Department, which will provide approved users with appropriate VPN user guide.

VPN users may be automatically disconnected from the AUA network after some period of inactivity. The user must then logon again to re-authenticate in order reconnect to the network.

Applicability

The AUA Remote Access Policy applies to all AUA employees and third parties, with an AUA-owned or personal device that require VPN access to AUA's network and network resources to perform necessary task when not on AUA's campus.

Accountability

This policy regulates the use of all VPN services to the AUA campus network. To maintain security, VPN services will be terminated immediately if any suspicious activity is detected. Service may also be disabled until the issue has been identified and resolved.

Any AUA employee found to have intentionally violated this policy might be subject to disciplinary action, up to and including termination of employment.

Third parties are directly responsible for damage as a direct result of policy violation. Intentional and non-intentional violation will result in termination of service and may result in revocation of contract.