_
Document title: **VPN/Remote Access Policy – October 2022**

Approval date: **January 2018**

Purpose of document: **The document addresses the process of granting certain members of the AUC community and external entities access to AUC resources.**

Office/department responsible: **Office of Information Security**

Approved by: **Nagwa Nicola, Chief Technology Officer**

Document classification level: **PUBLIC**

Document accessible: **[**https://www.aucegypt.edu/about/university-policies**]**

Related documents/see also: **[AUC Acceptance Use Policy, AUC Password Policy, Peer to Peer file sharing policy, Information Security Policy]**

VPN/Remote Access Policy

Policy Statement

VPN and remote access policy governs the process of granting valid stakeholders appropriate access to AUC resources that are unavailable to the public. This policy states the broad lines of prerequisites, needed approvals, and the scope of the offered service. This policy applies to all AUC community as well as all external parties.

Reason for Policy/Purpose

AUC is committed to providing the acceptable secure means to protect its resources and, at the same time, to enable all valid stakeholders efficiently to access their respective AUC digital resources.

Who Approved This Policy

Nagwa Nicola, Chief Technology Officer

Who Needs to Know This Policy

This policy applies to all AUC community, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing VPNs to access the AUC network/services. This policy also applies to implementations of a fixed VPN that allow direct access to the university network from outside AUC

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

Contacts

Responsible University Official: Wessam Maher, Chief Information Security and Risk Officer.

Responsible University Office: Office of Information Security.

If you have any questions on the policy, you may send an e-mail to infosec@aucegypt.edu

Definitions

Term	Definition as it relates to this policy
Virtual Private Network (VPN):	Encryption and tunneling technology is used to connect users or branch offices securely over a public network, usually the Internet; typically, a VPN will be configured to allow an authorized user to obtain remote desktop control of his or her office system. In the absence of a user-controlled system on the AUC network, permissions will be configured only for remote access to the systems to which the user has prior authorized access.
AUC Network:	refers to the interconnected local and wide area networks maintained and managed by the AUC's IT units.
ISP	Internet Service Provider
Token	A device or software used to provide a password that is valid for one time and a short period

Policy/Procedures

Roles and Responsibilities

1. AUC IT is responsible for:
    1. Providing VPN access to approved employees and documenting VPN Access Request requests
    2. Providing all software as required for the VPN operations and in order to match compliance with AUC Information security requirements.
2. Personal devices used by users for remotely accessing AUC's internal network/services via VPN must match the criteria advised by AUC IT.

VPN Approval

1. Only approved AUC staff, faculty, and other authorized parties (students, vendors, etc.) may utilize the VPN.
2. Approval should be granted upon a request that is filled by the requesting staff, faculty, or the sponsor by submitting the appropriate request form.
3. IT Security unit handles the request review and fulfillment operationally and technically. IT support units "like IT Help Desk and Desktop Support" offer support to the end-user regarding setup and basic troubleshooting
4. The approvals are handled as the following: -
    a. Applicable students' requests must be accompanied by a faculty sponsor
    b. Applicable faculty and staff requests must be approved by the direct manager/dean/chair
    c. Non-AUC personnel and supporting companies (contractors, consultants, vendors…etc.) requests must be filed and approved by the respective business sponsor
5. The request must contain the exact services that will be used; for related technical requests, IP addresses and ports numbers must be submitted. No open/unlimited access is allowed. If the requested service, IP address, or ports are not publicly available to users internally, then the relevant service/application owner must approve this request additionally.
6. The VPN users and sponsors must have read, understood, and acknowledged this policy before using the service or sponsoring a third-party request.
7. VPN access granting for non-AUC personnel (consultants, vendors, etc.) must be preceded by a signed confidentiality agreement that has been approved by the legal office. Accounts will not be issued until this process has been completed and approved collectively by the information security office.

8. VPN accounts for non-AUC personnel, and students must be time-bounded. The account duration is specified by the sponsor within the request form. The sponsor is responsible for notifying IT to disable the accounts whenever the need does no longer exist or if the contractual relationship with the VPN user has been discontinued.

9. Critical accounts specified by the Information Security office will have an extra factor for authentication "hardware token, software token, SMS…etc."

VPN User Responsibilities

1. By using VPN technology with personal equipment, users must understand that their machines are an extension of the AUC's network and as such are subject to the same rules and regulations that apply to AUC-owned equipment, and their machines must be configured to comply with all AUC security policies.
2. All computers (including personal computers) connected to AUC networks via VPN must use up-to-date virus-scanning software and virus definitions. In addition, all relevant security updates must be installed.

3. The VPN service functionality depends on Internet access as a prerequisite. Therefore, the user is responsible for selecting an ISP, coordinating installation, installing any required software, and paying associated fees for having the Internet connectivity available and stable.
4. It is the responsibility of the AUC VPN user to ensure that unauthorized users are not allowed to use the granted VPN service or access to AUC network.
5. VPN access is controlled using ID and password authentication. The password must comply with the AUC's password policy.

6. The users who will receive a second-factor authentication tool have to safeguard that token, software, phone used… etc. at all times
7. Each VPN user must have a unique account. Shared profiles are not permitted.

VPN Restrictions

1. AUC's VPN services are to be used solely for AUC business. All users are subject to auditing of VPN usage.
2. Only one network connection is allowed per VPN session.
3. AUC's network access will be limited to the resources to which they need access. Open access to accounts is not permitted. In addition, VPN tunnels made to the AUC must contain access restrictions at the remote termination point of the tunnel that prevents unauthorized access to the AUC network. Tunnels should not be accessible by unauthorized users or the Internet.
4. All VPN gateways on the AUC network will be set up and managed by the AUC's IT department. User-created VPN gateways are not permitted on the AUC network.
5. Inactive VPN accounts that exceed 6 months will be deleted.
6. HR office, Provost office, and all VPN accounts sponsors are responsible for providing the list of users that have ended or frozen their relation with AUC as accordingly; their VPN accounts will be disabled

VPN with non-AUC locations

1. VPN connections with vendors, cloud providers, …etc. Requests must be approved by the CTO operationally and by Information Security Office from a security perspective.
2. A proper mutual confidentiality agreement must be signed and approved by the legal office.

3. Relevant documentation and assigned business and technical focal points of contact from both sides must be in place.
4. Access to AUC network and services must be restricted to the minimum; access details must be approved by the relevant AUC service owner and AUC technical administrator.
5. In case of contract/service discontinuation, the AUC business focal point must notify AUC IT to disconnect the VPN connection.

Forms/Instructions

Kindly contact the IT Help Desk at support@aucegypt.edu

History/Revision Dates

Origination Date:	January 30th, 2018
Last Amended Date:	January 30th, 2018
Last Review Date:	October, 2022
Next Review Date:	October 2025