UNIVERSITY OF GEORGIA

Network Access Policy

Policy Number

Pending

Policy

1. Purpose

The Network Access Policy outlines the standards for securely connecting devices to the University of Georgia (UGA) campus network. The purpose of this policy is to ensure the integrity, availability, and confidentiality of university resources, protect against unauthorized access, minimize potential security risks, and ensure compliance with laws and regulations.

2. Scope

All departments and units and all users of the UGA campus network, including faculty, staff, students, guests, and any other individuals granted access, are required to comply with this policy. All devices connected to the UGA campus network including devices owned by the university, devices owned privately or by a third party, and devices owned by guests with temporary access to the campus network are required to comply with this policy.

3. Policy

a. Identification, Authentication and Attribution

Users must authenticate in order to connect a device to the UGA campus network, or a device must be registered to an individual user in a system of record operated by Enterprise Information Technology Services (EITS). Authentication or registration to an individual shall be sufficient to ensure network activity can be attributed to an individual.

b. Device Security

All devices connecting to the UGA campus network must adhere to the following security requirements:

i. *Security Updates* - Devices shall be configured with an operating system supported by the manufacturer. All applicable security updates should be installed (I) as soon as practicable and at a minimum within 2 weeks of the security update release date or (II) according to established change and patch management criteria established by the operating university department or unit. Critical security updates declared as “Emergency Patches” by the Office of Information Security must be implemented immediately without delay.

ii. *Anti-Malware Software* - Anti-malware software shall be used and kept updated on devices where the use of such software is practical.

iii. *Access Control and Passwords* - Devices shall require sign-on or login for users. Users shall be authenticated by means of passwords or by other authentication processes (e.g., biometrics or Smart Cards). Unencrypted authentication mechanisms or protocols are prohibited. When passwords are used to control access, password construction and management shall comply with the UGA Password Standard. Default or blank passwords on devices are prohibited.

iv. *Un-authenticated Email Relays and Proxy Services* - Devices shall not operate as an unauthenticated email relay or proxy service.

v. *Unauthorized Network Bridges and Network NATs*– Devices shall not operate an unauthenticated bridge or NAT.

vi. *Unnecessary Services* - Services that are not necessary for the device to perform its function or mission shall be disabled.

c. Authorized Wireless Networks

EITS provides wireless Wi-Fi networks for students, faculty, staff, and guests. These authorized wireless networks include “eduroam,” “PAWS-Secure,” and “UGA_Visitors_Wifi.”

Wireless networks operated by individual departments or end users and providing access to the UGA campus network are prohibited.

d. Remote Access

i. Remote Access Virtual Private Network (VPN)

Remote access to the university network shall be facilitated through the Remote Access VPN provided by EITS. End user or department and unit operated technologies providing remote access to the UGA Campus Network are prohibited.

ii. Multi-Factor Authentication (MFA)

All remote access to devices on the UGA campus network or to internal network services and resources shall require strong authentication via the ArchPass multi-factor authentication service provided by EITS.

4. Implementation

Each University department/unit is responsible for implementing, reviewing, and monitoring internal policies, practices, etc. to assure compliance with this standard.

5. Enforcement

The Vice President for IT is responsible for enforcing this policy.

6. Consequences and Sanctions

Any device or network segment that does not meet the requirements outlined in this policy may be removed from the UGA campus network, disabled, reconfigured, etc. as appropriate until the device or network segment can be brought into compliance.

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

7. Exceptions

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request an exception to this policy, contact the Office of Information

Security at infosec@uga.edu or complete the Request Policy Help form located at: https://uga.teamdynamix.com/TDClient/2060/Portal/Requests/ServiceDet?ID=10066.

References & Related Documents

Policies on the Use of Computers - https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/aup/
Password Standard - https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/passwords/password_standard
ArchPass Standard - https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/archpass_standard/
Remote Access VPN - https://eits.uga.edu/access_and_security/infosec/tools/vpn/
ArchPass - https://eits.uga.edu/access_and_security/infosec/tools/archpass/
Guide to Performance Management - https://hr.uga.edu/Current_Employees/Managers/Manager_Performance_Management/
Student Code of Conduct - https://conduct.uga.edu/code-of-conduct/

Key Words

Network, Device, Security, Wireless, Remote, VPN, MFA, ArchPass

Approvals & Revisions

Approved by Vice President for Information Technology
Version 1 – replaces Minimum Standards for Networked Devices

Policy Contacts

University Senior Administrator: Vice President for Information Technology
Policy Owner (*Responsible Unit):* Chief Information Security Officer (Office of Information Security)
Contact (*Name/Title, Phone/email*): Ben Myers, Associate VP for IT and Chief Information Security Officer - bmyers@uga.edu