Augusta University
Policy Library

Remote Access Policy

Policy Manager: Chief Information Officer

1.0 POLICY STATEMENT
Augusta University is committed to protecting the confidentiality, integrity and availability of its information resources while enabling secure and flexible access for academic, research, and administrative purposes. Remote access to University systems—whether from off-campus locations or non-University networks—shall be conducted in a manner that safeguards institutional data and supports the operational needs of the University community.

All users who access University networks or information systems remotely shall use approved, secure connection methods and shall comply with all applicable University policies, information-security standards, and legal or regulatory requirements. Users are responsible for ensuring that any device used for remote access meets minimum security controls, including up-to-date software, strong authentication, and protection against unauthorized use.

The University reserves the right to monitor, manage, and restrict remote access to its systems to maintain security and operational integrity. Unauthorized or insecure remote access poses significant risks to university data and infrastructure and is strictly prohibited. Failure to comply with this policy may result in suspension of access privileges and other corrective actions.

This policy supports the University's mission by enabling secure, reliable remote connectivity while protecting the digital environment essential to teaching, learning, research, and administration.

2.0 AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☐ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☐ Other:

3.0 DEFINITIONS
This section defines key terms used in this policy to support consistent understanding and application.

Remote Access means accessing AU networks, systems, applications, or organizational data from off-campus locations, non-AU networks, or via third-party networks

Internal Remote Access means remote access that establishes a connection into AU internal network resources (for example, through AU-managed VPN, virtual desktop infrastructure (VDI), bastion/jump services, or other AU IT-approved secure access methods)

Internet-Facing Application Access means accessing AU-approved services that are intended to be reachable from the internet without connecting into the AU internal network (for example, web-based email such as Outlook on the web, cloud collaboration tools, or other AU IT-approved web applications)

AU-approved secure methods mean remote access services and configurations authorized and maintained by AU IT

University-owned and managed means AU-owned devices enrolled in AU endpoint management and configured in accordance with AU IT configuration standards.

Additional definitions are provided in the *Cybersecurity Charter* (Appendix B) in the Augusta University Policy Library.

4.0 SCOPE

This section describes where this policy applies, including the types of data formats, systems, and environments covered.

Abstract: Scope includes remote access to AU systems and organizational data in on-premises, cloud-hosted, and third-party environments.

This policy applies to all remote access to Augusta University (AU) networks, systems, applications, and organizational data, including access to on-premises and cloud-hosted services, whether access is provided through AU IT or third parties. It applies to all users and devices used to establish remote access, including workforce members, students, and Vendors/Contractors, when accessing AU resources.

For clarity, this policy distinguishes between (1) **Internal Remote Access** (connecting into AU internal network resources via AU approved secure methods) and (2) **Internet-Facing Application Access** (using AU-approved applications that are designed to be accessed directly from the internet via a browser or client application). Both are forms of remote access; however, the strict managed-device requirement in Section 6.1.2 applies to establishing remote connections to **internal** organizational resources. Access to AU-approved internet-facing applications may be permitted under the limited conditions described in Section 6.1.2.

5.0 ROLES AND RESPONSIBILITIES

This section describes who is responsible for implementing, maintaining and managing remote access.

5.1 Division of Information Technology
- 5.1.1 Shall approve and authorize AU-managed remote access services and configurations.
- 5.1.2 Shall provide and maintain secure remote access options for the organization.
- 5.1.3 Shall establish logging and monitoring of remote access session activity.

5.2 System Owners/Data Owners

5.2.1 Shall approve remote access to the specific systems and data they own (or administer), consistent with documented business need, least privilege, and applicable data classification requirements.

5.3 AU Workforce Members

5.3.1 Shall utilize remote access in a responsible manner.

5.3.2 Department managers, System Owners, or Security Authorities shall request remote access for workforce members or Vendors/Contractors as needed to perform job duties.

5.3.3 Shall ensure workstations used to connect remotely to university resources meet minimum AU security standards per the IT Configuration Standards Policy.

5.3.4 Shall report any suspected violations or non-compliance with this policy to AU Cyber Defense at 72CYBER@augusta.edu.

5.4 Vendors/Contractors

5.4.1 Shall be responsible for complying with requirements put forth by this policy, applicable contract requirements, and AU IT security controls (including MFA, encryption, and monitoring/logging, as applicable). Vendors/Contractors shall promptly report suspected compromise of vendor credentials or remote access to AU IT/Cyber Defense.

6.0 REQUIREMENTS

This section sets the minimum requirements for granting, maintaining and terminating remote access.

Abstract: Remote access shall be approved, least privilege, and performed using AU-approved secure methods with strong encryption, MFA, logging/monitoring, and device security requirements. AU-owned and AU-managed devices are required for internal remote connections unless an approved exception applies.

6.1 AU Workforce Members

6.1.1 Users shall submit requests for approval to be provided with remote access via ticket to AU IT. Remote access approvals shall be based on documented business need and least privilege. AU IT may require periodic revalidation of access and may implement time-bound access, just-in-time access, or other technical controls for higher-risk systems and privileged access. Additional access requirements may apply for certain datasets under the Data Management and Classification Policy.

6.1.2 **Internal Remote Access:** Only University-owned and managed devices are permitted to establish remote connections to internal organizational resources. Personal/BYOD devices are prohibited from establishing remote connections to internal resources.

6.1.3 **Internet-Facing Application Access (e.g., browser-based access to AU-approved services such as Outlook on the web):** Access to AU-approved internet-facing applications from a non-managed device is limited to web-based access that enforces MFA. For non-managed devices, users shall not download, sync, cache for offline use, or otherwise store AU Confidential data locally (including through client application "sync" features), unless explicitly authorized and protected in accordance with AU standards. If a service or client application cannot reasonably prevent local storage of AU Confidential data on a non-managed device, it shall not be used from that non-managed device. Any other deviation requires an approved exception through the AU Cyber Defense GRC Exception to Policy (ETP) process.

6.1.4 Remote access to organizational datacenter and internal network resources shall use AU-approved secure access methods and shall not expose administrative protocols (e.g., RDP, SSH, management ports) directly to the public internet such as directly connecting from home to an internal server using Remote Desktop Protocol (RDP) or SSH over the internet is prohibited; accessing an AU-approved internet-facing web application in a browser (e.g., Outlook on the web) is not considered exposing an administrative protocol. Remote administration shall be performed using AU- approved tools and configurations (e.g., VPN with MFA, privileged access controls, bastion/jump services, or other AU IT-approved methods).

6.1.5 A user's remote access shall be revoked by AU IT as a result of a violation of this policy or by request of the associated department.

6.2 Vendors/Contractors

6.2.1 University departments shall submit vendor remote access requests for any Vendors/Contractors that require access to internal organizational resources via the Vendor VPN request form.

6.2.2 Vendor remote access requests shall be reviewed and approved by AU IT, and access shall be restricted to only resources the Vendor/Contractor requires according to the agreed contract requirements.

6.2.3 Approved vendor remote access requests may be valid for six (6) months, at which point approval shall be resubmitted to continue access.

6.3 All Remote Access Users

6.3.1 All remote access activity shall be logged and monitored by AU IT. Remote access logs may include user identity, device identifier, source IP/location indicators, authentication events, session start/stop, and accessed services as technically feasible. Logs shall be retained and protected in accordance with AU logging standards and records retention requirements and may be used for security, audit, investigation, and operational purposes.

6.3.2 Workforce members and Vendors/Contractors shall only be granted remote access to resources needed to perform their job responsibilities.

6.3.3 Remote access to university resources shall be conducted exclusively through AU-approved secure methods that use strong encryption for data in transit consistent with AU standards and applicable NIST or FIPS guidance.

6.3.4 Remote users shall comply with the Data Security requirements in Acceptable Use of Information Technology and with the Data Management and Classification Policy. Confidential data shall not be stored locally on endpoints unless explicitly authorized and protected by required controls (e.g., encryption) in accordance with AU standards.

6.3.5 All remote users shall ensure remote access sessions, including access to data, credentials, and unattended or unsecured workstations, are not shared with unauthorized users.

6.3.6 All remote access shall be protected by multi-factor authentication (MFA) (see Section 6.1.2). AU IT may require phishing-resistant MFA and/or additional controls for privileged access and higher-risk systems.

6.3.7 MFA requirements apply to both Internal Remote Access (e.g., VPN/VDI) and Internet-Facing Application Access (e.g., AU-approved web applications) as described in Section 6.1.2.

6.3.8 When using Internet-Facing Application Access from a non-managed device, users shall not download, sync, cache for offline use, or otherwise store AU Confidential data locally, unless explicitly authorized and protected in accordance with AU standards (see Section 6.1.2).

6.3.9 Remote access sessions shall enforce session timeouts and automatic disconnections for periods of inactivity where applicable.

6.3.10 Devices used for remote access shall comply with the Vulnerability and Patch Management Policy and the Acceptable Use of Information Technology Policy.

6.3.11 In the event of an incident or data compromise, all remote users shall immediately notify AU Cyber Defense at 72Cyber@augusta.edu or the Compliance Hotline at 1-800-576-6623.

6.3.12 Remote access may be blocked or restricted from certain countries/regions, networks, or locations, or for certain sanctioned parties, consistent with applicable federal and state requirements and AU risk decisions (including guidance such as OFAC). Users traveling internationally should follow AU travel guidance and may be required to use additional protective measures as directed by AU IT.

7.0 COMPLIANCE

This section explains how compliance with this policy is managed, including how to request documented exceptions and the potential consequences of non-compliance.

Abstract:

- If you cannot comply, you shall request a documented exception through the ETP process.
- Approved exceptions shall be time-limited and reviewed periodically.
- Non-compliance may result in disciplinary action and/or suspension or revocation of system and data access.

Exceptions: If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request approval for a documented exception through the AU Cyber Defense Governance, Risk and Compliance (GRC) Exception to Policy (ETP) process. (Service Now Knowledge Base Article Computer Standard Configuration Exception Request KB2300201). All approved exceptions shall have a defined expiration date and shall be reviewed periodically for continued necessity.

Exception conditions: Failure to adhere to the approval conditions outlined in an approved exception to policy may result in revocation of the exception.

AU may suspend or revoke remote access at any time based on security risk, suspected compromise, policy violation, or failure to meet approved exception conditions.

Non-compliance: Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment, as well as other administrative action as appropriate. Sanctions may also include suspension, limitation, or revocation of access to AU's computing environment, systems, applications, networks, and data.

8.0 REFERENCES & SUPPORTING DOCUMENTS

This section lists external regulations, frameworks, USG requirements, and AU supporting resources that inform or support this policy.

NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations
NIST Special Publication 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security

University System of Georgia (USG) Information Technology (IT) Handbook
Board of Regents (BOR) Policy Manual, Section 10.4.2 (Information Security)

Service Now Knowledge Base Article, KB2300201, Computer Standard Configuration Exception Request

9.0 RELATED POLICIES

This section lists internal policies, standards and resources that inform or support this policy.

Acceptable Use of Information Technology
Cybersecurity Charter
Data Management and Classification Policy
Encryption Policy
IT Configuration Standards Policy
Password Protection Policy
Vulnerability and Patch Management Policy

All AU Policies can be found online in the Augusta University Policy Library.

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/13/2026

President, Augusta University Date: 5/14/2026