Augusta University
Policy Library

Remote Access Policy

Policy Owner: Information Technology Support and Services

POLICY STATEMENT

It is the responsibility of Augusta University workforce (faculty, staff, students and volunteers), contractors, vendors and agents who have been granted remote access privileges to Augusta University's network infrastructure to ensure that their remote access connection is given the same consideration as the user's on-site connection to Augusta University's network. Remote access to confidential/regulated data (ex. protected health information (PHI), personally identifiable information (PII) and student records) is only granted to authorized users based on role within the organization and must connect using Augusta University's approved standard(s) for secure data transmission.

Remote access to the Internet through the Augusta University network for recreational use by non-Augusta University workforce members on any device is not permitted.

Augusta University workforce, contractors, vendors and agents who have been granted remote access privileges bear responsibility and shall be held accountable in accordance with the HIPAA sanctions and all relevant legal remedies up to and including termination, should the remote access privilege be misused.

Augusta University has a moral, legal and ethical obligation to maintain the confidentiality, integrity and availability of confidential/regulated data, including data accessed remotely. To ensure Augusta University is able to meet this responsibility, remote access to confidential/regulated data will be restricted to those persons who have an authorized need to know and are members of the Augusta University workforce or under written agreement with Augusta University to provide services such as Business Associates.

The purpose of this policy is to define requirements for connecting to Augusta University's network from any remote host. These requirements are designed to minimize the potential exposure to Augusta University from damages that may result from unauthorized use of institutional resources. Damages include the loss and/or potential exposure of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

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: All members of Augusta University workforce, contractors, vendors and agents to include its Business Associates

Office of Compliance and Enterprise Risk Management Use Only
Policy No.: 630
Policy Sponsor: Type the title of the Executive Leader of the department.
Originally Issued: Not Set
Last Revision: 11/01/2016
Last Review: 06/09/2017

DEFINITIONS

Business Associate: A person or entity that creates, receives, maintains or transmits protected health information to perform certain functions or activities on behalf of a covered entity.

Three categories of service providers are specifically identified as business associates under the final rule:

- Health information organizations, e-prescribing gateways, and other people or entities that provide data transmission services to a covered entity with respect to protected health information and that require access on a routine basis to such protected health information
- People or entities that offer personal health records to one or more individuals on behalf of a covered entity
- Subcontractors that create, receive, maintain or transmit protected health information on behalf of business associates

Confidential/Regulated Data: Any data regulated by federal, state, and/or local statutes or policy. This includes, but is not exclusive to protected health information, personally identifiable information about students or research subjects, information that could be used for identity theft, or data deemed business sensitive such that unauthorized disclosure could have a negative impact on Augusta University operational, financial, or reputational business relations.

Departmental Security Authority: Roles that include requesting access and permissions for various Augusta University clinical and administrative systems, assisting in information security awareness training and cooperating with the Enterprise Privacy Officer, Information Security Office, Human Resources, and Public Safety with incident investigations.

Dual homing: A dual-homed host is a term used to reference a type of firewall that uses two (or more) network interfaces. One connection is an internal network and the second connection is to the Internet. A dual-homed host works as a simple firewall provided there is no direct IP traffic between the Internet and the internal network.

Information Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Need to Know: Workforce member's, contractor's, vendor's and/or agent's access to information must be based on their job duties / assigned roles.

Personally identifiable: Any one or more of the following data elements in combination with an individual's first name or first name or first initial and last name, when either the name or the data elements are not encrypted or redacted:

- Social security number;
- Driver´s license number or state identification card number;

- Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the above, bulleted items when not in connection with the individual´s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

The term personally identifiable does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Protected Health Information (PHI): PHI means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Remote Access: Using any device, regardless of ownership, to access Augusta University information or information systems from outside the enterprise network. Examples would include: virtual private network (VPN), email access offsite, Citrix web access offsite, etc.

Split-tunneling: The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. This method of network access enables the user to access remote devices, such as a networked printer, at the same time as accessing the public network.

Workforce: Workforce means employees, students, volunteers, contracted personnel, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the covered entity or business associate.

PROCESS & PROCEDURES

Requirements

1. It is the responsibility of the Augusta University workforce, contractors, vendors and agents to limit the use and disclosure of confidential/regulated data for purposes that have permission, authorization, to include IRB approval, and/or by law.
2. Secure remote access must be strictly controlled. Control will be enforced through approved authentication method. For information on creating a strong passphrase see the Password Protection Policy.
3. At no time should any Augusta University workforce, contractors, vendors and/or agents provide their login or email password to anyone, not even family members.
4. Workforce, contractors, vendors and agents with remote access privileges understand that their Augusta University-owned or personal computer, mobile device or workstation that is remotely connected to Augusta University’s internal network, shall not connect to any other network at the same time.
5. Reconfiguration of any computing equipment for the purpose of split-tunneling or dual homing is not permitted.

6. During the remote connection to Augusta University, workforce, contractors, vendors and agents with remote access privileges understand that their Augusta University-owned or personal devices that can be remotely connected to Augusta University's internal network, shall not be shared with non-Augusta University workforce.
7. All remote hosts that connect to Augusta University's internal networks via remote access technologies must use the most up-to-date anti-virus software and operating system security patches.
8. In the event that an incident or data breach (i.e. information security incident) occurs during the course of remote access to confidential/regulated data, the workforce member and/or the Business Associate is required to immediately notify the Information Security Office at 706-840- 4266 or the Compliance Hotline at 1-800-576-6623. Both are available 24 hours/7 days a week/365 days a year.
9. Any workforce member found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.

   Note: Augusta University faculty, staff and students who violate the AU Medical Center (AUMC) Remote Access Policy will be disciplined through a collaboration of the Information Security Office, the Enterprise Privacy Officer and either Department of Human Resources or Augusta University Division of Student Affairs.

Remote Access Request

1. The Departmental Security Authority (SA) receives a request from a requesting supervisor of workforce member(s) who has an authorized need for remote access.
2. The SA will vet the workforce member's authorization for remote access through a documented approval process.
3. If the access request is validated by the SA, the SA places the request within Information Technology Services' (ITS) work management system for access to be granted.
4. ITS will receive the request, fulfill the requested access and provide information back to the SA on its completion status.
5. The ITS Service Desk is available as a resource for any troubleshooting needs at 706-721-4000.
6. Remote access privileges can be revoke by the SA by placing a request into ITS' work management system if they are no longer necessary.
7. Upon termination, the SA is responsible for submitting a "revoke all" request within the ITS work management system to remove all privileges to information systems.
8. The Information Security Office, in collaboration with the Enterprise Privacy Officer and the Department of Human Resources, reserves the right to remove remote access at any point.

REFERENCES & SUPPORTING DOCUMENTS

Student Remote Access User Agreement

Security Authority Remote Access Authorization Checklist

RELATED POLICIES
Intentionally left blank.

APPROVED BY:
President, Augusta University and CEO, AU Health System Date: 06/09/2017