University Policy
VPN Remote Access

Introduction

The Policy was created to comply with University System of Georgia (USG) information technology policies. Pursuant to the USG Information Technology Handbook, 5.12.1.

Purpose

This policy defines the necessary practices required to gain access to Albany State University's (ASU)'s Virtual Private Network (VPN). 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 ASU from damages which may result from unauthorized use of ASU resources. Damages may include the loss of sensitive or confidential data, intellectual property, damage to public image, or damage to critical internal systems and services.

Scope

The ASU VPN Remote Access Policy applies to all ASU employees, contractors, consultants, vendors, non-paid affiliates and agents with an ASU owned or personally owned computer, laptop, or workstation that require VPN access to ASU's network and network resources to perform necessary task when not on ASU's campus.

Policy

General

1. Approved ASU employees and authorized third parties may utilize VPN to connect to the campus network. Students, alumni, and student employees are NOT eligible to use VPN services.
2. VPN profiles will be created at the user's request once his/her department head and or approving authorities approve the VPN request. Additionally, the user must have read and signed both the VPN Remote Access Policy and Acceptable Use Policy.
3. VPN profiles for non-ASU personnel (contractors, vendors, non-paid affiliates etc.) must be approved by the ASU designated sponsor. Additionally, the VPN Access Request Form, VPN Policy, and the Confidentiality Agreement must be signed by the designated company's Approving Authority and filed with ASU's Non-Disclosure Agreement (NDA). Accounts will not be issued until this process has been completed.

Requirements

By using VPN technology, users must understand that their machines are a de facto extension of the ASU network, and as such are subject to the same policies and regulations that apply when connected directly to the campus ASU network.

1. Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any associated service issue. VPN services work best over broadband connections (cable modem or DSL).
2. All computers connected to ASU campus network via VPN must have up-to-date virus-software and virus definitions files. This anti-virus definition file must not be older than seven days. Use of anti-virus software other than ASU provided LANDesk anti-virus must be approved for use by the ASU Chief Information Security Officer (CISO). Additionally, all relevant software and security patches must be installed.
3. It is the responsibility of the employee or company with VPN privileges to ensure that unauthorized users are not allowed access to ASU campus networks.
4. VPN access must be strictly controlled. Control and access will be enforced using access control methodologies and end user authentication. All passwords must comply with the ASU Password Policy. Each VPN user must have a unique profile. Shared profiles are not permitted.

VPN Restrictions and Enforcement

1. ASU VPN services are to be used solely for ASU business and/or academic support purposes. All users are subject to auditing of VPN usage as per the ASU Acceptable Use Policy.
2. When actively connected to the ASU campus network, the VPN will force all traffic to and from the remote node through the VPN tunnel. Dual (split) tunneling is NOT permitted.
3. ASU campus network access for non-ASU personnel will be limited to the resources to which they need access. Open access for these accounts will not be permitted.
4. All VPN gateways on the campus network will be set up and managed by ASU Information Technology Services group (ITS). ITS will provide approved users with appropriate client software.
5. VPN users may be automatically disconnected from the ASU network after thirty minutes of inactivity.

Definitions (Optional)

Definitions associated with this policy are available in the Information Technology and Data Security Terms Glossary.

Accountability

This policy regulates the use of all VPN services to the ASU campus network. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified and resolved. Any ASU employee found to have intentionally violated this policy might be subject to disciplinary action, up to and including termination of employment. Non-ASU employees and vendors 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.

Exceptions

Exceptions to the ASU VPN Remote Access Policy, other than those previously discussed, are evaluated on a case-by-case basis by the Vice President and Chief Information Officer.

Contacts

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

References

- USG BOR IT Handbook, http://www.usg.edu/information_technology_handbook

Last Update

July 31, 2018