Policy Information

ISSUING OFFICE

Information Services

POLICY

This policy provides security requirements for all Liberty University employees/ faculty and any vendor or third party who are manipulating/accessing University data classified as confidential/restricted from remote locations.[1]

STANDARDS

Liberty employees and authorized third parties using the VPN or Microsoft Remote Desktop Connection, or any other technology used to remotely access Liberty University networks and computer systems must ensure that unauthorized users are not allowed access to internal University networks and associated information/data.

All individuals and machines connecting remotely are subject to the University?s Acceptable Use Policy.

All individuals connecting remotely should only connect to or have access to machines and resources they have permission and rights to use.[2]

All devices connecting remotely should have current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.

Multifactor authentication will be required when nonlocal maintenance sessions are established from an external network connection.[3]

Remote sessions connected via VPN will have all Internet traffic routed through

VPN and will not be allowed to have a simultaneous non-remote connection.[4]

Encrypt all non-console administrative access using strong cryptography.[5]

Additional requirements exist for remote work:

The machine/device must be trusted. This means that the machine/device must be built and maintained in a manner that creates confidence in the security of the machines. The use of non-Liberty University managed assets to access VPN, RDP, SSH or any other technology used to remotely access Liberty University networks and computer systems is prohibited. The use of Web kiosks and other untrusted machines for accessing any form of University sensitive or highly sensitive data (as defined in the Data Classification policy) or for entering a Liberty ID and password, or other University related credentials is an extremely dangerous practice and is a violation of this standard. Use of mobile devices to access email and other campus resources remotely should also be used with caution. Many of the same risks found with PC?s apply to these devices.

The user must be approved by the unit/department to work remotely.

All reasonable efforts must be made to protect University data, keeping it inhouse, on secured servers and devices wherever possible.

Users who connect remotely to University systems that contain confidential/ restricted data are required by University policy to use the campus VPN to maintain security of University data.[6]

Users needing access to their work desktop machines, or who need wider access to campus resources, must use the VPN in conjunction with an approved remote access technology such as Microsoft Remote Desktop Connection.

The use of Liberty University VPN services on personally owned or non-Liberty University managed devices is not permitted.

Any exceptions to the Remote Access Policy must be made in writing by the CIO or DCIO on a case-by-case basis.

SCOPE

Faculty, staff, consultant, vendor or any third-party

PURPOSE

The purpose of this policy is to state the requirements for remote access to computing resources and data hosted at Liberty University using VPN or Microsoft Remote Desktop Connection, or other remote access technologies.

DEFINITIONS

Strong Cryptography - ?Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and include both encryption (which is reversible) and hashing (which is ?one-way?; that is, not reversible).

At the time of publication, examples of industry-tested and accepted standards and algorithms include AES (128 bits and higher), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/ publications/) for more guidance in cryptographic key strengths and algorithms).? (From PCI DSS glossary, April 2018)

Virtual Private Network (VPN) - A secured private network connection built on top of a public network. It provides a secure encrypted connection, or tunnel, over the Internet between an individual computer/device and a private network. Use of VPN allows members of the Liberty community to securely access University network resources from off campus as if they were on campus.

REFERENCES

ISO/IEC 27001 2013 (More information available upon request)

6.2.2 Teleworking

NIST 800-53: More information here

MA-4 Nonlocal Maintenance

SC-7 Boundary Protection

NIST 800-171 More Information here

3.1 Access Control

3.7 Maintenance

3.13 System and Communications Protection

PCI DSS 3.2

Requirement 2: Do not use vendor-supplied defaults for systems passwords and other security parameters.

---

[1] . ISO 6.2.2 (ISO Policy 030103)

[2] . NIST 800-171 3.1.15

[3] . NIST 800-171 3.7.5; NIST 800-53 MA-4

[4] . NIST 800-171 3.13.7; NIST 800-53 SC-7(7)

[5] . PCI DSS 2.3

[6] . NIST 800-171 3.1.13, 3.1.14