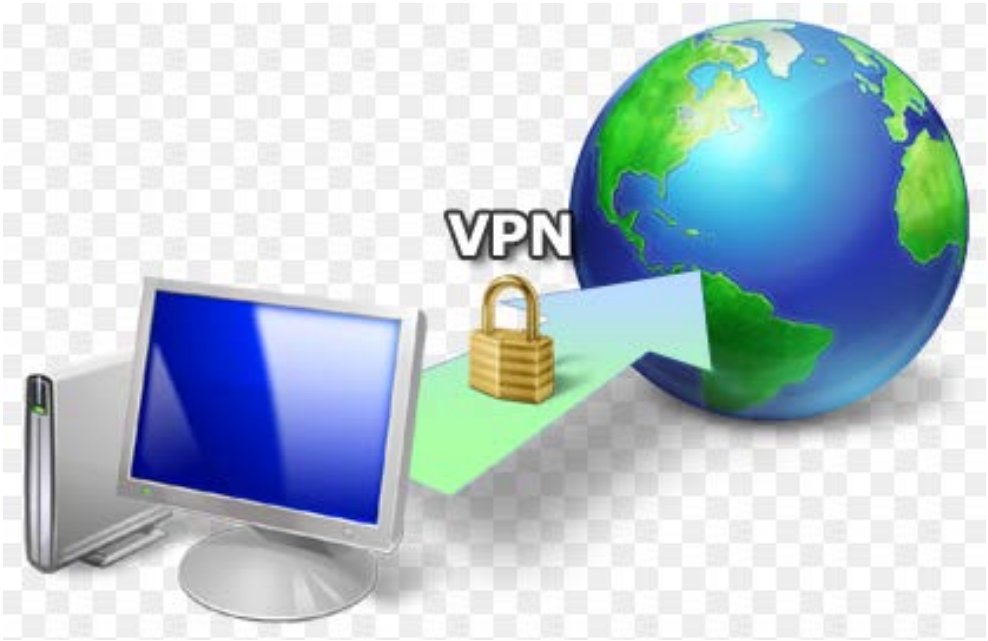

UTHSC G.U.A.R.D.

March 2017

IN THIS ISSUE

What is a VPN and Why Should You Care?

by Chris Madeksho, UTHSC Information Security Team

A VPN, or *Virtual Private Network*, creates a secure connection to a network from an outside source, such as the Internet. VPNs are used to protect sensitive data on a network from being accessed by those who should not have such access. It also allows the convenience of not having to be at a certain location (on-campus) while being able to get to important data.

Security is the main reason why an organization, such as UTHSC, would use a VPN. Having a secured VPN to a network is a necessary tool for anyone needing to access the network remotely. Today, most individual computer users wouldn't dream of connecting to the Internet without a firewall in place as well as up-to-date antivirus software. It is the same with a network. Using a VPN, a user cannot remotely access the network without having permission.

At UTHSC, we already have a VPN in place. However, up until now, just about anyone with a NetID has had the potential to reach our restricted data and networks from off campus using that VPN software. This presented a significant security risk. Starting in March, access via the VPN will be restricted to current employees and certain student groups. This is to ensure that individuals, even those with NetIDs, who have no legitimate reason for accessing the network while not on campus, cannot do so.

Anyone outside an approved group will be able to apply for VPN access.

When connected via VPN, the user's computer is temporarily part of the UTHSC network. System that require VPN to access when off-campus or on Eduroam include Volshare, all electronic health record (EHR) systems, IRIS (non-web - version), and others. For additional information about VPN access, visit www.uthsc.edu/vpn. For any information security concerns, contact the Information Security Team at itsecurity@uthsc.edu or (901)-448-1579.

Do You Use a VPN?

Learn what a VPN is and how it is used on our network.

Does Your Data Need Protection?

Understand the different classifications of data to know what needs protecting

Data Classification – Know What Type of Data You Possess

by Frank Davison and Chris Madeksho, UTHSC Information Security Team

Data classification is the process of organizing data into categories for security purposes. This is so owners and users of data can have clear definitions regarding their data and how well they need to protect it.

In the news, we hear numerous stories at the national level of leaks of *classified* information from government agencies, or how *classified* information was potentially stored improperly. People are routinely asked to sign confidentiality agreements before starting employment or projects stating that they will keep *confidential* the data with which they work.

On a personal level, every single individual is a data owner. Everyone has sensitive data, such as banking information, health records or even their social security number. No one wants to see his or her *private* information handled in an unsecure manner. Users of that data also have an obligation to protect the data while it is in their possession.

At the University of Tennessee and UTHSC specifically, policies have been established to categorize data and protect it based on its categorization*. There are four different levels of categorization of information. They are the following:

- **Classified** – information critical to our Nation's security
- **Confidential** – any data protected by regulatory, contractual or specialized agreements of understanding
- **Private** – information that is proprietary, not protected by regulation, contract or agreement but not open to public scrutiny
- **Public** – information freely available to the public

These levels are matched to the risk level in the University of Tennessee's policy IT0115 – Information and Computer System Classification.

IT0115 establishes *Federal Information Processing Standard 199* (FIPS 199) as the University's categorization model. When applying data classification standards, the severity of the potential impact of a breach must be examined. The loss of confidentiality, integrity or availability could be expected to have:

- Low impact (FIPS 199 low): limited adverse effect
- Moderate impact (FIPS 199 moderate): serious adverse effect
- High impact (FIPS 199 high): severe or catastrophic adverse effect on organization operations, organization assets or individuals

Knowing the classification of data a person is using is the first and most important step in knowing what needs to be done to protect that data.
For more information, contact the Information Security team at 901-448-1579 or itsecurity@uthsc.edu.

*UTHSC-Information Technology Practice InfoSec-GP-001.02- Information and System Categorization

UTHSC Categorization	IT0115 Risk Level
Classified	High
Confidential	Moderate
Private	Low
Public	Low