Remote Access Procedure\Guidance

Introduction

Remote network access is provided for those employees who find themselves doing business from a remote location, such as home or when traveling. Remote access to the UAEX data network is also provided to consultants and contractors as needed. While the connection is as secure as possible, remote access is inherently a security risk. Consequently, policy and procedures are required to minimize this risk.

Purpose

UAEX provides remote network access so that authorized personnel have access to network services from off site. The procedures and guidelines provided in this document were developed to minimize risk associated with this activity. It is, therefore, very important that employees, and contracted workers who are granted remote access privileges, follow these regulations.

Standards

Employees and authorized contractors are permitted remote network access through VPN client software with the approval of the requester's supervisor or by contractual agreement. VPN is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated connection fees.

Additionally,

- VPN access is provided through the Department of Information Technology. No other department may implement VPN services.
- Only the VPN client software distributed by IT may be used.
- VPN account names and passwords will be assigned by an IT network administrator or authorized delegate.
- It is the responsibility of employees and third parties with VPN privileges to ensure that unauthorized users are not allowed access to the UAEX network.
- All network activity during a VPN session is subject to UAEX policies and may be monitored for compliance.
- You are only allowed to connect to the UAEX network via VPN using work assigned equipment. Loading the VPN software on your personally owned equipment is not allowed. You must ensure that your work assigned equipment has the most up-to-date anti-virus software and updated virus definitions loaded.
- VPN users will be automatically disconnected from the UAEX network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN gateway is limited to an absolute connection time of 12 hours.

Key Performance Indicators (KPIs)

The following success of the policy will be assessed annually using the following quantifiable measures:

- No security issues over this connection
- No violations of procedures

Procedures

The following procedures should be followed to acquire VPN access:

Employees

1. Employees must discuss the viability of remote access with their immediate supervisor.
2. If the supervisor approves, enter a request for VPN services via the Remote Access Request Form.
3. The request must be filled out appropriately by the requester and their supervisor, and then sent to the IT Network Admins.
4. The IT Network Admins or delegate will setup the account and provide the software and setup instructions.
5. The employee\call center will install the VPN software on the target computer as instructed.
6. If you will be accessing your work computer using the VPN, you will need to install and setup RealVNC Server\Client. Instructions are available on our website or will be sent when requested.

Consultants and Contractors

1. Intention of use must be included with bid submissions and in final contracts.
2. The Remote Access Request Form must be completed for each individual who will be utilizing remote access.
3. Each individual must provide proof of anti-virus compliance to the IT Network Admins.
4. The IT Network Admins or delegate will provide the software and setup instructions.
5. The consultant/contractor will install the VPN software on the target computer as instructed.

Guidelines

The *minimum* hardware/software requirements for connectivity are:

- A work computer capable of providing appropriate network connectivity
- Broadband connection to the Internet via a local Internet Service Provider (ISP)
- Internet interface device (provided by and connects to the ISP network)
- Ethernet network interface in computer (connects to ISP interface device)
- VPN Client Software (provided by IT) and installation instructions
- RealVNC Server\Client software

Sanctions for Violations

Misuse of the remote access will be a violation and may result in:

1. Restriction or termination of a user's remote access to UAEX Computer and Network Resources.
2. The initiation of legal action by UAEX and/or respective federal, state or local law enforcement officials, including but not limited to, criminal prosecution under appropriate federal, state or local laws.
3. The requirement of the violator to provide restitution for any improper use of service; and disciplinary sanctions, which may include dismissal or expulsion.

Exceptions and Exemptions

Exception to or exemptions from any provision of this guidance must be approved by the Information Technology Security Group. Similarly, any questions about the contents of this guidance, or the applicability of this guidance to a particular situation should be referred to the Information Technology Security Group.