# Secure Remote Access Policy

Purpose: To insure the security of customer data, Hogland Office Equipment staff accessing customer systems remotely must adhere to established procedures to safeguard that data.

Policy Statement: All Hogland employees accessing customer business systems from our corporate office location must be authorized by the customer to access their systems and authorized to work remotely. He or she must then comply with Hogland security standards for secure data communication.

Responsibilities: Hogland Office Equipment staff will access customer systems from our corporate home office location (2401 Avenue F Lubbock, TX). Hogland Office Equipment staff will abide by the standards for remote access as determined by IT Staff/Director of IT. Hogland Office Equipment staff will complete and submit the Remote Access Authorization form to the customer for initial review; the customer will approve/deny the request and submit back to Hogland whereas the request will be submitted to the President or Director of IT for final approval and processing. Hogland Office Equipment / Information Technology staff must use secure system generated meeting ID’s via GoToAssist Express when managing customer infrastructure resources off-site.

Customer Responsibilities: You (the “customer”) understand and agree that prior to contacting Hogland Office Equipment to perform diagnostic or other services on your workstation pc or business system it is your responsibility to back-up the data, software, information or other files stored on your computer disks and/or drives. You (the customer) acknowledge and agree that Hogland Office Equipment shall not be responsible under any circumstance of any kind for any loss or corruption of data, software, and/or any damages to hardware or other computer peripherals.

## Hogland Standards for Remote Access

The following security standard, which defines required tools and practices, is intended to ensure that remote access to customer business systems and networks is performed in a secure fashion. These tools and practices will provide a baseline level of security in order to reduce security risks. The standard also implies that customer systems are only accessed via compliant computers and that malicious data is not transferred to the remote machine. Use of the following tools and practices is required in order to be in compliance with the standard:

**The following tools and practices are required by authorized employees connecting to customer workstations or networks:**

-Use local domain accounts to authenticate to the Hogland network
-All remote access requests must be generated using the secure GoToAssist Express tunnel
-Only run the services that are needed to perform the required job function
-Antivirus/Spyware removal software must be installed on the Hogland Office Equipment staff machine with the latest virus definitions installed and real-time scanning/protection enabled.
-Hogland Office Equipment staff workstations must have the latest operating system patches installed
-Firewall enabled

Acceptance ________________________________________________