

# Requirements for NICE interaction with the Wilco Network

This is intended to be part of the contract/SOW for Motorola. These can be pasted into the appropriate section or incorporated as reference.

- Operating systems, device firmware, and anti-virus must all run versions that are currently supported by the vendor as well as the latest service packs/patches applied that are compatible with NICE/Motorola. Every effort should be made to apply service packs and patches as soon as possible, especially those that are related to security.
- All system-level passwords (for servers, switches, firewalls) must be unique to Williamson County's installation (no shared passwords across installations).
- The servers must be part of the County Active Directory Domain, but they will be segregated in the domain such that the "standard" server policies will not apply for updates or other Group Policies that would apply to the OS patches or anti-virus.
- User logins to the system must utilize the user's Active Directory credentials for authentication. User access list will be defined by Williamson County Emergency Communications.
- Any logins to out-of-band management systems or other hardware logins (i.e. Integrated Lights-Out) must be non-default and unique to Williamson County's installation (no shared passwords across installations).
- Once data is transmitted to the Motorola-supplied firewall, NICE/Motorola is responsible for compliance when handling regulatory-protected data (CJIS, HIPAA, Texas Privacy Act, and others) as well as any audit requirements from the appropriate regulatory body (or compliance vendor).
- Ensure the Motorola installed firewall between the NICE Servers and County's network will support at least 1Gbps throughput.
- All software installed on end-user County computers must meet the requirements of the Technology Services Department and be installed by Technology Services Staff (per the County's Electronic System Use Policy).
- Designated, single CJIS POC representing the Williamson County Technology Services reserves the right to audit the systems for compliance with the provisions outlined above and other security risks that may pose a threat to the security and integrity of County data as well as the County network. This can be done with the assistance of the project staff or vendor, if desired, and County staff will not make any changes to any NICE system.

If there are risks or deficiencies found in the audit, these will be returned to the NICE/Motorola team for remediation. In addition, the County may block traffic to or from the NICE servers if there are serious risks or issues found until such issues are remediated.