



Complete IT recommends that all managed networks be configured in accordance with the standards outlined below. Doing so ensures proper network security and reliability, which ultimately results in the best possible experience for our customers.

We ask that you acknowledge the importance of these standards and work with Complete IT toward a common goal of successful implementation.

COMMON CONFIGURATION STANDARDS
Servers and workstations are deployed with remote monitoring and management agents
Anti-malware software is enabled on all Windows devices
Virtual machines and workstations receive weekly critical updates

CONFIGURATION STANDARDS – SERVERS
Servers run a licensed and supported copy of Windows Server operating system
Servers must be under current hardware warranty
Servers use hardware RAID for local storage
Servers employ RocketCyber security monitoring agents
All servers are protected with backups with daily offsite data replication
Backup repository is stored on a separate, dedicated server

CONFIGURATION STANDARDS – WORKSTATIONS
Workstations run a licensed and supported copy of Windows Professional operating system
Data is stored on network file shares to protect against possible data loss
Workstations employ Bitlocker data encryption
Workstations employ RocketCyber security monitoring agents (<i>optional</i>)

CONFIGURATION STANDARDS – EMAIL AND CLOUD
Microsoft 365 or equivalent is used for email and file storage
Multi-factor authentication is enabled for all email accounts
Single sign on is used for local network and email authentication
Cloud storage / synchronization is employed file storage on mobile workstations
Mobile device management is employed for mobile devices and laptops (<i>optional</i>)

CONFIGURATION STANDARDS – NETWORK
Edge security is provided by an enterprise class firewall with valid vendor support agreement
Managed VLAN capable switches are used for local network connectivity
Complete IT has documented access to customer internet domains
802.1x enterprise authentication is employed for internal network access (<i>optional</i>)