Complete IT takes its responsibility to safeguard customer data seriously. As such, we impose strict mandates on our internal network to ensure that our trusted access can only be used by authorized technicians.

These security standards are periodically updated to reflect industry best-practices and the latest available security offerings. The current revision of these standards can be found at the following link: CIT Standards

PHYSICAL SECURITY
Secure building access with locked suite
Complete IT suite has a monitored alarm system with unique code per employee
Motion sensitive security cameras cover suite entrances and working areas
Locked cage protects all CIT servers and network equipment within the suite

INTERNAL NETWORK SECURITY
Remote access to Complete IT networks requires multi-factor authentication
Access to third party services used for customer administration requires multi-factor authentication
Command and control applications are deployed in a secure colocation facility
Server and workstation builds are performed on a separate VLAN with no internal network access
Internal wireless access is restricted to domain joined computers
Internal wireless employs both 802.1x enterprise authentication and MAC address filtering
All internet domains under Complete IT management are protected via multi-factor authentication
Internal network administration and access to sensitive documentation is limited senior staff only
UAC and software firewalls are enabled on all Windows devices and enforced by domain policy

REMOTE ADMINISTRATION
All administrative tasks are performed using secure protocols
Remote administration is restricted to Complete IT public IP addresses wherever possible
Complete IT employees use non-privileged accounts on their local workstations
Technicians must use unique credentials to perform changes to workstations requiring elevated privileges
SNMP access is limited to read only and restricted by source IP address
Customer notes stored in cloud-based SOC 2-compliant IT documentation platform
All security related requests must be submitted via trouble ticket with management visibility
Secure notes are used to communicate sensitive information requiring unique URL and password for access
Secure notes are one-time use and automatically expire after 7 days if not retrieved
Network and server changes are tracked via Liongard IT Automation

4029 South Capital of Texas Highway
Austin, Texas 78704

(512) 674-4134
service@completeit.com

Complete IT internal network resources configured in accordance with the standards outlined below. Customers retain ultimate authority over their own networks and may not choose to implement all recommendations, however, highlighted items are required to comply with Complete IT minimum standards.

COMMON CONFIGURATION STANDARDS
Operating systems and software must be licensed and supported by the software vendor
Servers and workstations are deployed with remote monitoring and management agents
Servers and workstations employ RocketCyber security agents
UAC and software firewalls are enabled on all Windows devices
Windows Defender / Bitdefender anti-malware software is enabled on all Windows devices
All TPM-enabled servers and workstations employ data at rest encryption (Bitlocker)
Virtual machines and workstations receive weekly critical updates

CONFIGURATION STANDARDS – SERVERS
All servers are protected with Veeam Backup & Replication software with daily offsite data replication
All backup data is encrypted at rest with unique encryption keys assigned to each customer
Backups are stored on a dedicated server which is not domain joined and uses unique local credentials
All Windows file servers employ local VSS snapshots on data volumes
Unused network services are removed or disabled
All production servers employ RAID for local storage and are under hardware warranty
Unique accounts and passwords are used for authenticated services

CONFIGURATION STANDARDS – WORKSTATIONS
Cloud storage / synchronization is employed for document and file storage
Internal password policy requires a minimum of 14 characters with lockout triggered by failed attempts
Workstations sessions automatically lock after 15 minutes of inactivity

CONFIGURATION STANDARDS – NETWORK AND CLOUD
Edge security is provided by an enterprise class firewall with valid vendor support agreement
Multi-factor authentication is enabled for all email accounts
Managed network devices use unique, complex passwords
Single sign on is employed wherever possible using Microsoft Azure AD
Emails received from external recipients are tagged with warning message
Mobile device management is employed for mobile devices and laptops
802.1x enterprise authentication is employed for internal network access
Externally accessible network services are restricted via source IP address
Complete IT assumes management responsibility of customer registered internet domains
Separate VLANs are deployed for servers, workstations, guest wireless, network management, and printers