To ensure we can effectively manage and secure your IT (Information Technology) infrastructure, we require that all clients achieve, and maintain, compliance according to the NIST Cyber Security Framework In addition to this compliance all assets managed by dotnet must meet, or exceed, the baselines mentioned in the below categories

Windows Based Workstations, Laptops and Servers

*This includes all devices provided by the company as well as BYOD devices and devices not meeting these will have very limited, or no, access to company resources

Physical Hardware

- Support for TPM 2.0 or higher

*The following requirements are designated for newly procured devices

- Intel/AMD CPU 2021 or newer (i5,7,9 11xxx, Ryzen 5,7,9 5XXX)
- 16 GB Physical Memory (RAM)
- 250 GB Storage capacity for OS drive
- USB A,C 3.0 or higher
- HDMI/Display Port for video out
- Wifi 6 or Gigabit ethernet port

Software

- Remote Monitoring and Management agent from dotnet
- Windows Professional Operating System Must be a version supported by Microsoft
- Must maintain subscription from dotnet that includes at least the following
- dotnet recommended Advanced Malware Protection
- dotnet recommended Application Control Software
- dotnet recommended Antivirus Services
- dotnet recommended DNS Web Filtering
- dotnet recommended MFA application
- Must maintain a supported Firmware, and no more than 1 Major version behind
- All new software must be approved or elevated by dotnet prior to installation
- All Software needs to be supported by the vendor and receive current security patches
- Web browsers – Google Chrome, Microsoft Edge, Mozilla Firefox (with browser-stored passwords disabled)
- Adobe free PDF Viewer
- Microsoft Office 365
- Windows 10 or 11 Pro for workstations (including latest service packs and security updates)

- Windows Server 2016 Standard or newer
- Cloud Storage via OneDrive (for user files) and/or Sharepoint (for company files)
- Personal accounts are prohibited from OneDrive sync on company devices

Security

- Drive encryption on all internal storage devices
- Strong passwords on any user account with Admin privileges This includes local, domain, and Azure accounts (12 Character Minimum, both uppercase and lowercase, numbers, and symbols)
- dotnet MDR Security Software installed
- Attached to internal Active Directory, or Azure Active Directory
- All devices must be password protected and must lock themselves if idle for more than 15 minutes
- Local accounts are to be replaced with local AD, Microsoft Azure, or managed by a Zero Trust Solution

Network Hardware and Configuration

Physical Hardware

- Must be current and not in an EoL or unsupported status by the manufacturer
- Wall ethernet Jacks are to be locked down to specific devices through firewall/switch port security

Software

- All firewall appliances must maintain Universal Threat Management licensing on the appliance

Network Configuration

- Must be configured with deny first firewall rules
- Each Administrator must have a separate user account with MFA (Multifactor Authentication)
- Access from the outside will be limited to only dotnet
- All unused, or inactive, ports are to be disabled
- All personal and guest devices must be connected to a network separate from the primary office network
- Must have a firewall that is currently supported and receiving security updates from the vendor
- All IOT devices will be moved onto their own sub-network unless explicitly needed on the corporate network
- All wireless access points must be supported, and security protocols are required (WPA2/3)
- VLANs for production, office, guest networks, IoT

Email Security

End User and Administrator Accounts

- All users, including administrators, must be protected by MFA
- Strong password policies, with password rotation, are required
- Self-service password resets are to be disabled.
- Personal email accounts are not permitted in Outlook for desktop/cannot be troubleshooted.

Administration

- All accounts with administrative permissions will be properly segmented
- Standard users will NOT have administrative privileges
- No "Global" access account with be used as the day-to-day administration account
- All employees MUST go through dotnet provided email phishing training and testing

Backup and Disaster Recovery

Data Backup, Retention, and Recovery

- All devices identified by the client to be a Critical Asset are to be backed up at least 1 once per day
- All backed up devices will carry a minimum retention period of 30 days
- All backups are to be encrypted and stored on encrypted media, whether it be cloud or local
- All data recovery processes will be tested at least once per quarter
- A disaster recovery plan (DRP) and Incident Response Plan (IRP) must be maintained and updated once per calendar year

Security Assessments and Management

Assessments

- All new clients will undergo a base level audit within the first 90 days post onboarding
- All managed service clients will undergo, and sign off on, a yearly security review

General

- All purchased devices must come from reputable sources Used devices are prohibited without being inspected by dotnet personnel
- Access to physical network and server locations must have some form of access control into the physical room and into the network rack