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 technologies must meet, or exceed, the baselines mentioned in the below categories.

# Windows Based Workstations and Laptops

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

## Physical Hardware

- Support for TPM 2.0 or higher

## Software

- Remote Monitoring and Management agent from dotnet technologies (N-Able)
- Windows Professional Operating System. Must be a version supported by Microsoft.

## Security

- Bit locker drive encryption on all internal storage devices
- Strong passwords on any user account with Admin privileges. This includes local, domain, and Azure accounts.
- EDR Security Software by SentinelOne 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

# Network Hardware and Configuration

## Physical Hardware

- Must not be EoL or unsupported by the manufacture

## Software

- Must maintain subscription from manufacture that includes at least the following
    - Advanced Malware Protection
    - Application Control
    - Antivirus Services
    - Web Filtering

    - Intrusion Prevention
- Must maintain a supported Firmware, and no more than 1 Major version behind

### Configuration

- Must be configured with Deny first firewall rules
- Each Administrator must have own user account with MFA (Multifactor Authentication)
- Access from the outside will be limited to only dotnet technologies
- All unused, or unactive, ports are to be disabled
- All personal and guest devices must be connected to a network separate from the primary office network

## 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

### 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

## 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 during the onboarding process
- All managed service clients will undergo, and sign off on, a yearly security review