Ninja Inc Cyber Policy

The execution of executables, scripts, installers, programs, and applications shall be prevented from within base user profiles

The execution of executables, scripts, installers, programs, and applications shall be prevented from within temporary folders

Assets discovery shall be conducted automatically every ten (10) calendar days

The vulnerability scanner database shall be kept up-to-date

The vulnerability scanner shall be used daily to check for missing patches and updates for security vulnerabilities on internet facing assets

The vulnerability scanner shall be used every ten (10) calendar days to check for missing patches and updates for security vulnerabilities on all other assets

Patches, updates, and/or mitigations for vulnerabilities in internet facing assets are applied within two (2) weeks or forty-eight (48) hours if an exploit is known to exist

Patches, updates, and/or mitigations for vulnerabilities in all other assets are applied within one (1) month or two (2) weeks if an exploit is known to exist

Assets which are no longer supported are removed from any systems on which they are hosted

Microsoft Office macros shall be disabled unless an exception is requested and approved

Microsoft Office macros in external files shall be blocked

Microsoft Office macro antivirus scanning shall be enabled

Users shall be prevented from changing Microsoft Office settings

Web applications shall not process java from the internet

Web browsers shall not process web advertisements from the internet

Internet Explorer 11 shall be disabled

Users shall be prevented from changing web browser security settings

Requests for privileged access shall be validated

Privileged accounts shall be forbidden from accessing the internet, email, and web services

Privileged users shall use separate privileged and unprivileged environments

Unprivileged accounts shall be forbidden from logging into privileged environments

Privileged accounts, except for local admins, shall be forbidden from logging into unprivileged environments.

Local admin accounts shall be allowed to log into unprivileged environments

Data, software, and configurations settings shall be backed up weekly

All back ups shall be synchronized

All back ups shall be secured and hosted in an on-site location

All back ups shall be secured and hosted in an off-site location

Back up restoration shall be tested

Accounts, excluding backup admins, shall be forbidden from accessing the back ups of other accounts

Accounts, excluding backup admins, shall have read only access to back ups

Backup administrators shall have access to all backups

Backup admins shall have full permissions for all back ups

Application control shall be implemented on all assets

Application control employs a white-list method

All allowed and blocked execution events on all assets shall be centrally logged

Microsoft Office macros shall be blocked from making Win32 API calls.

Allowed and blocked Microsoft Office macro execution events shall be logged.

Microsoft Office is blocked from creating child processes.

Microsoft Office shall be blocked from creating executable content.

Microsoft Office shall be blocked from injecting code into other processes.

Microsoft Office shall be configured to prevent activation of OLE packages.

Users shall be forbidden from changing Microsoft Office security settings

PDF software shall be blocked from creating child processes.

Users shall be forbidden from changing PDF software security settings

Vendor hardening guidance for web browsers, Microsoft Office and PDF software shall be implemented.

Blocked PowerShell script execution events shall be logged.

Privileged access to systems and applications shall be automatically disabled after 12 months unless revalidated

Privileged access to systems and applications shall be automatically disabled after forty-five (45) days of inactivity

Privileged operating environments shall not be virtualised within unprivileged operating environments

Administrative activities shall be conducted through jump servers.

Credentials for local administrator accounts and service accounts shall be long, unique, unpredictable and managed.

Privileged access events shall be logged.

Privileged account and group management events shall be logged.

Microsoft's 'recommended block rules' shall be implemented.

Microsoft's 'recommended driver block rules' shall be implemented.

Application control rulesets shall be validated annually

Event logs shall be protected from unauthorised modification and deletion.

Event logs shall be monitored for signs of compromise and actioned when any signs of compromise are detected.