Assessment Form

Techtron Group1

HARDWARE

Asset Inventory		
	At Risk	Asset Inventory is not being performed.
	Needs Attention	Asset Inventory is manual and time consuming.
	Needs Attention	Asset inventory is manual for Chromebooks and tablets.
	Satisfactory	Asset Inventory is largely automated and included in the service agreement.

Power Management		
	At Risk	Existing UPS is at EOL and / or does not have enough capacity to support the environment.
	Needs Attention	Battery backup is attached to server - however configuration has not been tested.
	Satisfactory	Mission Critical equipment is protected by a UPS.

Workstations		
	Not Applicable	There are no workstations.
	At Risk	Some workstations are past EOL or have warranty that has expired.
	Needs Attention	Some workstations are approaching EOL or warranty expiration.
	Satisfactory	Workstations are not approaching EOL or warranty expiration.

Servers		
	Not Applicable	There are no servers.
	At Risk	Some servers are past EOL or have warranty that has expired.
	Needs Attention	Some servers are approaching EOL or warranty expiration.
	Satisfactory	Servers are not approaching EOL or warranty expiration.

Storage		
	At Risk	Primary data storage is less than 20% free. Low free space can cause issues with back and maintenance tasks. It will impede the company's ability to scale the business.
	Needs Attention	Primary data storage is less than 30% free. Low free space can cause issues with back and maintenance tasks. It will impede the company's ability to scale the business.
	Acceptable Risk	There is no shared storage OR files reside on local workstations
	Satisfactory	Primary data storage is in the cloud and scale-able to meet business needs.
	Satisfactory	Primary data storage is located onsite and offers sufficient room for expansion/ growth.

Spare Device Inventory		
	At Risk	The company does not keep spare equipment on hand.
	Needs Attention	The company keeps only minimal spare equipment.
	Acceptable Risk	The company keeps only minimal spare equipment.
	Satisfactory	The company maintains at least 5% spare equipment.

Switching		
	At Risk	Switches are over 5 years old and not cloud managed/monitored. This will have performance implications and increases potential for failure and increased downtime.
	At Risk	Switches are beyond end of life as per vendor. Firmware updates and security patches will not be made available even if a vulnerability is discovered.
	Needs Attention	Switches are managed and VLANs are deployed, but cloud visibility is not available, which may impede monitoring and troubleshooting.
	Needs Attention	Client has deployed Next Generation cloud managed switches, but NOT Techtron approved and refreshing them on a schedule as part of regular lifecycle management.
	Satisfactory	Client has deployed Techtron approved Next Generation cloud managed switches (Unifi) and refreshing them on a schedule as part of regular lifecycle management.

Firewall - Internet Security Appliance		
	At Risk	Current device is a router only and lacks monitoring and up to date security features.
	Needs Attention	Current firewall is not configured to block unwanted content.
	Needs Attention	Firewall is managed and up to date, but nearing the end of its lifespan.
	Satisfactory	Sophos XG Firewall is included and managed.

WiFi		
	Not Applicable	WiFi does not exist and the organization has no business case to introduce it into the environment.
	At Risk	Wireless is ad-hoc and lacks visibility and management.
	At Risk	Wireless hardware is beyond end of life. Firmware updates and security patches will not be made available even if a vulnerability is discovered.
	Needs Attention	Wireless is managed, separated SSID's for guest and staff, but no separate VLANs, or MAC Authentication, additional security controls required
	Satisfactory	Wireless is managed, separated into VLANs, with MAC Authentication, and allows for guest access separate from corporate data networks.

Business Applications / Software

Hosted Email		
	At Risk	Office uses consumer grade email with minimal security features.
	Needs Attention	Google Apps for Business in in place. We recommend Office365.
	Needs Attention	Email is hosted with Office 365 but security standards are not aligned with best practices.
	Satisfactory	Email is outsourced to Office 365, with Office 365 Defender and recommended security controls enabled, including email encryption.

DLP Policy		
	Not Applicable	Users do not send sensitive information by email.
	Unknown	Unknown - more information is required.
	At Risk	Sensitive information is being sent by email without any DLP policies in place.
	Satisfactory	DLP Policies have been configured to manage the risk of emailing sensitive information.

Operating System		
	At Risk	Some Operating Systems are no longer vendor supported, which creates a security risk to the company and places the company out of major industry best practices and compliances.
	Satisfactory	All Operating Systems are current and vendor supported.

Software License Management		
	At Risk	License Management is not being performed. Client may be at risk of an audit from vendors like Microsoft.
	Satisfactory	License Management is handled by the IT Provider and the client is believed to be in compliance.

SECURITY

Microsoft Conditional Access Policy		
	At Risk	No Conditional Access Policy is in place.
	Needs Attention	Basic Conditional Access Policies are in place, but further restrictions are recommended.
	Satisfactory	All Recommended Conditional Access Policies are in place and are reviewed on a regular basis.

Dark Web Monitoring		
	At Risk	No Dark Web monitoring is in place.
	Satisfactory	The Dark Web is being monitored for employee credentials and a process is in place to provide additional training if/when credentials are breached.

Directory Services		
	At Risk	No central source of authentication is in use. This creates unnecessary risk/exposure caused by lack of accountability and an inability to deploy adequate security policies.
	Needs Attention	Users, groups, and permissions are managed in Azure (free), which will limit group policy capabilities.
	Satisfactory	User accounts and permissions are authenticated against an onsite Domain Controller.
	Satisfactory	User accounts and permissions are authenticated against Azure (paid), which offers a robust cloud based authentication system.
	Satisfactory	User accounts and permissions are authenticated against Jumpcloud, which offers a robust cloud based authentication system.

Email Protection / Filtering		
	At Risk	There is no email anti-spam and/or virus filter in use. The email client provides filtering.
	Needs Attention	There is a 3rd party anti-spam and virus filter that is integrated with the hosted Exchange provider.
	Needs Attention	Minimal email filtering is provided by Office 365 but may be insufficient.
	Needs Attention	Minimal email filtering is provided by Google Apps but may be insufficient.
	Satisfactory	Microsoft Defender for Office 365 is deployed and protecting the email environment.
	Satisfactory	Third party email protection is enabled such as Mimecast or alternative

Endpoint Security Software		
	At Risk	Anti-virus is installed manually with some machines unprotected or out of date.
	Needs Attention	Anti-virus is managed internally using a server based console and all endpoints are up to date.
	Needs Attention	Quality anti-virus is installed and centrally managed.
	Satisfactory	Traditional Anti-virus was replaced with or is supplemented by Next Gen Endpoint Protection with Endpoint Detection and Response.

Intrusion Detection & Prevention		
	At Risk	IPS/IDS is not supported on current firewall solution.
	Satisfactory	IPS/IDS is included as part of Firewall as a Service subscription.

Virtual Networks (VLANs)		
	At Risk	The network does not have VLANs deployed which increases the threat from lateral movement of hackers and malware throughout the network.
	Needs Attention	A minimal number of VLANs have been deployed with access rules between them to provide an additional security layer but further segmentation is recommended to achieve best practices compliance.
	Satisfactory	A reasonable number of VLANs have been deployed with access rules between them to provide an additional security layer and aid in best practices compliance. MAC authentication has been configured for internal networks.

Workstation/Server Encryption		
	At Risk	Encryption is not in place on workstations and servers.
	At Risk	Some workstations are consumer grade and lack TPM hardware required for proper encryption.
	Acceptable Risk	Mobile Workstations are encrypted but desktops and servers are deemed not likely to be lost/stolen. The company understands the risks in the event that a workstation or server were removed from the o
	Satisfactory	TPM is activated and Bitlocker encryption is monitored on all systems authorized to contain sensitive information.

Mobile Device Encryption		
	Unknown	More information needed
	At Risk	Mobile device encryption is not enforced or mandated by company policy.
	Acceptable Risk	Mobile device encryption is not forced, but is required as per company policy.
	Satisfactory	MDM policy or Office 365 security policy includes forced mobile device encryption.

Mobile Device Management		
	At Risk	MDM is not in use.
	Needs Attention	Company owned mobile devices are managed, but personal devices are attached to company data which increases risk/exposure.
	Satisfactory	MDM is in place and company owned devices are managed and patched regularly.

Multi-Factor Authentication		
	At Risk	MFA is not deployed.
	Needs Attention	MFA is deployed for Office 365, but needs to be added for other critical systems.
	Acceptable Risk	MFA is not deployed. Customer is aware of the risks and accepts full responsibility for a breach of critical systems.
	Satisfactory	MFA is deployed on all critical systems including workstations, servers and web applications.

Password Manager		
	At Risk	No password management solution is in use, or users are left to find a solution on their own.
	Satisfactory	A Password Manager is in use and shared password vaults are shared among restricted groups only as necessary.

Scan & Fax to Email		
	Unknown	Unknown - more information is required.
	At Risk	Fax and/or scan to email are in use, causing potentially sensitive information to be stored un-encrypted inside mailboxes.
	Satisfactory	Fax and/or scan to email are not in use.
	Satisfactory	A Secure Fax service and/or scan to folder are in use, limiting the potential for sensitive information to wind up in email.

SIEM		
	At Risk	SIEM is not deployed.
	Needs Attention	A Limited SIEM or SOC Service is deployed, may not run 24/7 or offer a limited scope of security services
	Acceptable Risk	SIEM is not deployed due to cost. Organization is aware that this additional layer of security may stop threats missed by other layers of security, and is willing to accept the risk.
	Satisfactory	SIEM is deployed and monitored 24/7

Social Engineering and Phishing		
	At Risk	Insufficient social engineering and/or phishing training is being performed.
	Acceptable Risk	Training is being performed by the organization, but IT is separated from the process. The organization is aware that not including IT in training and its results may limit the ability of IT to fore
	Satisfactory	Social engineering and phishing training is performed at least quarterly and employees are identified who require further training. A process is in place to provide additional training as needed.

Vulnerability Management		
	At Risk	Client is in a high compliance industry, yet does not have a system to manage vulnerabilities.
	At Risk	A manual process in in place to deal with discovered vulnerabilities but no regular checks or automation is in place to look for vulnerabilities
	Acceptable Risk	Client accepts the risk of not checking for known vulnerabilities.
	Satisfactory	Automated vulnerability scanning is performed on a regular basis and reviewed by the IT team.

SOC Service for Endpoints		
	At Risk	Client does not have any SOC in place to monitor devices
	Needs Attention	A SOC services is active for servers and important workstations
	Acceptable Risk	Client accepts the risk of not having a SOC service in place.
	Satisfactory	All servers and workstations subscribe to an active SOC service to check for any cyberthreats 24/7 and report or block any incidents.

VPN / Remote Access		
	Not Applicable	Not Applicable
	Unknown	More information needed
	At Risk	VPN Access is required to work remotely. Unmanaged personal devices are being used for remote access.
	Needs Attention	VPN Access is required to work remotely. Company equipment is furnished for remote access.
	Satisfactory	Organization's infrastructure is built for mobility first / secure remote access by hosting all critical components in the cloud and making use of Zero Trust network security.

Vendor Risk Management		
	Unknown	Unknown - more information is required.
	At Risk	Vendor risk audits are not being performed.
	Needs Attention	Some vendors are asked to complete risk audits, but the audits are not regularly scheduled and/or required for all vendors.
	Acceptable Risk	No vendors have access to sensitive data, or the risk has been deemed minimal. Vendor risk audits are not being performed and the company accepts the risk that this may introduce.
	Satisfactory	All vendors are required to complete an audit annually to ensure reasonable security based on their level of access and sensitivity of their access to corporate data. Policies are in place to address
	Satisfactory	Vendors with access to sensitive data are required to complete an audit annually to ensure reasonable security. Policies are in place to address vendors who score poorly on an audit.

DNS Management		
	Unknown	Unknown - more information is required.
	At Risk	The organization has an outsourced resource for managing the company DNS or Managed the DNS themselves internally. That resource does not collaborate with the MSP for changes, which could result in downtime for the organization.
	Satisfactory	Techtron hosts and manages the DNS for the company. All DNS information is documented and setup correctly.

Documentation		
	Unknown	Unknown - more information is required.
	At Risk	Documentation is out of date and missing information
	Needs Attention	Documentation is in place but have not been reviewed in the last 6 months to confirm if they are still accurate and up to date.
	Satisfactory	Documentation is in place and they have been reviewed in the last 6 months, all documentation is up to date and available.

Patching		
	Unknown	Unknown - more information is required.
	At Risk	Patching is manual and software is out of date and missing updates
	Needs Attention	Automated Patching is setup for the operating system but not third party applications, Patch policy is documented but has not been reviewed in the last 6 months.
	Satisfactory	Automated patching is setup for the operating system and third party applications. Documentation is in place and they have been reviewed in the last 6 months, all documentation is up to date and available.

Backup Review		
	Unknown	Unknown - more information is required.
	At Risk	Backups are in place but they have not been reviewed in the last 6 months
	Satisfactory	Backups are in place and they have been reviewed in the last 6 months, all documentation is up to date and backups still align with business requirements

Website Management		
	Unknown	Unknown - more information is required.
	At Risk	No resource is currently maintaining the company website. Website patches and security fixes may need to be applied.
	At Risk	The organization has an outsourced resource for managing the company website. That resource does not collaborate with the MSP for changes, which could result in downtime for the organization.
	Satisfactory	The organization has an outsourced resource for managing the company website. That resource is documented and collaborates with the MSP for any DNS changes.

Logs		
	Unknown	Unknown - more information is required.
	At Risk	Logging for important application/services is not enabled
	At Risk	Logging for important applications/services is enabled but not backed up or stored for any specific period. Logs are not centrally managed or actively monitored.
	Acceptable Risk	Logging for important applications/services is enabled and backed for at least 6 months. Logs are not centrally managed or actively monitored.
	Satisfactory	Logging for important applications/services is enabled and backed for at least 6 months. Logs are centrally managed in a SIEM or other platform and actively monitored.

CONTINUITY

Backup & Disaster Recovery		
	At Risk	Backups require human intervention to run or change media.
	At Risk	Backups are not currently running.
	Needs Attention	Backup is being performed to Google Drive/Dropbox or other cloud service.
	Satisfactory	Direct to Cloud backups offer geo-redundancy and both bare metal and file level restore. Solution is separate from the corporate network and resistant to malware/encryption.
	Satisfactory	Onsite BDR appliance caches backups while they replicate to a geo-redundant cloud infrastructure. Solution is separate from the corporate network and resistant to malware/encryption.

Backup of Cloud Services		
	At Risk	Microsoft and Google both recommend a third party backup of their cloud services. No such backup has been implemented.
	Acceptable Risk	Client understands the risk and is willing to accept the loss of all data stored in third party cloud environments.
	Satisfactory	Cloud Backups have been deployed. Monitoring and test restores are part of the Client's service plan.

Cloud File Server		
	Not Applicable	Not Applicable.
	Unknown	More information needed
	At Risk	Business files are hosted on an internal file server, and files are being accessed by unmanaged computers, putting the entire organization's data at risk.
	Needs Attention	Business files are hosted on an internal file server, and accessibility from the outside requires either VPN or another form of remote access.
	Satisfactory	Business files are hosted on geo-redundant cloud infrastructure. Proper security is being applied while desktop and mobile accessibility are readily available for those who require it.

Email Archiving / Retention Policy		
	At Risk	Client has sensitive data and/or reporting requirements and Email Archiving/Retention is not in place.
	Acceptable Risk	Email Archiving/Retention is not in place and the Client accepts the risk of lost or incomplete data searches in the event of a request (i.e. FOYA)
	Satisfactory	There is no sensitive information in email. Email is deleted regularly to limit exposure in the event of a breach.
	Satisfactory	Email Archiving/Retention is in place to protect sensitive data from loss and/or simplify reporting in the event of a data request (i.e. FOYA).

Print Management		
	Unknown	More information needed
	At Risk	Wireless printers are in use. The lack of reliability in wireless printing significantly increases the risk of downtime.
	Needs Attention	A number of inefficient desktop printers throughout the company make printing difficult to support and more expensive than necessary.
	Satisfactory	Printing is handled centrally by high volume print/copy devices with desktop printers only deployed for sensitive print jobs.
	Satisfactory	Printix is setup to manage all printers centrally from the cloud.

Redundant Internet		
	Acceptable Risk	Client is aware that redundant solutions exist, but has identified minimal downtime as an acceptable risk that has minimal impact on the business.
	Satisfactory	Client has implemented alternative Wireless, LTE or similar unmanaged backup link, or backup link from the same ISP.
	Satisfactory	Client is running 2 ISP circuits in tandem, or has a managed backup link from independent ISP.

Internet Service		
	Needs Attention	ISP is unreliable and/or circuit speed is inadequate for the operations of the business.
	Satisfactory	ISP is reliable and circuit speed is appropriate for the operations of the business.

Infrastructure Wiring		
	At Risk	Infrastructure wiring is disorganized and lacks labeling, adding downtime in the event of a network issue.
	Satisfactory	Infrastructure wiring is reasonably clean and well labeled, speeding up the troubleshooting process in the event of a network issue.

TECHTRON / OTHER

User Onboard		
	At Risk	No formal documented process for new user onboarding
	Needs Attention	Formal documented process exists but majority of setup done manually, process has not been reviewed in the last 6 months.
	Acceptable Risk	Formal documented process, partially automated using Intune, has been reviewed in the last 6 months.
	Satisfactory	Formal documented process and fully automated deployment using Intune, and reviewed in the last 6 months

User offboard		
	At Risk	No formal documented process for user offboarding
	Needs Attention	Formal documented process exists but majority of removal done manually
	Acceptable Risk	Formal documented process exists, partially automated, and process reviewed in the last 6 months.
	Satisfactory	Formal documented process and fully automated deployment and reviewed in the last 6 months

User Security Groups		
	At Risk	User security groups don't exist or partially exist or have not been reviewed in the last 6 months
	Satisfactory	User groups are clearly documents, actively used and have been reviewed in the last 6 months.