Cyber Security Assessment Approval Letter

Client Name
Client Address

In order to comply with our Cyber Liability Errors & Omissions Insurance Policy, we must recommend that your organization have certain IT service offerings in place:

- Advanced Endpoint anti-virus, malware and ransomware endpoint protection should be on all desktops, laptops, tablets and servers. Advanced Endpoint detection systems should also include the ability to protect against file-less and script based attacked.
- Ensure that all security or product related patches are installed in a timely manner and are actively being monitored for any new patches.
- Networks should be protected by a business grade firewall with a comprehensive security subscription including intrusion prevention systems and that the subscription is actively licensed at all times and is downloading and applying new signatures as they are made available.
- If a server is in place, a BDR (Backup & Disaster Recovery device) MUST be in place, actively backing up at a minimum nightly both onsite and offsite in a secured compliant facility. Quarterly test restores should take place with a documented record of success of restores and nightly backups.
    - If no server is in place, at a minimum critical data must be backed up daily, is monitored for success/failures, and quarterly test restores should take place.
- A security and network assessment must be completed annually at a minimum.
- Business grade spam filtering services used in conjunction with either onsite email or 3rd party hosted email.
    - Email must be either internal exchange server OR Business Gmail OR Office 365.
    - Email must be included in backups either as critical data, BDR or through cloud backup specifically for Business Gmail or Office 365.
- Password Policy must be outlined, following current NIST recommendations and be implemented.
    - At no time can ANY passwords be stored on a document or spreadsheet. A Password Manager should be in place if the client wants to store passwords on a desktop, laptop or server.
- Ongoing security awareness training should include any user who has a device that accesses the network either internally or via an external connection. This training should include both online and in person training, should be mandatory, and reported on.
- Multi-factor authentication should be enabled on desktops and ALL cloud software services where available.
- Dark web monitoring should be enabled in the event that a credential or private information is compromised. Monitoring should include alerting to be able to take action to protect the business from stolen credentials that have been posted for sale.
- A log management software like SIEM should be established to allow big data engines to review all data and security logs from all covered devices to protect against advanced threats and to meet any compliance requirements.
- Secure Web Gateway should be active to protect users against phishing, malware and other Internet-borne threats that can access devices and be infected by malicious web traffic, websites and virus/malware.
- Mobile device security should be implemented on all devices that may access company information.
- Encryption should be enabled for data at rest and data in motion. Each desktop and laptop should be encrypted. Encryption should also be enabled for email and for any cloud file sharing services like OneDrive, Dropbox and/or Box.
- The main office location should have the following documentation stored securely. Policies should be disseminated to employees.
    - Breach Incident Response Plan
    - Disaster Recovery Plan

Cyber Security Assessment Approval Letter

- BYOD Policy
- Data Loss Prevention Policy
- Cloud Application Policy (Dropbox, CRM's, etc)
- Acceptable Use Policy
- Various other security policies

If you choose not to comply with the above recommendations, we will continue to service your account, however, you agree and understand that if there is a system failure or data loss caused by not following the defensive actions identified above, that we will not be held responsible for any data loss or network failures.

CLIENT COMPANY	[MSP NAME]
_____	_____
Print Name:	Print Name:
_____	_____
Signature:	Signature:
_____	_____
Date:	Date: