NEWFIELDS SUBCONTRACTOR CYBER SECURITY POLICY

SCOPE

This Subcontractor Cyber Security Policy applies to all companies and individuals with whom NewFields contracts to provide services to NewFields or its clients. The term "subcontractor" as used herein includes Independent Contractors and Independent Consultants. The term "NewFields Resource" includes E-Mail, Websites, or any other business application or electronic resource provided by NewFields.

POLICY OBJECTIVE

NewFields frequently utilizes subcontractors to provide services to NewFields' clients. As with all companies and individuals who rely on technology to collect, store, and manage information, NewFields' subcontractors are vulnerable to security breaches. Human errors, electronic attacks and system malfunctions could cause great financial and reputational damage not only to the subcontractor itself, but also to NewFields and its clients.

For this reason, NewFields has implemented this Subcontractor Cyber Security Policy which outlines the minimum measures that NewFields subcontractors must take to mitigate security risks.

POLICY

This section describes key safeguards that NewFields subcontractors are expected to use to protect and manage their information technology (IT) environments. Subcontractors must be able to demonstrate compliance with these standards to NewFields' IT Department upon request.

Use strong passwords. Select strong passwords and protect all user credentials, including passwords, security tokens, badges, smart cards, or any other means of identification and authentication you may be asked to use while providing services to NewFields and its clients. Passwords should be at least 8 characters long and contain a mix of upper- and lower-case letters and numbers. They should not contain easily guessable words (usernames, names of friends or family, hometowns) or be similar to other passwords you have used.

Treat passwords as highly confidential information. Protect your passwords at all times. This means that you may not disclose a password for your NewFields account to anyone, including co-workers, managers, clients, or family. Any password that is inadvertently disclosed must be reset immediately. Passwords may not be written down or stored unencrypted on any computer system. Passwords used for access to any NewFields Resource may not be reused, nor may similar passwords be used for any other purpose or account.

Use Two-Factor Authentication. Two-Factor Authentication is required to access some NewFields Resources. If access to these resources is needed, the subcontractor must install a compatible security application on a mobile device accessible only to that subcontractor and use this as a second authentication factor to access these NewFields Resources.

Protect Information Assets. Ensure that computers and devices that will be used to access NewFields Resources or perform services for NewFields or its clients utilize secure software. Computers and devices must be configured according to current best practices. All software including operating systems and anti-virus software installed on the system must be legally purchased, up-to-date, and fully patched. Firewalls, account passwords, and automatic lock screens must be enabled and properly configured. NewFields Resource may not be accessed from any computer owned or managed by someone other than the subcontractor or NewFields without written or emailed authorization from the project manager.

Keep Contact Information Up to Date. Make certain the project manager with whom the subcontractor is working has an up-to-date phone number for the subcontractor.

Report any Breaches. Subcontractors should immediately report any known or suspected breach involving NewFields or its clients' information immediately to the NewFields IT Department at IT@newfields.com. Subcontractors must assist as needed in investigations of any security incident, including allowing the NewFields IT Department to perform forensics on any computer or device used to access any NewFields Resource.

OWNER

The NewFields IT Department is the Owner of this Contractor Cyber Security Policy, and the Legal Department is a Stakeholder in this policy.

APPROVALS

Approved this 21st day of September, 2022.

_____

Patrick C. Gobb
Chief Executive Officer