# Protecting Confidential Information Checklist

**By Don Phin, Esq.**

When considering what confidential information you need to protect, and how you can protect it, it helps to take a checklist approach.

## Who to Protect

- ☐ Employees
- ☐ Customers
- ☐ Clients
- ☐ Vendors
- ☐ Contractors
- ☐ Partners
- ☐ Investors
- ☐ Other stakeholders

## Who/what causes problems

- ☐ AI.bots
- ☐ Competitors
- ☐ Employees- malicious or mistakes
- ☐ Hackers
- ☐ IT vulnerabilities
- ☐ Phishing schemes
- ☐ Storage/deletion/destruction

## What to protect

- ☐ Contact information
- ☐ Background check information- criminal, financial, etc.
- ☐ Documents- in paper and electronic
- ☐ Financial information
- ☐ Formulas
- ☐ Health information
- ☐ Immigration status
- ☐ Inventions
- ☐ Legal information

- Licenses
- Logins/Passwords
- Management information- business plans, M&As, layoffs, security, investigations, etc.
- Methods
- Patents
- Social security numbers
- Trade secrets

## How to protect

- Background checks of employees, contractors, and vendors
- Checklists
- Cybersecurity experts, audits and testing
- Email, social media and publication policies
- Employment agreements with Confidentiality provisions
- Equipment use- servers, laptops, mobile devices, BYOD, etc.
- Investigations- prompt, independent and thorough
- Internet/social media monitoring
- Labeling as “Confidential”
- Legal action, including injunctions
- Monitoring and tracking 24/7
- Non-competition agreements
- Non-disclosure agreements (NDA)
- Permissions required for disclosure
- Policies and procedures
- Proper backup, storage, and destruction
- Reporting programs for employees and third parties
- Restrict access to “need to know”
- Robust passwords, dual authentication, and encryption
- Shredding
- Training
- Wifi- no “public” Wifi use.