TRADE SECRET[1] IS:

- Information that can be described with particularity to separate it from matters of general knowledge in the trade.
- Information that derives independent economic value from not being generally known (includes, e.g., formulas, patterns, devices, blueprints, business strategies, and compilations of information).
- Reasonable efforts are undertaken to maintain the secrecy of the information; the sufficiency of reasonableness can vary depending on the nature of the trade secret.[2]
- Trade secrets can potentially be protected indefinitely.

REASONABLE EFFORTS[3] INCLUDE, FOR EXAMPLE,

- Establish a Company-wide trade secret policy; include explicit prohibition of unauthorized use of AI systems for handling, storing or transmitting trade secret or confidential information.
- Limiting access to trade secret information.
- Obtaining signed confidentiality agreements and non-compete agreements with all employees, and people having access to the trade secrets. The agreement should require the signer to protect the information *indefinitely* and should include explicit prohibition of unauthorized use of AI systems for handling, storing or transmitting trade secret or confidential information.
- Marking hard copies and soft copies of documents as confidential or trade secret.
- Keeping copies of trade secret material in a secure physical environment (e.g., by use of fences, locked doors, security guards, restricted areas, etc.); incorporate access controls for AI and datasets.
- Use security systems and access restrictions for personnel (e.g., ID badges).
- Use visitor badges, escorts and sign-in procedures for all visitors.
- Use notices (e.g., no trespassing signs, restricted area signs, document/binder/container "Confidentiality" labels).
- Use and enforcement rules and practices (e.g., materials locked-up when not in use, clear desk practice, distribution on a "need to know" basis, authorized user lists, copy numbers, distribution logs, etc.).
- Maintain computer and network security (e.g., by encrypting data, using passwords, requiring strong passwords, changing passwords periodically, secure transmission/reception, anti-virus/spyware measures, transmission, copying and printing restrictions, ongoing cyber-security training, AI use risk training, etc.).
- Require watermarking of proprietary documents, datasets and trained models; track unauthorized use of datasets and models.
- et all cloud, SaaS, or external AI service providers to ensure they do not inadvertently use client confidential data as AI training material. Include contract language specifying how data will be isolated and not incorporated into generalized model development.
- *Promptly* investigate suspected misappropriation.
- Communicate expectation of secrecy to employees who have access to trade secrets.
- Regularly educate employees regarding trade secret.
- Restrict use of smart phone tools (e.g., some companies restrict the use of Siri to record ideas because of the privacy policy and the way in which the information is handled).
- Conduct exit interviews with departing employees that includes a discussion of ongoing obligations concerning trade secret and prohibition against future use of company confidential materials with the help of AI.

ADDITIONAL STEPS TO CONSIDER INCLUDE,

- Limit access to computer databases and document files on the network.
- Provide CD burners and USB ports *only* for those who require them.
    - Consider software that tracks documents copied to USB.
- Require employees to use only company-owned computers.
- Maintain printed materials and specimens in central location with access control.
- Use barcodes or RFID technology to track samples and prototypes.
- Maintain a separate, wholly internal computer system, without Internet or other external network access for most sensitive information.

---

[1] *See,* Restatement of Torts, Section 757 and Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1831-39 (https://www.govinfo.gov/content/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap90.htm).
[2] *See,* Uniform Trade Secrets Act.
[3] Reasonable measures are based on a number of factors including the value of the information (e.g., the more valuable, the greater the security measures required) and the cost of security measures. The selection of additional measures can also vary depending on the law applied.