Checklist for Trade Secret Protection Mechanism for Small and Medium Enterprises (SMEs)

【2021.06.08】

Checklist Items	Check Indicators
1. Establish Clear Trade Secret Management Policy	□1.1 Designate personnel or team responsible for trade secret management □1.2 Allocate budget for trade secret management mechanisms □1.3 Draft different IP-related agreements based on employee roles: □1.3.1 Non-disclosure agreements (NDAs) □1.3.2 Intellectual property rights agreements □1.3.3 Non-compete agreements (in compliance with Article 9-1 of the Labor Standards Act) □1.4 Implement trade secret management rules： □1.4.1 File classification standards □1.4.2 File usage regulations □1.4.3 Management of physical (paper) documents □1.4.4 Management of electronic documents
2. New Employee Management	□2.1 Sign NDAs: □2.1.1 Confidentiality obligations for undisclosed company information known or held in the course of duties □2.2.2 No unauthorized use/disclosure of confidential materials without company consent □2.2.3 Obligation of confidentiality continues post-employment □2.2 Agreement on ownership of intellectual property created on duty □2.3 Sign non-compete agreements: □2.3.1 Non-compete duration does not exceed 2 years □2.3.2 Compensation no less than 50% of the employee's average monthly wage upon departure □2.3.3 Scope limited to businesses in direct competition □2.4 Due diligence for new hires： □2.4.1 Check for violations of previous non-compete agreements; understanding new employee's duties in their previous company □2.4.2 Declaration guaranteeing no prior trade secrets are brought into the company □2.5 Inform employees of job content and applicable trade secret rules □2.6 Assign proper access permissions for company information

Checklist Items	Check Indicators
	systems based on job roles
3. Management of Physical Documents	□3.1 Classify and label internal and external documents by confidentiality level □3.2 Supervisors may revise classifications post-review □3.3 Classified Preservation Tiered storage based on confidentiality; documents managed by designated personnel or self-stored securely. □3.4 Establish a registration system for confidential paper documents Designated personnel shall establish a registration and numbering system for confidential paper documents, to ensure centralized management or to provide a standardized protocol for implementation and compliance by employees of all departments. □3.5 Access control: □3.5.1 Applications are required for viewing/using classified documents □3.5.2 Verify employee identity and permissions before access □3.5.3 Keep a record of the return of all documents, including time and personnel □3.6 Establish a Standard Operating Procedure (SOP) for the destruction of confidential paper documents： Confidential paper documents that have exceeded their confidentiality period or meet the conditions for destruction shall be reviewed periodically and destroyed in accordance with the established SOP.
4. Electronic Document Management	□4.1 Implement comprehensive IT monitoring and protection: □4.1.1 Firewalls, antivirus software on cloud drives, internal systems, servers, and computers □4.1.2 Monitor software installations and external device connections (e.g., USBs) □4.2 Assign personnel to plan and execute trade secret management of digital files □4.3 Newly created electronic files must be classified and registered □4.4 Store based on confidentiality level (e.g., servers, cloud, personal computers) □4.5 Access and use management: □4.5.1 Password protection based on classification and confidentiality □4.5.2 Logging and reviewing access, copying, printing,

Checklist Items	Check Indicators
	transmission □4.5.3 Email content/attachment scanning for confidential keywords or competitor names □4.6 Establish a Standard Operating Procedure (SOP) for the deletion of confidential electronic files Confidential electronic files that have exceeded their confidentiality period or meet the conditions for destruction shall be reviewed periodically and deleted in accordance with the established SOP.
5. Auditing and Disciplinary Measures	□5.1 Establish audit and early warning SOPs: Random or scheduled audits with reports to senior trade secret management □5.1.1 Access/use logs of confidential files □5.1.2 Monitoring records of installations and device connections □5.1.3 Email alerts and detection logs □5.2 SOP for correcting trade secret management deficiencies If deficiencies in the management of trade secrets are found during random inspections, the issue shall be reported to senior management, and the improvement SOP shall be initiated. □5.3 SOP for violation handling: □5.3.1 Report violations for handling per internal SOP □5.3.2 Depending on severity, consider internal sanctions or legal action □5.3.3 Document violations and disciplinary actions, prepare case studies to raise awareness
6. Employee Management	□6.1 Reporting and declaration duties during job transfers: □6.1.1 Declare and return held confidential files □6.1.2 Submit a declaration confirming return and destruction of duplicates □6.2 Company management during transfers: □6.2.1 Evaluate need for new agreements based on new duties □6.2.2 Inform of new job scope and applicable trade secret rules □6.2.3 Adjust access permissions accordingly
7. Exit Procedures	□7.1 Establish mechanism to review departing employee's file access history □7.2 If irregularities in the access, viewing, or use of confidential documents by employees are discovered during inventory checks, an investigation SOP shall be initiated. □7.3 Conduct exit interviews and obtain written/online declarations

Checklist Items	Check Indicators
	of file deletion □7.4 Immediately revoke access credentials after departure □7.5 Monitor for non-compete violations, such as joining a competitor
8. Trade Secret Training	□8.1 Regular training and testing: □8.1.1 Hold training sessions on management rules □8.1.2 All employees must obtain full scores on testing □8.1.3 Maintain training records □8.2 Periodic measures to raise awareness: Employees shall be reminded of confidentiality obligations on appropriate occasions, and confidentiality-related informational materials shall be displayed.
9. Management of Outsourcing, Partners, and Contractors	□9.1 Sign NDAs with outsourced vendors, partners, and contractors: □9.1.1 Confidential documents shall not be used, delivered, or disclosed to any third party without the prior consent or authorization of a person authorized by the company. □9.1.2 Whether improvements may be made to the technology contained in confidential documents. □9.1.3 Agreement on the ownership of intellectual property rights arising from technical improvements. □9.2 Determine the scope of confidential materials which may be disclosed to third parties per company policy □9.3 Maintain a disclosure list and review mechanism □9.4 Review NDA compliance of external personnel □9.5 Upon contract termination, follow SOP for handling trade secrets: □9.5.1 Return confidential files □9.5.2 Provide records of file usage and outcomes □9.5.3 Notification and request for the destruction or deletion of copies of confidential documents.
10. External Interactions for Trade Secret Protection	□10.1 Attend trade secret seminars and promotion activities □10.2 Establish liaison contacts with agencies like the Ministry of Justice Investigation Bureau or National Police Agency Second Security Corps

Notes for Using This Checklist:

1. The company may formulate general or department-specific policies for confidentiality, intellectual property, and non-compete agreements depending on business needs.

2. Confidential files should be classified into at least three levels:
   Level 1: Core business secrets
   Level 2: Disclosure would cause serious harm
   Level 3: Disclosure would cause moderate harm

3. Agreement handling for new employees or job changes may be administered by HR or unit supervisors.

4. Audit, early-warning, SOP improvements, and violation handling may be conducted by HR, trade secret management units, IT, or relevant supervisors.