`	**G.1** **L.1** **L.2**					
Category	**Control ID**	**Control**	**Implementation / Description**			
Governance	G.1	Leadership & accountability	Establish someone is the organization as the ultimate authority and accountable for Trade Secret protection. This person may also be the cybersecurity delegated leader.			
Governance	G.2	Metrics and Reporting	Reporting on weekly, monthly or quarterly insider security metrics including data classification statistics, incident reporting, employee exit summaries, incentives, tabletop results, and progress indicators			`
Legal	L.1	Confidentiality Agreements	Develop tailored confidentiality agreements for different stakeholders (employees, contractors, vendors, partners). Include specific language identifying: clear definition of what constitutes confidential information, specific obligations for handling and protecting information, duration of confidentiality obligations (extending beyond employment/relationship), consequences of breach, return/destruction of confidential information upon termination. Regularly review agreements with legal counsel to ensure they remain enforceable in all relevant jurisdictions.			
Legal	L.2	Non-Compete Agreements	Draft enforceable non-compete agreements that: define reasonable geographic limitations, set appropriate time restrictions (typically 1-2 years), specifically identify prohibited competitive activities, offer consideration (something of value) in exchange for the restriction, include provisions addressing inevitable disclosure concerns. Customize agreements based on employee role and access to sensitive information. Verify compliance with local laws, as enforceability varies significantly by jurisdiction.			
Legal	L.3	Intellectual Property Assignment Agreements	Require all employees and contractors to sign agreements that: clearly establish company ownership of all intellectual property developed during employment, include "work for hire" provisions, cover inventions, ideas, processes, and improvements, address potential rights to pre-existing intellectual property, establish reporting requirements for new innovations.			
Legal	L.4	Evergreening background checks	The ability to re-screen employees with the same vigor as pre-employment is powerful tool to both encourage good behavior, but also alert on drastic life changes.			
Administrative	A.1	Information Classification System & Schema	Develop a multi-tiered classification system with: clear categories (e.g., Public, Internal, Confidential, Highly Confidential), specific handling procedures for each level, visual indicators (watermarks, headers, footers), guidelines for conversion between classifications, regular review processes for reclassification. Train all personnel on proper classification and create decision trees to help employees determine appropriate classifications.			
Administrative	A.2	Need-to-Know Access Policies and RBAC (Role Based Access Controls)	Establish formal processes that: document justification for access requests, require managerial approval for accessing sensitive information, implement time-limited access privileges, create formalized revocation procedures, maintain detailed access logs. Conduct quarterly access reviews to verify all access remains appropriate and necessary.			
Administrative	A.3	Document Control Procedures	Create comprehensive document management systems that: apply unique identifiers to all sensitive documents, track document version history, record distribution details, implement check-in/check-out procedures, set automatic expiration dates for sensitive materials, establish secure destruction protocols (including certificates of destruction). Deploy document management software that enforces these controls automatically. (SharePoint, Cavelo, Echo Mark)			
Administrative	A.4	Data Retention Policies	In addition to corporate data retention obligations, establish data retention policies that are optimal for employee activity reviews. Many documents are dynamic now such as Office 365 and Google Workspace documents. It might be necessary to capture document static copies whenever there is data transit.			
Technical	T.1	Data Classification Tools	Use data classification tools that classify data according the schema above. Privacy data is typically found using regex based expression given its uniform value. Proprietary data may be manually applied tagging, but also using contextual language models that identify more common documents such as legal, financial, and research documents.			
Technical	T.2	Asset Inventory Tool	Use an asset inventory tool to audit the classification of data across the enterprise and consistently confirm scanning and compliance. Account for shadow IT or unsanctioned data access or exit points			
Technical	T.3	Data Loss Prevention (DLP) Systems	Deploy enterprise DLP solutions that: monitor and filter outbound communications (email, web, FTP), detect sensitive data patterns using content inspection, block unauthorized transmissions of protected data, log attempted policy violations, integrate with email gateway and web proxy servers. Configure policies to identify trade secret information using keyword lists, regular expressions, and fingerprinting of sensitive documents. Many of these functions may overlap a managed browser			
Technical	T.4	Encryption	Implement a layered encryption strategy: deploy full-disk encryption for all endpoints (laptops, desktops, mobile devices), use file-level encryption for sensitive documents (AES-256 or higher), ensure encrypted communications channels (TLS 1.3, VPN), implement encrypted databases for sensitive information, establish strong key management procedures with appropriate key rotation. Utilize hardware security modules (HSMs) for cryptographic key storage and operations.			
Technical	T.5	Access Controls	Deploy multi-layered access controls: implement role-based access control (RBAC) frameworks, require multi-factor authentication for all sensitive systems, create segregated network zones for critical information, employ privileged access management (PAM) solutions, implement just-in-time access for highly sensitive systems, conduct regular entitlement reviews. Configure systems to automatically revoke access after periods of inactivity.			
Technical	T.6	Digital Rights Management	Deploy DRM solutions that: apply persistent protection to sensitive files, control viewing, editing, copying, and printing permissions, enable remote wiping of protected documents, maintain audit trails of document access and usage, expire document access automatically, prevent screen capture when viewing protected materials. Integrate DRM with authentication systems to provide seamless user experience while maintaining protection.			
Technical	T.7	Enterprise managed browser	The use of enterprise managed browser can be a critical barrier to preventing uploads to non-sanctioned domains, files sharing services, email and more. These advanced browser may also limit screen shots, copy/paste, and other functions. Enterprise browsers are critical to limited corporate access to outside domains.			

`	G.1 L.1 L.2					
Category	**Control ID**	**Control**	**Implementation / Description**			
Technical	T.8	Network Security Controls	Create defense-in-depth with: next-generation firewalls with application awareness, network segmentation with security zones, encrypted VPN access for remote workers, intrusion detection/prevention systems, data flow monitoring, regular vulnerability scanning, web application firewalls for customer-facing applications. Implement advanced threat protection solutions that can detect anomalous data movement patterns.			
Technical	T.9	UEBA (User Behavior Analytics)	UEBA and the use of other logging event and correlation tools (Sometimes included in SIEM) to create rules and alerts based on confidential file movements. Creating baselines and reviewing anomalous activity as it occurs			
Technical	T.10	Create visual deterrents	Establish visual warnings (watermarks on critical documents), access review summary emails, and pop-ups (toasts) that remind or warn users of the mishandling of sensitive data. Tools such as Harmonics Security and the Enterprise Managed browser may have this functionality. Also overlaps with DRM			
Physical	P.1	Secure Facilities	Establish layered physical security: deploy electronic access control systems with unique credentials, install CCTV monitoring with 90+ days of footage retention, create mantrap entries for highly sensitive areas, implement visitor management systems with escort requirements, install tamper-evident seals on sensitive equipment, conduct regular security sweeps for unauthorized devices, establish clear desk and clear screen policies. Document physical security measures to demonstrate reasonable protections in case of litigation.			
Physical	P.2	Secure Disposal	Develop comprehensive disposal procedures: deploy cross-cut or micro-cut shredders (at minimum DIN Level P-4), contract with certified destruction vendors for bulk materials, maintain chain of custody documentation, ensure witnessed destruction with certificates, implement secure wiping protocols (NIST 800-88 compliant) for electronic media, deploy degaussing equipment for magnetic media, establish physical destruction requirements for end-of-life hardware. Conduct regular audits of disposal practices to ensure compliance.			
Human Resource	H.1	Security Awareness Training	Develop a comprehensive training program that: includes initial onboarding training on trade secret protection, delivers role-specific training for employees with greater access, provides quarterly refresher courses, uses scenario-based learning and real-world examples, tests comprehension through assessments, tracks completion and comprehension metrics, addresses social engineering awareness. Supplement formal training with regular communication through newsletters, posters, and other awareness materials.			
Human Resource	H.2	Background Checks	Background checks should include inventor disclosure, github, social media, and signs of any criminal records.			
Human Resource	H.3	Employee Onboard Procedures	It's imperative that employees do not make the organization liable for receiving trade secrets from the new employees past employer. The employee must sign and agree not violate the past employees confidentiality obligations. Additionally the employee should list any IP they own that might be applicable before starting employment.			
Human Resource	H.4	Employee Incentives Program	Companies should be creative to support incentives for championing proprietary data protection and valuable IP. Incentives include rewards for process improvements, consistent awareness testing results, and creation of large amounts of classified proprietary data			
Human Resource	H.5	Exit Procedures	Create thorough offboarding processes that: include exit interviews focused on confidentiality obligations, require signed acknowledgment of ongoing obligations, recover all company property and credentials, maintain detailed checklists for HR and IT departments, perform comprehensive access termination (including cloud services and third-party accounts), conduct forensic imaging of devices when appropriate, send reminder letters about confidentiality obligations. Implement different levels of exit procedures based on risk assessment of the departing employee. Implement standard reviews of the last 6 months of activity. If there are any suspicious activities, it may be necessary and advantageous to conduct this research before an exit interview commences.			
Human Resource	H.6	Whistleblower and anonymous reporting	Establish a formalized program that: creates clear reporting channels for suspicious behavior, trains supervisors on warning signs, implements behavioral analytics to detect anomalies, conducts enhanced monitoring of high-risk positions, forms a cross-functional response team, develops investigation protocols, establishes remediation processes. Ensure the program balances security with employee privacy and workplace culture. Consider an anonymous reporting tool or whistleblower incentives.			
Incident Response	I.1	Breach Response Plan	Develop a specialized plan for trade secret incidents that: creates a dedicated response team with legal, IT, HR, and executive representation, establishes containment procedures to limit exposure, defines escalation paths based on severity, documents evidence collection requirements, includes communication templates for various scenarios, outlines coordination with law enforcement, details remediation requirements. Conduct regular tabletop exercises to test the plan's effectiveness. Make sure to quarantine and create discrete communication lines if the insider may be in this response group			
Incident Response	I.2	Forensic Readiness	Build forensic capabilities that: maintain appropriate tools for evidence collection, establish chain of custody procedures, deploy enhanced logging on critical systems, create secure evidence storage facilities, train key personnel on forensic principles, maintain relationships with external forensic experts, develop templates for preservation notices. Implement automated forensic collection capabilities for critical security events.			
Incident Response	I.3	Legal Remedies Preparation	Prepare for potential legal action: document all trade secret protection measures, maintain evidence of reasonable steps taken, prepare templates for cease and desist letters, establish relationships with specialized IP litigation firms, develop criteria for pursuing legal remedies, create procedures for emergency injunctive relief, establish valuation methodologies for trade secrets. Review and update preparation annually with legal counsel.			