Risk ID	Asset / Area	Threat	Vulnerability	Impact (1–5)	Likelihood (1–5)	Risk Score (I × L)	Current Controls	Recommended Controls	Risk Owner	Status
R-001	Employee Email	Phishing Attack	Users may click malicious links	4	4	16	Basic spam filter	Implement MFA + phishing training	IT Manager	Open
R-002	Laptops & Endpoints	Malware Infection / Ransomware	Outdated OS patches and unmonitored software installations	5	3	15	Antivirus installed	Deploy EDR, enforce automatic patching, restrict admin privileges	Security Analyst	In Progress
R-003	Customer Database	Unauthorized Access	Weak password hygiene and no MFA	5	4	20	Access logging enabled	Implement MFA, enforce password manager usage, quarterly access reviews	CTO	Open
R-004	Cloud Storage (e.g., Google Drive/Azure)	Data Leakage	Employees share files externally without controls	4	3	12	Basic sharing permissions	Enable DLP (Data Loss Prevention), restrict external sharing, audit permissions monthly	Compliance Lead	Open
R-005	Wi-Fi Network	Network Eavesdropping	Weak Wi-Fi encryption (WPA/WPA2 only) & shared passwords	3	4	12	Router firewall enabled	Upgrade to WPA3, rotate passwords quarterly, create guest network	Network Administrator	Open
R-006	Remote Work Environment	Unauthorized Access to Company Data	Employees using unsecured home networks	4	3	12	VPN available	Enforce mandatory VPN, require encrypted devices, provide secure WFH guidelines	IT Manager	Open
R-007	Internal File Server	Data Loss	No tested backup/recovery strategy	5	2	10	Manual weekly backups	Implement automated daily backups, test recovery quarterly, store offsite backup	Systems Administrator	In Progress