Cyber Insurance

Underwriting Appetite Guide

PROGRADE SPECIALTY

TARGET MARKET	ELIGIBLE CLASSES		INELIGIBLE CLASSES	
• Small-to-Medium Enterprises (SMEs)	11	Agriculture & Forestry	• 22	Utilities
• Gross revenue up to $100,000,000	23	Construction	• 4811/12	Air Transportation
• Businesses handling PII, PHI, or payment data	31–33	Manufacturing*	• 5182	Data Processing/Hosting
• Email-reliant or digitally active operations	42	Wholesale Trade	• 5222	Non-depository Credit
• No cyber losses in prior 3 years (referral option available)	44–45	Retail Trade	• 522320	Financial Transactions
• Adequate cyber risk management in place	52*	Finance & Insurance	• 523120-523160	Securities/Commodity
	54	Professional & Technical Services	• 561440/50	Collections/Credit Bureaus
	62*	Healthcare & Social Assistance	• 611310	Colleges & Universities
	72*	Accommodation & Food Services	• 721120	Casino Hotels
	* Subcode restrictions apply — see guidelines		• 813940	Political Organizations

Coverage Ability

LIMITS	
Minimum Coverage Limit	$50,000
Maximum Coverage Limit without Referral**	$3,000,000
Maximum Coverage Limit with Referral	$5,000,000
Minimum Deductible**	$0
Maximum Deductible	$50,000

**Certain class codes may be subject to higher deductible requirements or max coverage limits

Key Underwriting Controls

MFA

Multi-factor authentication (MFA) is the leading cause of ransomware and data breach claims. Accounts protected by MFA are over 99% less likely to be compromised.

Verification Procedures

Robust wire transfer verification procedures are a key essential an organization's controls against social engineering and fraud.

Security Patching

Timely security patching reflects an organization's commitment to reducing its exploitable attack surface by addressing known vulnerabilities before they can be weaponized.

Data Backups

Regular, tested data backups are a foundational element for an organization, ensuring critical systems and information can be restored after a disruptive event.

Coverage Snapshot

BASE POLICY Included with every policy	OPTIONAL ENDORSEMENTS Available add-ons	OPTIONAL ENDORSEMENTS Available add-ons
✓ Security & Privacy Liability	◆ Funds Transfer Fraud & Social Engineering*	◆ Service Fraud and Cryptojacking
✓ Breach Response Expenses	◆ Invoice Manipulation*	◆ Technology E&O
✓ Regulatory Defense & Penalties	◆ Hardware Replacement & Bricking	◆ Third-Party Platform Suspension
✓ Cyber Extortion & Ransom	◆ Post-Breach Remediation	◆ Telecommunications Fraud
✓ PCI Fines & Penalties	◆ Contingent BI – Security Failure	◆ Extended Reporting Period (up to 3 years)
✓ Business Income & Extra Expense	◆ Contingent BI – System Failure (IT)	◆ Waiver of Subrogation (referral required)
✓ Funds Transfer Liability	* MFA deployed + dual-channel verification procedures required for Funds Transfer Fraud/Social Engineering and Invoice Manipulation eligibility.	
✓ Reputational Harm		