



TechDefender®

The Risk:

Technology companies are susceptible to the potential of greater risk with the fast pace of new and specialty product and service offerings. Furthermore, the majority of states in the U.S., the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification for privacy breaches involving non-public personal information. The current regulatory environment on privacy is imposing more stringent reporting provisions, creating additional liability for companies and their directors and officers.

The Coverage:

IRONSHORE TECHDEFENDER POLICY:

IronPro's TechDefender is a comprehensive policy designed to provide coverage for a broad range of perils in the technology sector with a menu suite of coverage as follows:

Network Security Liability

- Pays the company for loss arising out of the failure of network security, including theft, corruption or deletion of electronic data, unauthorized access and use, denial of service attacks and transmission of malicious code.

Privacy Liability Coverage

- Pays the company for loss arising out of the unintentional and unauthorized disclosure or loss of non-public personal information or confidential corporate information in any format.
- Provides protection against a violation of any privacy regulations including the HITECH Act, HIPAA, GLBA and Massachusetts 201 CMR 17 or the failure to comply with the company's own privacy policies.

Privacy Breach Expenses

- Pays the company for legal services to create a breach response plan, computer forensics, public relation expenses, notification and call center services, ID and credit monitoring for affecting individuals and monetary assessments, including contractual fines and penalties levied by a card association.

Regulatory Fines and Proceeding Coverage

- Reimburses the company for costs incurred in responding to a regulatory proceeding and in making payments to a consumer redress fund.
- Reimburses the company for regulatory civil money penalties and fines where insurable by law.

Internet Media Liability

- Pays the company for loss arising from the infringement of copyright, title or trademark and invasion of privacy, libel or slander on the company's website.

Digital Asset Expenses

- Pays the company for expenses incurred to replace or restore electronic data, software, audio files and images stored on the company's computer system due to the corruption or deletion as the direct result of a network security incident.

Business Interruption Income Loss

- Pays the company for business income interruption loss and extra expense incurred by an Insured as the direct result of a network security incident.

Network and Data Extortion Threat and Reward Payments

- Pays the company for any extortion expense, and reward paid by the company as the direct result of a network extortion threat.

Technology Errors & Omissions Liability

- Pays the company for loss arising out of the unintentional error, omission, neglect or breach of duty in connection the rendering or failure to render technology services.

Miscellaneous Professional Liability

- Pays the company for loss arising out of the unintentional error, omission, neglect or breach of duty in connection the rendering or failure to render non-technology professional services.

Targeted Tech Classes

- Technology Consultants and Service Providers
- Packaged and Custom Software Developers
- Internet and Application Software Providers
- Website Developers
- Telecommunications Companies

Targeted MPL Classes

- Consultants
- Third Party Administrators
- Business Brokers
- Trustees
- Real estate agents, brokers and property managers
- Temporary staffing
- Freight forwarders

Limits Available

- Up to \$10 million

Minimum Premium and Retention

- Minimum premium - \$5,000
- Minimum retention - \$5,000

The Ironshore Advantage

- The Other Insurance Provision - Ironshore's policy serves as primary insurance
- Privacy Breach Expenses, Digital Asset, Business Interruption and Network/Data Extortion are on a Pay on Behalf Basis and not Reimbursement Basis
- Excess Side A D&O coverage available for non-indemnifiable claims arising from a Privacy and Network Security Wrongful Act
- Breach of contract exclusion - The exclusion shall not apply (a) only with respect to the coverage provided pursuant to Network Security Liability and Privacy Liability, to any obligation of the Insured to maintain the confidentiality or security of Non-Public Personal Information or of Confidential Corporate Information, (b) only with respect to Internet Media Liability, for misappropriation of ideas under implied contract, (c) PCI Fines and Penalties, or (d) to the extent such liability which would have attached in the absence of such contract or agreement
- Extortion includes both a Network and Data Extortion event
- Coverage extends to the Insured's Service Provider's computer systems for a Network Security Incident (first party coverage) and a Network Security Wrongful Act and Privacy Wrongful Act (third party coverage)
- Affirmative coverage for Cyber Terrorism
- No failure to maintain information security exclusion
- Affirmative coverage for Regulatory Proceedings and Regulatory Fines and Penalties where insurable by law
- Affirmative coverage for monetary assessments, including contractual fines and penalties, levied by a card association where insurable by law
- Insured vs. Insured carve back for the Insured as a customer of the company or as an Insured for a privacy incident
- Defense and settlement of claims modified to include 50% claim expenses
- Consumer Redress Coverage
- Partial severability of the application limited to officers, directors, attorney, risk manager, principal or partner of the company
- Worldwide coverage where legally permissible

Pre and Post Loss Control Services

- The C3 Voluntary Program and National Cybersecurity Assessment & Technical Services (NCATS) powered by U.S. Department of Homeland Security (DHS) (For all Ironshore cyber policyholders that operate in the critical infrastructure sector - Chemical, Telecommunications, Manufacturing, Dams, Defense Industrial Base, Financial Services, Food and Agriculture, Government Facilities, Healthcare, Information Technology, Transportation and Water and Waste Water Systems)
 - Ironshore will also offer every critical infrastructure policyholder, at no cost, a cybersecurity assessment and technical services review conducted by U.S. Homeland Security. The C3 Voluntary Program and National Cybersecurity Assessment & Technical Services (NCATS), provides an objective third party prospective on the current cybersecurity posture of the policyholder's network. Ironshore's On-Call Chief Security Officer can then assist the policyholder to address and remediate identified vulnerabilities.
- Ironshore eRisk Hub, powered by NetDiligence
Ironshore policyholders have access to the eRisk Hub, a private and secure web-based portal that provides policyholders access to the following:
 - Security awareness training tools;
 - Sample network security and privacy policy templates, including those for computer security and network extortion;
 - News, whitepapers and content from leading practitioners in risk management, network security, computer forensics, crisis management and legal counsel
 - Information and technical resources that can assist you in the prevention of network and privacy losses and support you in the timely reporting and recovery if an incident occurs.
 - Pre-negotiated Ironshore rates from highly credentialed security experts for threat

Claims – Our Policies are Our Promises

- Ironshore TechDefender distinguishes itself in the industry by operating its professional liability claims and underwriting services under the same leadership, and functioning as one team to meet our customers' needs
- One point of contact for information on your claims
- Open dialogue with insureds

Product Contact

Kurt Suhs

Vice president, National Practice Leader of Privacy, Security and Technology E&O
(404) 845-7549
kurtis.suhs@ironshore.com

Regional IronPro Contacts

New York Region

Daniel Frusciano
Vice President
daniel.frusciano@ironshore.com
(646) 826-6771

Northeast Region

Eugene McDonough
Regional Executive
eugene.mcdonough@ironshore.com
(617) 502-5360

Mid-Atlantic Region

Jill Kebler
Regional Manager
jill.kebler@ironshore.com
(267) 443-2888

Southeast Region

Scott Fitzmaurice
Regional Executive
scott.fitzmaurice@ironshore.com
(404) 845-7547

Mid-West Region

Kevin Burt
Assistant Vice President
kevin.burt@ironshore.com
(312) 496-7507

Southcentral Region

Kristi Janicek
Vice President
kristi.janicek@ironshore.com
(469) 248-4336

Southwest Region

Adam Witten
Regional Executive
adam.witten@ironshore.com
(213) 416-2320

Northwest Region

Jeremy Frumkin
Branch Manager
jeremy.frumkin@ironshore.com
(415) 291-2708



About Ironshore

Ironshore provides broker-sourced specialty property and casualty coverages for risks located throughout the world. Select specialty coverages are underwritten at Lloyd's through Ironshore's Pembroke Syndicate 4000. The Ironshore group of insurance companies is rated A u (Excellent) by A.M. Best with a Financial Size Category of Class XIV. Syndicate 4000 operates within Lloyd's where the market rating is A (Excellent) by A.M. Best, AA- (Very Strong) from Fitch and A+ (Strong) from Standard & Poor's. For more information, please visit www.ironshore.com.

The information contained herein is for general informational purposes only and does not constitute an offer to sell or a solicitation of an offer to buy any product or service. Any description set forth herein does not include all policy terms, conditions and exclusions. Bound insurance policies, rather than summaries thereof, govern. Not all insurance coverages or products are available in all states and policy terms may vary based on individual state requirements. Some policies may be placed with a surplus lines insurer. Surplus lines insurers generally do not participate in state guaranty funds and coverage may only be obtained through duly licensed surplus lines brokers.