# ACE Privacy Protection Policy

***Today a person can easily store the equivalent of an entire pickup truck of printed social security numbers, credit card numbers or health insurance records on a small USB flash drive. Any breach of sensitive customer or employee information can become a public relations nightmare, destroying not only your restaurant's reputation but your balance sheet in the process.***

The ACE Privacy Protection Policy is designed to protect a restaurateur's most sensitive information about their business, customers and employees. The policy provides coverage arising from:

- Lost computer equipment
- Network security breaches
- Human error; and
- Mistakes made by outside service providers

**The ACE Privacy Protection coverage also includes a Data Breach Response Fund.**

**Three Reasons Why Every Restaurant Needs ACE Privacy Protection®**

1. Increasingly stringent laws and regulations have elevated a restaurant's duty of care for how it safeguards personal information. Failure to comply with legal and regulatory obligations places your restaurant's reputation at enormous risk. Given the potential loss in customer confidence, historically many companies kept security breaches quiet. Today state identity theft notification laws make it illegal to sweep privacy breach events under the rug - keeping quiet is no longer an option.

2. Advances in technology make safeguarding client trust and restaurant's reputations from privacy breaches far more difficult. Technology has made it easier to store, transport, steal or simply lose sensitive information.

3. Any restaurant that entrusts outside contractors to handle its sensitive data, including payroll management firms, accounting/bookkeeping firms, employee benefit firms and consultants, ultimately bears the burden of any privacy breach stemming from an outsourced operation. Your restaurant may require your service provider to carry privacy coverage, but it does not eliminate your responsibility to protect your customer and employee data. **If your customers are affected by a data breach, your company is obligated to respond, regardless of who made the error.**

## Coverage & Limits Overview

**Limits - Up to $5 million**

**Privacy Liability**

Covers loss arising out of an organization's failure to protect sensitive personal or corporate information in any format including paper.

Provides coverage for regulatory proceedings brought by a government agency alleging the violation of any state, federal, or foreign identity theft or privacy protection legislation.

**Data Breach Fund**

Covers expenses to retain a computer forensics firm to determine the scope of a breach, to comply with privacy regulations, to notify and provide credit monitoring services to affected individuals, and to obtain legal, public relations or crisis management services to restore the company's reputation.

For a Quote Email or Call

Tel: 866-821-9572

info@firstchoiceii.com

# ACE Privacy Protection Policy

**Internet Media Liability**

Covers infringement of copyright or trade mark, invasion of privacy, libel, slander, plagiarism, or negligence arising out of the content on the organization's internet website.

**Additional Coverages include:**

Privacy coverage includes customer and employee information, personal information in any format, and network, as well as non-network security breaches

Data breach expenses include voluntary notification and expenses to comply with the consumer notification provisions of the applicable jurisdiction that most favors coverage

No retention, coinsurance, prior written approval, or post-discovery time restrictions for Data Breach Fund (voluntary notification subject to prior written approval)

Privacy Regulations coverage includes the latest regulations including the Identity Theft Red Flags Rule, HITECH Act and Massachusetts 201 CMR 17

Definition of damages includes regulatory fines where permitted by law, a consumer redress fund, and punitive and exemplary damages (most favorable jurisdiction language)

**Support Services & Benefits**

Access to Data Breach Coach, an independent law firm providing data breach consultation services

Access to Data Breach Team, an independent panel of specialists in the legal, computer forensic, notification, call center, public relations, fraud consultation, credit monitoring, and identity restoration service areas

Sound claims experience and handling

Free access to eRisk Hub®, a web-based loss prevention resource containing information and technical resources to help policyholders manage their privacy and network risks

**Key Features of the eRisk Hub® www.eriskhub.com**

- **Incident Roadmap** – suggested steps to take following a network or data breach incident and free consultation with a Breach Coach®
- **News Center** – articles on major breach events, security and privacy blogs, IT security updates, risk management events and helpful industry links
- **Learning Center** – a library of best-practices articles, white papers and webinars from leading technical and legal practitioners
- **Risk Manager Tools** – self-help for managing cyber risk, including a cyber-risk assessment survey, breach notification guides, what-if modeling tools to estimate the cost of a breach, and research tools to monitor the type, frequency and severity of incidents occurring in your business sector
- **eRisk Resources** – a directory to help you find qualified third-party resources with expertise in pre- and post-breach disciplines

For a Quote Email or Call

Tel: 866-821-9572

info@firstchoiceii.com