SAMPLE RISK MANAGEMENT PLAN: CYBER SECURITY

Step 1: Identify Your Business’ Cyber Risks

Breaches to computer networks and unauthorized access to sensitive data are the key elements of cyber risk. These risks include personal injury, intellectual property infringement, and financial injury from allegations of negligence, as well as fines, costs and obligations associated with Consumer Protection and Data Privacy Regulations. When the security of the network is compromised, information which should be private may be made public. This is the essence of a data breach event.

Step 2: Assess Your Risk

To assess your risk, it can be helpful to start by asking yourself “What are you trying to protect?” about your products, services, customers, vendors, communication and information networks.

- Third-Party Risk: Ensure you know what your third parties are doing to protect data to keep your company secure. This is even more critical in situations where you’re sharing data with these third parties, or allowing them access to your internal network.
- Regulatory Requirements: Ensure you’re up to date on any new Cyber Security regulations and how these requirements may impact how you conduct business, and what controls you need to have in place to protect sensitive data.

Step 3: Identify Mitigating Methods

A Data and Security Plan can help protect your company not only from regulatory scrutiny, but also help prevent breaches and mitigate the fallout if a breach occurs. Once your risk analysis is complete, identify one or more methods for mitigating each risk. Revisit this risk assessment regularly to re-rank the risks as your company’s organizational controls and systems evolve and improve.

Resource:
Sample Cyber Risk and Controls

Resources:
Quick eRisk Assessment – eRiskHub®
What if Modeling – eRiskHub®

Resources:
FCC Small Business Cyber Planning Guide – eRiskHub®
Step 4: Create Your Company Policies

Company policies and procedures establish the rules of conduct within an organization, outlining the responsibilities of both employees and employers. Company policies and procedures are in place to protect the rights of workers as well as the business interests of employers.

Step 5: Communicate Your Program and Expectations

Communicate your Data and Privacy Security Plan and company expectations to every employee. Through effective communication, your employees will learn what behavior or performance changes are necessary. Review the program with your employees and make a reference copy accessible to them when they are at work.

Step 6: Train Your Employees

The best security technology in the world can’t help you unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. Training employees is a critical element of security. They need to understand the value of protecting customer and company information and their role in keeping it safe.

Step 7: Monitor Results and Take Necessary Action

Regularly measure the effectiveness of your Data and Privacy Security Plan by revisiting and reevaluating all of the factors that went into developing them. Regular audits should evaluate your information-security practices and whether your company is effectively following those practices, including conducting tests to ensure that employees are properly and consistently implementing the solutions.

The information provided in this plan is intended to be general in nature. It may include recommendations, suggestions or ideas that are not applicable to the unique conditions and operations of your business. Obtain the advice of an independent legal or business advisor in developing forms and procedures tailored to your specific business. This publication may also provide information on services offered by companies wholly independent from Federated Mutual Insurance Company, Federated Service Insurance Company*, and Federated Reserve Insurance Company* (*Not licensed in all states). Federated provides its clients with access to these services with the understanding that neither Federated nor its employees provide legal or employment advice. Some services may be subject to regulations or restrictions in your state. The recommendations provided may help reduce the risk of loss, but should not be construed as eliminating any or all risk of loss nor is it an exhaustive list of all risk exposures. Qualified counsel should be sought regarding questions specific to your circumstances.