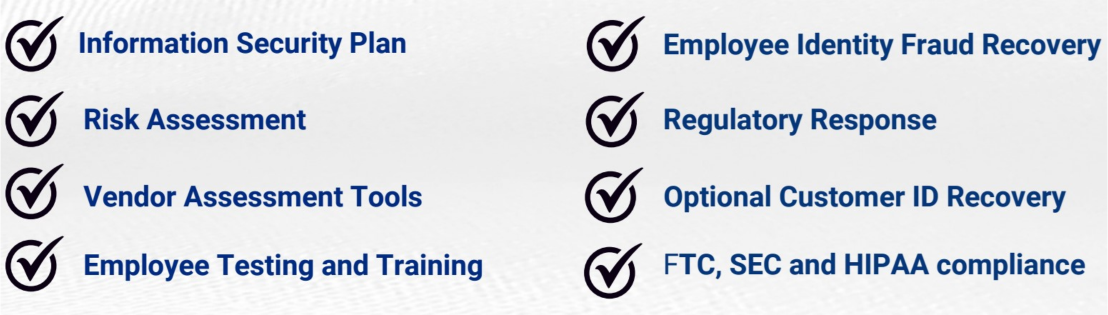
Business Cyber Security Program

The rising threat of cyber attacks on small and medium-sized business has prompted companies to seek action and protect their business from fraud. We provide the necessary written protocols, action plans, and 24/7 monitoring to keep you compliant with cyber security insurance policies.



- ✓ Information Security Plan
- ✓ Risk Assessment
- ✓ Vendor Assessment Tools
- ✓ Employee Testing and Training
- ✓ Employee Identity Fraud Recovery
- ✓ Regulatory Response
- ✓ Optional Customer ID Recovery
- ✓ FTC, SEC and HIPAA compliance

An Information Security Plan ISP (also referred to as a written information security plan WISP) is a critical component to cybersecurity that includes methodologies to keep networks safe and secure no matter the level of outside attacks. Small-to-medium-sized businesses (SMBs) are no stranger to these cyber-attacks.

An information security plan is a set of rules and policies that guide how digital information should be managed at all times. Even if you believe your small business doesn't require such strict control over data, it's important to recognize how rapidly technology evolves to meet your company's requirements. We are constantly changing the way we use technology to interact with our surroundings, and this highlights the need for an information security policy.

The advancement of technology is reshaping how we deal with data. Implementing an Information Security Policy requires small and medium-sized businesses to carefully consider and tackle all aspects of data management. It also enables them to establish strategies for safeguarding their data, despite the numerous techniques hackers may use to breach network defenses.
A solid ISP is a set of rules that clearly defines how users should safely use company technology.
It also serves as a plan for handling emergency situations if something goes wrong.

The ISP should include cybersecurity guidelines for employees to follow. It should have procedures for protecting employee, vendor, and customer information to prevent hackers from stealing important data. This is crucial because hackers can cause financial damage and harm relationships with employees, customers, and vendors. By implementing specific protocols in your InfoSec policy, you can reduce the risk of your small business becoming one of the many that fail within six months of a cyber-attack.

☎ 920-419-6570
www.encompass-security.net
Neenah, WI 54956

ENCOMPASS SECURITY
A CYBER AND IDENTITY SOLUTIONS COMPANY