

Security Program Checklist

Information Security Basics

Information security programs enable companies to meet their legal and business objectives by managing the multitude of risks associated with use of information and technology. Every company should have a formal, documented information security program.

With the ever-growing scrutiny of corporate security, it is an excellent time to evaluate your company's security program and verify that it meets legal requirements and manages risk sufficiently. Effective security programs contain five key components:

- (1) **RISK ASSESSMENTS** to identify threats and vulnerabilities;
- (2) **STRATEGY DEVELOPMENT** to prioritize and mitigate the risks
- (3) **CONTROLS IMPLEMENTATION** to assign responsibilities and deploy specific processes to manage risks;
- (4) **TESTING** to confirm that risks are appropriately mitigated by the controls; and
- (5) **MONITORING** to adjust of the controls given emerging threats.

The resulting safeguards should be reasonable and appropriate. This means that the safeguards should reflect both the sensitivity of the information being protected as well as the size and complexity of the organization.

Evaluating Your Security Program

The following checklist presents basic questions that can help you evaluate your company's information security program.

- Do you have a designated individual who is responsible for the security program? Are your current controls and security processes documented? Is the program approved by your Board of Directors or senior management?
- Do you classify your information assets based on the sensitivity of the data elements?
- Do you have an inventory of your information assets, software and hardware devices? Do you have an inventory of information and technology maintained by service providers?
- Have you identified and prioritized internal and external threats to your information and systems? Did you include threats from technical and organizational vulnerabilities (such as ineffective training), accidental loss, intentional damage, and environmental problems (such as natural disasters or power failures)?
- Do you have defined physical security zones? Do you control access within your facilities based on these zones? Do you control environmental contaminants or electronic penetration?



The Art of Information Management

Information Security Programs: Questions to Ask...

- ❑ Are all users required to execute appropriate acceptable-use policies and/or non-disclosure agreements?
 - ❑ Are users given access only to information and systems as needed to perform their required functions? Are the access rights adjusted periodically to reflect personnel or system changes? Are users appropriately authenticated, based on the level of risk?
 - ❑ Have you grouped your systems, applications, information and users into security domains and set access requirements within and between each security domain?
 - ❑ Do you secure your computer networks using multiple layers of access controls?
 - ❑ Are your networks appropriately protected using a combination of protocols, filtering routers, firewalls, gateways, proxy servers, and/or physical isolation?
 - ❑ Do you restrict access to operating systems applications and system utilities? Do you monitor access and use? Are operating systems and applications kept current with security patches? Do you use anti-virus products and other filtering technologies to protect against malicious code?
 - ❑ Are applications secured with appropriate time-of-day restrictions and other controls? Do you monitor application usage with software that analyzes user activity patterns?
 - ❑ Do you limit remote access to situations where it is needed for a particular business reason? Do you monitor remote access and secure/isolate remote access devices? Do you use strong authentication and encryption to secure communications?
 - ❑ Do you use encryption to protect sensitive information during transit? During storage? Do you employ effective key management practices?
 - ❑ Are security requirements established prior to development/acquisition of systems and applications? Do you have an effective change control process?
 - ❑ Do you perform background checks on new employees and onsite contractors?
 - ❑ Do you provide security training to all employees and onsite contractors?
 - ❑ Do you have appropriate media handling controls to protect paper and electronic media? Do you securely dispose of all paper and electronic media containing company or personal information?
 - ❑ Do you conduct due diligence on service providers? Do you require contracts that include confidentiality, defined security controls and reporting? Do you audit your service providers? Do you have a process for coordinating incident response?
 - ❑ Do you have processes to respond to an information system intrusion, including the containment and restoration of systems? Do you have a formal incident response plan? Has this plan been tested?
 - ❑ Do you have an established disaster recover and business continuity plan?
 - ❑ Do you have sufficient insurance coverage given the identified security risks?
- If you have any questions about the legal requirements for information security, please call PEGGY EISENHAUER at 404-914-1163.

This checklist is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia law firm specializing in privacy, security and information management. If you would like to join our mailing list to receive our quarterly newsletter, please email tanya@privacystudio.com.

The information contained in this alert has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.
4355 Cobb Parkway—Suite J-280, Atlanta GA 30339
Phone: 404-914-1163
www.privacystudio.com