



Information Security – #3 Procedures

Overview

As more and more manual processes are automated, securing electronically stored sensitive information becomes a priority. Your security umbrella should include your technology systems, people, and processes (procedures).

Step #3: Procedures

Protect your electronically transmitted and stored information with these simple steps:

- *Physical security.* Network defenses can be critical, but when it comes to protecting sensitive information, don't forget physical security. Ensure access to network servers is restricted to authorized personnel.
- *Encryption.* Use encryption to protect sensitive data such as credit card numbers, social security numbers, driver's license numbers, etc.
- *Viruses.* Viruses, spyware, and other malware can compromise your systems and your data. Ensure your anti-virus and anti-spyware software is updated on a regular basis.
- *Passwords.* Most organizations use an ID and password to grant access to your data. Ensure your passwords are long and complex and changed on a regular basis.
- *Education.* Remind your employees that electronic security is everyone's responsibility. Hackers certainly pose a threat, but sometimes the biggest risk to an organization's security is an employee who hasn't learned the basics about protecting sensitive information. Create a culture of security by implementing a regular schedule of employee training.
- *Access.* Provide access to sensitive information only on a "need to know" basis. Have a procedure in place for making sure that workers who leave your employ or move to another part of the business no longer have access to off-limits information.
- *Detection.* Intrusion detection systems can alert you to breaches in your network security. IT should monitor incoming and outgoing traffic for higher-than-average use at unusual times of the day.
- *Patching.* Check expert resources like www.sans.org and your software vendors' websites for alerts about the latest vulnerabilities and vendor-approved patches.
- *Providers.* Ensure security practices of your contractors and service providers. Before outsourcing business functions, ensure agreements define security requirements. Contractors and service providers should notify you immediately if they experience a security incident, even if it may not have led to an actual compromise of your data.
- *Documentation.* Organization policies give direction and guidance but generally lack sufficient details to describe how things should be done. By documenting your detailed procedures, your organization ensures consistent and sustainable protection of your information assets.



Publication and Author Information

Jim Kelton is Managing Principal of Altius IT (www.AltiusIT.com), an IT security audit, security consulting, and risk management company based in Costa Mesa, California. Mr. Kelton has over 30 years of experience in the Information Technology industry and is recognized as a security expert. He is certified by the Information Systems Audit and Control Association (ISACA) as:

Certified Information Systems Auditor (CISA)

Certified in Risk and Information Systems Controls (CRISC)

Certified in the Governance of Enterprise IT (CGEIT)

He sits on the Board of Directors of the following associations and organizations:

- Association of Professional Consultants (APC)
- International Association of Professional Security Consultants (IAPSC)
- Technology Professionals Association (TPA)