



## Information Security – #4 Disposal

### Overview

At some point, almost every piece of information reaches the end of its useful life. By securely disposing of information, an organization can protect personal information and prevent a security breach.

### #4: Information Security – Disposal

Ensure your organization take the following precautions when disposing of information:

- *Delete.* Deleting a computer file doesn't mean that the information has been permanently removed from your system. The data may continue to exist on the computer's hard drive and could be easily retrieved. Ensure your employees request assistance from your IT department when permanently deleting data.
- *Disposal.* When getting rid of old computers, laptops, hard drives, portable storage devices, cell phones, etc., use wipe utility programs or physically destroy the media. Wipe utility programs are inexpensive and overwrite the contents so that the files are no longer recoverable.
- *Remote.* Whether working from home or on the road, ensure telecommuters and business travelers maintain your company's high security standards. Remind employees and contractors to be as careful when disposing of sensitive documents off-site as they are when creating them.
- *Compliance.* If you use consumer credit reports in your business, you may be subject to the FTC's Disposal Rule. The Rule requires companies to adopt reasonable and appropriate disposal practices to prevent the unauthorized access to, or use of, information in credit reports.
- *Papers.* Effectively dispose of paper records containing sensitive data. Having shredders available throughout the workplace helps ensure employees understand the need to properly dispose of sensitive information

### Publication and Author Information

Jim Kelton is Managing Principal of Altius IT ([www.AltiusIT.com](http://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)