SEAM
SECURE ENTERPRISE ASSET MANAGEMENT

DATA SECURITY IN THE WORKPLACE:
DECOMMISSIONING COMPUTER EQUIPMENT

With data breaches on the rise, securely and effectively decommissioning your company's IT assets at the end of their lifecycle is essential. A well implemented plan can prevent unauthorized access and create an audit trail for compliance with data security and environmental regulations. In most companies, there are a few common areas that should be addressed:

Equipment Storage — When devices are removed from your network, where are they being stored? Many times decommissioned equipment is kept in the same area as new devices or set in an unlocked closet, out of sight and out of mind. This can leave assets vulnerable to loss, inappropriate access, or theft. Best practices include placing devices in a quarantined room with monitored, restricted access.

Inventory — Do you know what devices you have and where they should be? By creating and managing an accurate database of all incoming and outgoing equipment, you can make certain no data-containing device is misplaced or overlooked. This will support future inventory reconciliation and prevent discrepancies when using third party vendors as well as provide evidence of your due diligence for audit purposes.

Record Keeping — Can you easily provide documentation that your data was securely destroyed? Whenever liability is transferred from one party to another in the recovery or disposition of an asset, it should be recorded. A well documented chain of custody provides peace of mind and assurance for environmental, security and legal compliance with regulations such as HIPAA, FACTA, GLBA, SARBOX, EO 13693, FISMA, PCI DSS and FERPA.

Data Destruction — How is your sensitive data being destroyed? Before disposing of hardware, you must ensure that all the data on it has been permanently destroyed and is nonrecoverable. If you are performing data destruction internally, make sure your staff is well trained on the methods outlined by the National Institute of Standards and Technology (NIST) in their Guidelines for Media Sanitation (SP 800-88 R1). Data sanitization should be properly monitored from start to finish and checked for successful erasure to establish quality control. A dedicated, secure space should also be used to perform the wiping process for security prior to and during the procedure. A certified IT Asset Disposition vendor can offer convenience, efficiency, security and validation when it comes to data destruction, whether performed onsite at your location or offsite at their facility.

Disposal — What happens to your equipment when it leaves your possession? Whether its resold, reused, or recycled, make sure you know what the final disposition of your equipment will be. When choosing a partner, look for e-Stewards and R2 certifications. This guarantees they have the proper qualifications and processes in place to securely and safely resell equipment to maximize your value while properly disposing of any units or parts that no longer have use. Request a tour of their facility to verify that they follow the standards they say they do. Many service providers offer onsite hard drive shredding to provide complete data destruction before devices even leave your facility.

Questions? Contact SEAM to learn about our certified, secure Data Destruction and IT Asset Disposition services.

SEAMSERVICES.COM
605-274-SEAM (7326) | SIOUX FALLS, SD