



How to evaluate a data destruction company

If you decide you need to contract with a third-party service to help destroy your data, here are a few questions to consider as you evaluate their services:

How well does the service understand the various government guidelines or security classifications regarding data destruction?

Does the company perform data destruction as a primary business, or as an adjunct to what it is doing already?

Do you need a certificate of destruction outlining how and when the destruction took place? If so, can the service provide that for you?

What process does the company use to ensure a strong chain of custody for your data once it leaves your possession? Does the service ever outsource portions of this work to other subcontractors or third parties?

Can you observe the destruction of your data while it's in the service's care?

How does the service recycle any of its final byproducts (if it recycles at all)?

If it's important for you to know who is handling your data, what background checks and training does the service do, and what confidentiality agreements does it have with its employees?

How are the service provider's facility and operations secured from unauthorized access?

Has the service done work for the government before? What references from other clients can it provide?

Is the service open to spontaneous visits or audits of its operations and facilities? What independent audits or spot checks does it already perform during the course of business?

What other logs or reports can the service provide about the destruction process?

If it's important to you, can the service track asset numbers, serial numbers or other media information, and does it time-stamp its associated destruction activities?