

A PARTICLE OF SECURITY

A perspective on data destruction service specifications

Destruction is a process—not a “particle”.

When most people think of records destruction, even those responsible for data security, they think of shredding machines and the shredded paper they produce. As a result, when considering the security of records destruction, they focus solely on the size of the shredded material.

This is an understandable, but dangerous, misconception. It ignores the reality that the destruction of data, whether on paper or electronic media, is a process requiring security at several different points.

The process of data destruction includes the collection, staging, transfer of custody, acceptance of fiduciary responsibility, transport, processing (destruction), and the disposal of destroyed materials. It also includes other activities such as employee screening and monitoring, access control, employee training, policies and procedures, and audit trails.

By concentrating on (and relying on) solely on the size of the shredded material, the need for security throughout the process is completely overlooked.

No particle size, even the smallest, can overcome the security problems that could result if the destruction process is not secure throughout. On the other hand, there is less need to go to extremely small (and expensive) particle sizes if the process, including how the shredded material is finally discarded, is completely closed and secure.

Regulations favor a “process” perspective.

Every major data protection regulation in the US includes a requirement that organizations have written data protection policies and procedures. In other words, they require that the data protection “process” is identified. However, none of those regulations make any reference to a specific particle or shred size. In other words, the regulations focus on the process and not the shredded particles.

For example, in the Final Disposal Rule of the Fair and Accurate Credit Transaction Act (FACTA), the nation’s first data destruction requirement, the US Federal Trade Commission (FTC) addresses baseline vendor qualifications for destruction service providers. The FTC did not, however, prescribe any particle size whatsoever, simply stating that destruction must “reasonably” render the information “practically unreconstructable.”

In another example, the US Department of Veterans Affairs defaults specifically to the industry standard of NAID AAA Certification as a vendor qualification for secure destruction services. While NAID AAA Certification does contain reasonable particle

size requirements, its real strength and emphasis lies in verifying nearly twenty different aspects of the service provider's destruction process.

A false sense of security

When hiring a firm to destroy records, every customer has the right to determine the particle size that best protects them. The problem results when particle size becomes the most important consideration—or worse, the only consideration.

It is understandable why this happens. As described above, most people who hire destruction services think of destruction only as shredding and, as a result, focus solely on the size of the shred. From this perspective, destruction is seen as an event that happens when the materials pass through a machine.

In reality, there are many service providers that have machines that can make a certain particle size, but are grossly lacking the other process elements mentioned above that provide real security.

When destruction is viewed as a process, all elements of destruction are considered and included in the security specifications.

In truth, the particle size specification is only relevant after all other security aspects of the destruction process are addressed. If the “other” service provider qualifications are NOT addressed, then no particle size will be good enough to overcome the potential security risks posed by weaknesses in the overall process.

Outsourcing as more secure process

When materials are shredded in an office they often leave the office in the trash, which in turn goes into the dumpster outside the building. There is a saying among those who raid dumpsters looking for personal and competitive information: “When you're looking for information, take the shredded stuff.” By shredding materials and placing them in the trash, an organization essentially tells the bad guys what to take.

Commercial destruction services, when properly operated, do not allow such access. Certainly, the materials are still destroyed to a reasonable extent, consistent with the intent of the regulations. From there they are subsequently recycled into new paper products through documented controlled channels. Of course, comingling the materials in mass quantities further increases security, and results in making reconstruction attempts virtually impossible (or not practicable, as the regulations put it). The end result is that the paper is reduced to cellulose fiber in a chemical bath at the paper making mill.

With this knowledge of the inherent security of the process used by properly run secure destruction services, the commercially conventional sizes currently available in the marketplace are reasonable and actually deliver a higher level of security than even the smallest particle from an office shredding machine.

Still, even with a more secure method of destruction, commercial services must address the comprehensive laundry list of security elements that are included where there is a process-orientation.