



---

## Fact Sheet

XTINCT is a tool for wiping data to ensure the original data is unrecoverable. Make your data as extinct as the dinosaurs. Various options exist to meet your level of protection.

### Why is it necessary?

Years ago, disk media inside a glass house, accessed by only a few people and password protected was considered reasonably safe. Even disaster recovery testing at offsite locations didn't raise much concern for the safety of corporate data. After testing, many would scratch the table of contents and walk away feeling corporate data was reasonably safe. Today, however, is a different story.

Terrorism, identity theft, off-shoring, outsourcing, litigation, the internet and the global economy have all highlighted the need for increased data protection. Governments have passed legislation such as Sarbanes-Oxley (SOX), HIPAA and Gramm-Leach-Bliley (GLBA) to hold corporations responsible for securing private information under their care. Beyond government standards, industry regulations, such as the Payment Card Industry Data Security Standard, have further defined the rules, and corporations desiring to do business with them must be in compliance. Other techniques to render the data unreadable like encryption may appear to be adequate but still not good enough for your liability insurance. Failure to comply with these standards for data protection can result in large business losses and severe penalties; it is no longer simply a matter of due diligence to protect data under your control – it is a necessity.

XTINCT meets all the requirements of US Department of Defense 5220.22-M (Clearing and Sanitization Matrix for Clearing Magnetic Disk) by overwriting all addressable locations with a single character. XTINCT also meets the sanitization requirement by overwriting all addressable locations with a character, its complement, then a random character and verifying. For tapes, the DoD only considers degaussing or pulverizing the tape to be a valid erase. XTINCT meets the requirements of most users by overwriting the tape and use of the hi-speed data security erase patterns.

### When is it necessary?

- When moving disks to another location.

- When disks come off lease and are being returned to the vendor.
- When disks are being moved to a warehouse.
- When leaving a backup/recovery site after disaster recovery testing.
- Before re-using disks for a different group within the company.
- Before scrapping disks.
- Erase data sets with sensitive information every day.

### **Are there any free products available to Clear or purge Data?**

The short answer is NO.

With utilities such as IEHPROGM, individual data sets or the entire VTOC can be scratched. However, that simply removes the pointer to each data set while leaving all the data on the disk. ICKDSF can perform a MINIMAL INIT to create a label and a new VTOC, but that leaves all the data on the disk as well. A MEDIAL INIT will re-write the Home Address and record zero but may still not render data unreadable. Consequently, it will not satisfy the standard for clearing or purging. These techniques also take a VERY long time.

### **XTINCT: DSF/E Device Support Facilities/Extended**

For all of the aforementioned reasons, Dino-Software Corporation has developed XTINCT. It can help even the most demanding corporations meet their security needs.

- XTINCT has 2 primary commands: DISKINIT and TAPEINIT.
- DISKINIT to erase full 3390 disk volumes.
- Data set erases for both disk and tape are now implemented in JCL ONLY.
- DSINITV to erase VSAM data sets.
- TAPEINIT to erase tape data sets.
- XTINCT is reentrant and fully supports sub-tasking. Up to 64 volumes can be processed asynchronously. Other tools, like ICKDSF run serially.
- XTINCT makes extensive use of channel programs. Many functions operate at peak efficiency by only using enough CPU time to generate the channel programs, with the rest of the operation being carried out by the channel subsystem. This makes XTINCT a miser when it comes to valuable CPU time.
- Control statements allow for PACING the number of concurrent operations against a string using the TASKMAX parameter. The user can run one task or many at the same time.

- XTINCT provides four levels of erasing data to satisfy the needs of even the most demanding customers.
- XTINCT provides a pattern write that reverses each bit (one's compliment) to eliminate the possibility of reading residual data.
- To make sure that the data pattern is written to disk, XTINCT forces the storage controller to de-stage all modified tracks at the end of each pass and prior to starting the next one. This precludes a second pattern replacing the first pattern in cache and never being written to the disk, while still making efficient use of NVS and cache.

**The following discussion describes the techniques available.**

DISKINIT XTINCT(LEVEL0) - will create a 1 track VTOC on a disk at Cylinder 0 Track 1.

DISKINIT XTINCT(LEVEL1) - will perform a hardware erase of each disk track.

DISKINIT XTINCT(LEVEL2) - is the default technique. This will erase a track using full track patterns. The default pattern is binary zeroes.

DISKINIT XTINCT(LEVEL3) - is the most secure because it writes a pattern of data, then the one's complement of the data, followed by a full track of X'FF'. Consequently, each pattern will cause each track to be written and formatted multiple times. Writing a pattern of X'BC' as an example, causes the pattern BC to be written first, followed by the one's complement of BC or 43, followed by a pattern of X'FF.'

DISKINIT SIMULATE - is used to not only check all control statements before committing to an erase function, but will identify and display all volumes that would be included. Simply replace the SIMULATE control statement with the EXECUTE control statement to perform the actual erase after you have verified the disks that will be erased.