Information Retention and Deletion Landing Page

Information Retention and Deletion Landing Page

On this page:

Overview

One of the easiest ways to avoid exposing information you don't need anymore, including administrative and research data, is to destroy it.

For moderate and high risk information, observe applicable data retention policies upon project completion. Securely delete the information by means that make it impossible to reconstruct the records. Also destroy devices that contained high risk data in ways that make it impossible to recover.

If you must retain a copy of moderate or high information, ensure that it remains secure.

- For more information on how to classify and secure your data, see Information Protection @ MIT.

Electronic Information

- Removing Sensitive Data
- IS&T's Media Sanitizing
- Secure Delete for PC
- How do I remove downloaded files securely?

Physical Data

- How do I shred sensitive data files?
- VPF Property Office - includes disposing of MIT property securely

See Also

- Grad students uncover mountains of private data on discarded hard drives

Have Questions or Still Need Help?

- Contact the IS&T Computing Help Desk