



Private Data: let's keep it that way!

The University is legally obligated to secure private data; just a few simple practices will help to keep our systems “street legal.” If you have any questions or need help, please contact CLA-OIT.

EVERYONE

- **Know the backup plan for your data**, so that it's protected in case of a hard drive crash or stolen laptop. Ask your technician if you're not sure about it!
- **Create a strong password.** Use letters, numbers and punctuation. If you're an administrator, your password must be at least 15 characters long to guard against attacks from viruses, spyware and password-guessing attempts.
- **Don't accept passwords from others.** Not your assistant, not your brother, not the president of your fan club, not even your dog. University Policy forbids it, because it's an inappropriate sharing of legal power; use your own power instead.
- Be prepared to **re-enter your password** after 15 minutes away from your computer; think of it as a sentry at your front door.
- **Keep your laptop secure**; lock it up when it's not with you, and be sure your data is encrypted—protect both the owners of the data and the University!
- **Don't e-mail private data**, or even attach it to an e-mail. If a message or attachment is opened on an unsecured computer, most e-mail software (including Thunderbird and, to a lesser degree, GopherMail) will create and store a copy of it: *at that moment, privacy breaks down.*
Instead, use University-provided Active Directory home or shared drives or NetFiles.
- **Work from home safely:** view, store and edit data only on University-owned computers. Your home computer doesn't have University security standards in place. CDs and USB flash drives are easy to lose. Create a security plan with your technician; some customization is available, and we're here to help! **Questions? Check out connect.cla.umn.edu!**

