Secure IT. IT’s up to you.

**Longer and stronger**
Shorter passwords are easier for hackers to break. NIST, the National Institute for Standards and Technology, recommends that passwords be anywhere from **8 to 64 characters long.**

**Mix and match**
Do you like mixing languages or making up your own words? If so, then you have an easy way to improve your password. **If it only makes sense to you, it’s less likely to appear in the cracked lists of passwords hackers use.**

**Ditch the digits?**
While your own organization’s rules may be different, new federal guidance has advised that forcing users to include lots of symbols and numbers doesn’t necessarily increase password security. **Focus on length and memorability** instead.

**Thinking in sentences**
How do you remember a password that’s 64 characters long? Think in sentences, not words. A phrase or a sentence is easier to recall than a nonsensical combination of letters and numbers, and provides that all-important length to make it harder to crack.

```
jst4sm4l1t0wngrl!lvnnngn4l0nelyw0rl0d!!
t00kth3mdnghttr4ng0ng4nwh3r3!!!_
```