Security

- Choose strong passwords - at least 9 characters long, a mixture of alphanumeric mixed case and symbol characters. The password should be completely different from the password you use on any other system.
- **Never use the same password across different systems !**
- **NEVER copy your SSH private key to systems that you do not control!** The private key should remain in your .ssh directory on the system you generated it and should be readable only by you. If you need to login from two systems such as a laptop and a workstation you can copy the key pair to both systems ONLY if you really trust both. When copying always check that the copied files are only readable by yourself.
- SSH key passphrases must be as secure as other passwords.
- **Never setup passphraseless** ssh keys to allow unauthenticated login access between systems !!!

WARNING: Incorrectly configuring SSH keys can leave your accounts vulnerable to attack and, more importantly, can provide attackers with a trivial means to access remote systems with potential legal consequences for yourself. It is your responsability to keep your SSH authentication and your user account secure.

Revision #8
Created 21 February 2019 16:48:46 by João Pina
Updated 12 January 2021 13:45:56 by Jorge Gomes