



1.006 Password Policy

Policy Purpose and Scope

The purpose of this policy is to outline the requirements, best practices, and procedures for managing Company passwords.

Roles and Responsibilities

The IT Department will be responsible for managing and implementing this Policy.

Operational Procedures

- **Recording Passwords**

All Company passwords must be recorded in Passpack, with limited exceptions (noted below). You are free to store your personal passwords in Passpack.

- **Transfer of Control of Certain Passwords**

You must transfer control (in Passpack) of all Company passwords that are the master or single point of entry to a Company account. Personal company accounts do not need to be shared in Passpack.

- **Do Not Reuse Passwords**

With limited exception, passwords for external systems (e.g. a website, external server or application) should be unique for each system and must not be reused. Using the same password for two different websites, for instance, is generally not allowed. If desired, passwords can be randomly generated using Passpack or a similar tool.

- **Updating Passwords Given to Company**

You must periodically verify any passwords that have changed, where the Company has control of the password. If the password has changed, please update it in Passpack. If you do not have the ability to do so, please inform the IT Department of the change.

- **Use Secure Storage and Transmission**

Under no circumstances are passwords to be shared using insecure means (e.g. e-mail, text message). Sharing via Passpack is the recommended solution for avoiding this.

Likewise, with limited exceptions, passwords are not to be written down and stored on paper. Exceptions include cases where passwords may need to be shared but are too sensitive to be used with Passpack. In these cases, passwords may be written or printed out so long as it is for a temporary use and the physical articles are properly destroyed once they are no longer required.

Under no circumstances are passwords to be kept in plain sight or where they can be easily obtained. This includes using sticky notes with passwords anywhere near workstations.

- **What Not to Enter in Passpack**

Passwords that protect extremely sensitive information should not be entered into Passpack. These include: master password to Google Apps (email), development or production server accounts, online banking passwords.

For Uncertain Cases, it is best to err on the side of caution and avoid using Passpack or to contact the IT Department (IT Crowd) so that they can evaluate the situation and make a recommendation.

- **Password Complexity**

Any password relating to the Company, be it a personal account or one that is to be shared must consist of alphanumeric characters with mixed case, at least one symbol, and have a minimum of 12 characters where possible. Passwords should not use easy to guess words, in any form (such as hacker or “1337” speak).

Some sites (most notably Passpack) use additional security measures including a pass-phrase. This would be separate to the above guidelines. In these cases, the guidelines set for by the site/service that is requiring a pass-phrase should be followed and should be in addition to a standard password.

- **Use of Public/Private Key Cryptography**

Where applicable, the use of public/private key cryptography instead of, or in compliment of, a password is both accepted and highly encouraged. The most notable example is using SSH keys instead of passwords for file-transfer and shell services on Linux-based machines. As long as reasonable security measures have been taken on devices that store the private key, passwords on the private key need not be used. Where possible, key managers should be used to manage password-protected private keys and is the recommend solution.

- **Use Sub-Accounts Whenever Possible**

In cases where multiple users will need access to a system, use individual accounts wherever possible. In other words, avoid giving out the master password to all users. Please consult the IT department to explore exceptions to this rule.

Revision Date: 2013-12-18