Objective

Payroll data is by nature very sensitive data and should not be exposed.
To this end, over and above all the security mechanisms put in place by **Payroll Mauritius**, all users of the System should ensure that their access is protected to the best of their ability (Recommendation No. DAT-NT-001/ANSSI/SDE/NP) so as not to create a vulnerability on the information system as a whole (and not only on their workstation).

The major risk to an intrusion most often lies in exposing the password or choosing a password that is too "simplistic" and needs to be made more robust (i.e. difficult to retrieve using automated tools and difficult for a third party to guess).

How to do this ?

Here are some recommendations :

- Use a unique password for each service. In particular, the use of the same password between your professional and personal email should be imperatively prohibited;
- Choose a password that is not related to you (a password consisting of a company name, date of birth, etc.) ;
- Never ask a third party to generate a password for you;
- Change the default passwords systematically and as soon as possible when the systems contain them;
- Renew your passwords with a reasonable frequency. Every 90 days is a good compromise for systems with sensitive data;
- Do not store passwords in a file on a computer workstation that is particularly exposed to risk (e.g. online on the Internet), let alone on easily accessible paper;
- Do not send your own passwords to your personal mailbox;
- Configure software, including your web browser, so that it does not "remember" your chosen passwords.

If you want a simple rule: The longer the password, the harder it is to crack. Choose passwords of at least 12 characters of different types (upper case, lower case, numbers, special characters).

Two methods for example to choose your passwords :

- The phonetic method: "Woohoo! The Packers won the Super Bowl! " will become *WOO!TPwontSB*
- The method of the first letters: "one yours is better than two you'll get" will give *1ysbtTyl'g*. On this subject, you will find on the french CNIL website http://www.cnil.fr/fr/generer-un-mot-de-passe-solide a free generator of "strong" passwords to inspire you.

IMPORTANT: In addition to the above, we also recommend the implementation of **the two-factor authentication** that **Payroll Mauritius** has in place.
Explanations on this implementation can be found in the document FAQEN117 - How to set up two-factor authentication to secure the super-admin password in Payroll Mauritius

_____