Using your PEXA login credentials and Digital Certificates

This checklist will help you protect your identity and the integrity of the network when using your PEXA login credentials and Digital Certificate to electronically sign in PEXA.

Need help? Ask your question on the e-Conveyancing Community at **community.pexa.com.au**.

Security checklist

Following the steps below will help you remain compliant with your professional obligations, and those set out in the Model Participation Rules which govern your use of PEXA. Non-compliance with these obligations may result in the Registrar of Titles in your jurisdiction instructing PEXA to suspend or terminate your access to the network.

□ Ensure you are the only person who knows your PEXA password

Upon registering with PEXA, unique credentials are provided to an organisation's nominated Subscriber Manager. If required, the Subscriber Manager can then create individual user profiles with unique login details for additional employees within their organisation. Employees should never share User IDs or password login details for PEXA.

□ Select different passwords for your email, desktop access and PEXA

Using the same password across multiple log in channels is risky - if one was compromised, then all could be compromised. Strong passwords have a minimum of 10 characters and use a mix of uppercase and lowercase letters, numbers and special characters like **!**, **&**, and ***. #** (Using a special character in your password will increase the difficulty of breaking it significantly).

□ Ensure each employee required to sign documents and authorise funds in PEXA has their own Digital Certificate

Every Subscriber is required to obtain and maintain at least one Digital Certificate. The number required will depend on how many people will be signing on behalf of the organisation. Digital Certificates are assigned to an individual – when used to digitally sign, both the signer and organisation are clearly identifiable. If your Digital Certificate is shared within your firm and misused in a PEXA transaction, you will be identifiable as the signer.

□ Ensure no one else has access to your Digital Certificate and PIN

Your Digital Certificate is your unique, binding electronic signature. If a digitally signed document in a PEXA transaction is called into question, and it is suggested that the owner of the Digital Certificate was not the person who applied it, your professional reputation and ability to claim on your professional indemnity insurance could be impacted. Whenever your digital signature is applied in PEXA, it is taken to be signed by you and is binding, similar to a 'wet' signature. It is important to check documents and the Financial Settlement Schedule prior to signing. Should someone other than the owner of a Digital Certificate use it to sign in PEXA, it may be considered the equivalent of forging a 'wet' signature. We suggest you do not leave it inserted in your computer, and instead consider locking it away and ensure secure storage provisions are available for all employees with a Digital Certificate.

□ Plan ahead to ensure your business has sufficient coverage to sign in PEXA

Consider how many people in your organisation may be required to digitally sign in PEXA and arrange Digital Certificates for each unique user. When managing operations, you may need to account for staff leave, those who are frequently out of the office, and ensuring there are enough people present who are trained and authorised to sign in PEXA.

□ Know what to do if you or a staff member move on to a new job

A Digital Certificate identifies both you and the firm, therefore cannot be taken by the owner to a new job. A new Digital Certificate will need to be ordered by their new employer. In these circumstances, Digital Certificates must be cancelled by calling the PEXA Support Centre on **1300 084 515**.

□ Multi-factor authentication (MFA)

MFA is utilised to confirm that the person logging in to PEXA is the person who owns the profile being used, and not someone else. MFA requires the user to provide two or more types of evidence to verify their identity when logging in to an account or completing a transaction. As MFA requires the owner of the profile to pair their mobile phone, logging in requires the user to have their device on them, enabling them to receive their authentication code by SMS or the PingID app directly. It's important to note that each Subscriber will be required to authenticate with their own device every 12 hours.