YOUR ONLINE PROPERTY EXCHANGE

PEXA Subscriber Security Policy

Version 2.4
15 September 2018

PEXA
Property Exchange Australia

Contents

1. Definitions

Unless the context requires otherwise, capitalised terms used in this Security Policy have the meaning given to them in the Participation Agreement between PEXA and your organisation.

2. Purpose & objectives of this Security Policy

This Subscriber Security Policy (**Policy**) sets out the security requirements that Subscribers must ensure that they and their Users adhere to when using the PEXA System in order to maintain the overall security of the PEXA System.

3. Scope of this Policy

This Policy applies to all Subscribers of the PEXA System, including the devices, credentials and Digital Certificates used when accessing and Digitally Signing documents in the PEXA System.

4. Key Subscriber Obligations

4.1 General

4.1.1 Compliance

The Subscriber must comply with its security obligations as contained in this Policy and the Participation Rules. For a copy of the Participation Rules in each Active Jurisdiction refer to:

- VIC
- NSW
- QLD
- WA
- SA

4.1.2 Systems Security

The Subscriber must take all prudent and reasonable steps to:

(a) ensure that all of its systems and facilities which it uses to access the PEXA System are protected by the Logical Security measures set out in section 4.2 of this Policy and the Physical Security measures set out in section 4.3 of this Policy;

(b) prevent unauthorised access, damage or interference to PEXA's electronic systems, an Electronic Workspace or the ELN by any person employed or engaged by the Subscriber; or through any systems or access points owned or controlled by the Subscriber and through which the Subscriber can connect to PEXA, an Electronic Workspace or the ELN; and

(c) ensure the integrity and confidentiality of information retrieved or received from PEXA, and information supplied to PEXA.

The Subscriber must, immediately upon becoming aware, notify PEXA of any breach or suspected breach of this Policy and, to the extent permissible, of the security measures taken to address or mitigate the breach and any potential future breaches of a similar type, method or process.

4.1.3 Supported devices

The PEXA System does not currently support the use of tablet and smartphone access. It is possible to access the PEXA System using smartphones and tablets, however Subscribers will not be able to access full PEXA functionality (e.g. no digital signing functionality). PEXA does not recommend accessing the PEXA System from smart phones and tablets and does not guarantee system functionality when accessing the PEXA System from these devices.

4.1.4 Loss Mitigation

Subscribers must, immediately upon becoming aware of any theft, unauthorised disclosure or improper use of credentials and Digital Certificates used for accessing the PEXA System, ensure that they implement appropriate measures to mitigate any loss that may arise as a result of such theft, unauthorised disclosure or improper use.

4.2 Requirements to access the PEXA System (Logical Security measures)

4.2.1 PEXA Approved Digital Certificates

Subscribers must provide Users who require signing permissions in the PEXA System with Digital Certificates that comply with the Operating Requirements. Digital Certificates must not be shared between Users. Users must only sign documents in the PEXA System using their own Digital Certificate.

4.2.2 Approved technology for storage of Digital Certificates

Digital Certificates are available in either a secured software file (Software Certificate) or on a secure USB token (Hardware Token).

Subscribers must ensure that Digital Certificates are used and stored using Hardware Tokens.

A Subscriber can seek from PEXA an approval to use Software Certificates. PEXA will grant or withhold approval to use Software Certificates by having regard to the Subscriber's security framework, which may include PEXA evaluating (in its sole discretion) whether the Subscriber:

- can comply with ISO/IEC 27001;
- is adequately secured using multiple controls; and
- meets or exceeds accepted industry standards for information security.

Approval to use Software Certificates will be granted or withheld in PEXA's absolute discretion.

4.2.3 Virus and Firewall Protection

Viruses (and Malware) are forms of malicious software introduced into an electronic device with the malicious intent of causing harm to the IT systems to compromise the confidentiality, integrity or availability of any related IT system or data held on these systems.

The Subscriber must take prudent and reasonable steps to provide virus and firewall protection against any unauthorised intrusions or uncontrolled access to the systems and access points of the Subscriber through which the Subscriber may access PEXA, an Electronic Workspace or the ELN (regardless of whether such access occurs by means of the Internet or some other electronic form of communication).

The Subscriber must ensure that its virus and firewall protection must have, at a minimum, the following attributes:

- the ability to identify and remove viruses;

- the ability to identify and remove other types of harmful computer software, generally referred to as malware (or malicious software);
- the ability to automatically receive anti-Virus updates from the relevant anti-Virus software vendors;
- the ability to automatically scan for viruses and malware in documents on servers and workstations; and
- the ability to provide firewall protection either as a standalone device, or on the router and on the built-in software on the device.

Subscribers must ensure that the commercially available anti-Virus and firewall software in use meets the criteria set out above. Without limitation, PEXA has identified the following anti-Virus and firewall software vendors who provide products that meet these criteria:

- Symantec;
- McAfee;
- Trend Micro;
- Kaspersky Lab; and
- Sophos.

If you require further assistance in respect of Virus or firewall protection please refer to -

www.staysmartonline.gov.au

Subscribers are required to maintain the security of their computer systems and keep them up to date, including taking reasonable steps to install patches and operating system updates.

4.3 Protecting Security Items (Physical Security measures)

4.3.1 Protecting Access Credentials

Subscribers must ensure that they and their Users follow the requirements as set out in Section 4.7 of this Policy.

4.3.2 Protecting Digital Certificates

Subscribers must have in place and enforce appropriate security measures that restrict Users from storing Digital Certificates in places that may be accessed by unauthorised persons.

Subscribers must ensure that all Digital Certificates are protected by a password, PIN or passphrase.

4.3.3 Prevent Caching of Credentials

The Subscriber must ensure that the systems and applications provided and utilised by the Subscriber are not configured to cache passwords, PINs or passphrases needed to access the PEXA System. PEXA may deploy software to prevent Subscribers from caching passwords, PINs and passphrases.

4.4 Training and Monitoring

4.4.1 Compliance with and access to this Policy

Subscribers must provide a copy of this Policy to Users prior to allowing them access to the PEXA System. Subscribers must take reasonable steps to ensure Users understand and comply with this Policy.

4.4.2 Compliance with Certificate Authority policies

Subscribers must take reasonable steps to ensure Users issued with Digital Certificates have access to, and comply with, any agreements, policies and practice statements provided by the relevant Certification Authority.

4.4.3 Monitoring

Subscribers must take reasonable steps to monitor the usage of systems and activities of Users who are accessing the PEXA System to identify unusual or suspicious activities.

4.4.4 Training Obligation

Subscribers must take reasonable steps to provide Users with the training required to enable Users to comply with this Policy.

4.5 Users

4.5.1 User access

Subscribers must ensure that each of their personnel authorised to access the ELN is authorised to access the ELN under their own User profile and access credentials. Subscribers must take reasonable steps to ensure that User profiles and access credentials are not shared.

4.5.2 User management

Subscribers must perform regular checks of their User profiles and, where applicable remove inactive User profiles. Subscribers must regularly validate that details (including permissions, if any) relating to each of their Users are correct.

4.5.3 Compromised Access Credentials

Subscribers must immediately revoke a User's access to the PEXA System for any suspected or confirmed compromise of the credentials which they use to access the PEXA System ("**Access Credentials**").

4.5.4 Digital Certificate Compromise

The Subscriber must:

- promptly revoke a User's access to the PEXA System for any suspected or confirmed compromise of a Digital Certificate;
- immediately check all Electronic Workspaces in which the Digital Certificate has been used to Digitally Sign any electronic documents, Financial Settlement Schedule or any Line Items, and unsign any electronic documents in accordance with Participation Rule 7.9.2; and
- promptly notify the Certification Authority and revoke or cancel the relevant Digital Certificate (including doing everything reasonably necessary to cause the Certification Authority to revoke or cancel it).

4.5.5 Re-enabling Access

Subscribers must only re-enable access to the PEXA System after taking reasonable steps to mitigate the risk of the compromise re-occurring.

In case of a Digital Certificate compromise, access to the PEXA System must only be re-enabled after receiving confirmation from the Certification Authority that the affected Digital Certificate has been revoked.

4.6 Revoking Authorisation

4.6.1 Access to the PEXA System

When a Subscriber no longer wants a User to access the PEXA System at all, or in a particular capacity (e.g. Signers and Administrators), then the Subscriber must promptly modify the User's access privileges accordingly.

Subscribers must regularly (and in any event, at least annually) review access privileges granted to Users. These access privileges must be promptly updated if they are no longer accurate.

4.7 Subscriber Obligations

Subscribers must comply, and must take reasonable steps to ensure that Users comply, with the following requirements:

4.7.1 Protecting passwords

Subscribers must make, and take reasonable steps to ensure Users make, passwords as strong as possible. Passwords used to access the PEXA System must be at least eight characters long and contain 3 out of the following 4 categories: Upper Case [A-Z] Lower Case [a-z] Numbers [0-9] Special Characters [e.g. @#$%]. User name or personal details must not be used in passwords.

Subscribers must ensure that passwords, PINs and passphrases used in the PEXA System by Users are:

- not disclosed to anyone, including a colleague, supervisor, family member or friend;
- not disclosed to anyone whilst being entered into electronic equipment or systems;
- immediately changed if the Subscriber or the User becomes aware that a particular password, PIN or passphrase has become known or used by someone else;
- comprise a minimum 6 digits or characters for Digital Certificates;
- not be closely associated with the User's identity such that it may be easily guessed by others. This means avoiding the use of the User's date of birth, name, phone numbers or similar items as passwords, passphrases or PINs; and
- be different from other existing Access Credentials.

4.7.2 Protecting Digital Certificates

Subscribers must install Digital Certificates on Hardware Tokens unless otherwise approved.

Subscribers must:

- ensure that Hardware Tokens are protected by a PIN or passphrase;
- ensure that Users disconnect any Hardware Token from their computer when the User is no longer accessing the PEXA System; and
- take adequate measures to ensure that Users protect Hardware Tokens from unauthorised use or access.

4.7.3 Reporting non-compliance

Subscribers must take reasonable steps to ensure that Users promptly report all suspected or actual breaches of this Policy to the Subscriber.

5. Multi-factor Authentication

PEXA may require Users to perform multi-factor authentication when accessing the PEXA System or when performing certain actions within the PEXA System. PEXA reserves the right to determine the method and frequency of multi-factor authentication, which may change from time to time.

6. Reporting Obligations

The Subscriber must, immediately upon becoming aware, notify PEXA of any breach of this Policy that may affect the PEXA System or the integrity or security of the ELN.

7. Ongoing Review of this Policy

This Policy may be reviewed and amended by PEXA as required from time to time in accordance with the change management provisions contained in the Participation Agreement.

8. Definitions

Terms used in this Policy that are defined in the ECNL, the Participation Rules or the Operating Requirements shall have the meaning given to them in the ECNL, the Participation Rules or the Operating Requirements (as the case

may be). In addition, the definitions set out in Attachment B of the Participation Agreement shall apply in this Policy.