PEXA Subscriber Review Process

Guidance Notes

Version 1.0

PEXA
Property Exchange Australia

Contents

Introduction

Operating Requirement 14.7 of the Australian Registrars National Electronic Conveyancing Council's (ARNECC's) Model Operating Requirements (MOR) requires PEXA to establish, implement, review and keep current a Subscriber Review Process (SRP) to ensure Subscribers are complying with the Model Participation Rules (MPR).

The SRP has been developed to focus on the following three MPR categories:

1. Eligibility Criteria;
2. General Obligations; and
3. System Security and Integrity.

To support the completion of the SRP, these Guidance Notes are designed to assist PEXA Members with answering the SRP questions.

For each SRP question, you will see the following guidance structure:

Review question
The question as it appears in the SRP questionnaire.

Requirement
Your obligation under the Participation Rules.

Purpose
What the requirement is intended to achieve.

Compliance
PEXA's expectations of your arrangements to comply with the requirement.

Compliance Demonstration
How you are required to demonstrate your compliance.

Whilst completing the SRP questionnaire, it is recommended that you have these Guidance Notes readily available in addition to the following documentation:

- Participation Rules Version 5; and
- PEXA Subscriber Security Policy.

Further questions regarding the questionnaire or the Subscriber Review Process can be directed to: SubscriberReviewProcess@pexa.com.au

Questionnaire

Primary Subscriber Managers will be notified via email[1] if their organisation has been selected to complete the SRP questionnaire.

To access the Subscriber Review portal, Primary Subscriber Managers will need to log into the PEXA Exchange and click on the 'Subscriber Review' button located on the right-hand side of their Dashboard as per Diagram 1:

Diagram 1: 'Subscriber Review' button

Upon clicking the 'Subscriber Review' button, Primary Subscriber Managers will be directed to the Subscriber Review portal where the questionnaire link will appear as highlighted by the light purple oval object as per Diagram 2. Primary Subscriber Managers will need to click on the "SRP <Month> <Year> <Subscriber>" link to access the SRP questionnaire.

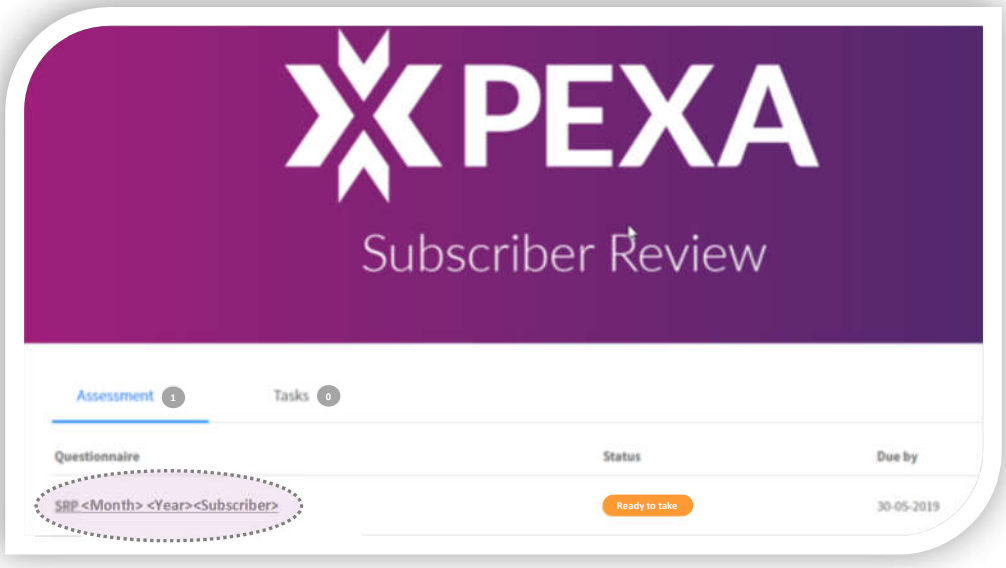

Diagram 2: Subscriber Review portal

[1] Note: The e-mail will not include a link to the Subscriber Review portal as PEXA will never send a link to a login page in an e-mail to its Members.

4.3.1(a) Good Character and Reputation – Organisation

Review question

4.3.1(a) If your organisation is not deemed to comply with Participation Rule 4.3.1(a), has it been subject to any of the matters listed in 4.3.1(b)(i) to (v)?

Requirement

Your organisation has an obligation to be of good character and reputation.

Purpose

The purpose of this obligation is to ensure all Subscribers that use the PEXA Exchange are of good character and reputation.

Compliance

Your organisation must not be or have not been subject to any of the matters listed below:

(i) an Insolvency Event within the last five years; or
(ii) a conviction for fraud or an indictable offence or any offence for dishonesty against any law in connection with business, professional or commercial activities; or
(iii) disqualification from managing a body corporate under the Corporations Act; or
(iv) any disciplinary action of any government or governmental authority or agency, or any regulatory authority of a financial market or a profession, which may impact on that Person's conduct of a Conveyancing Transaction; or
(v) any refusal of an application to subscribe to an electronic Lodgement service.

Compliance Demonstration

If your organisation **has** been subject to any of the above, select "Yes". In responding "Yes", you are required to outline which of the matters in (i) to (v) that your organisation has been subject to and subsequent steps taken to remedy the situation.

If your organisation **has not** been subject to any of the above, select "No".

If your organisation is **deemed to comply**, select "N/A (My organisation is deemed to comply)".
Note: Per Participation Rule 4.3.2, where a Subscriber is:

(i) an Authorised Deposit-Taking Institution; or
(ii) an Australian Legal Practitioner or a Law Practice; or
(iii) a Licensed Conveyancer; or
(iv) the Crown in right of the Commonwealth, a State or a Territory; or
(v) a Public Servant acting on behalf of the Crown in right of the Commonwealth, a State
(vi) or a Territory; or
(vii) a holder of an Australian Credit Licence; or
(viii) a Local Government Organisation; or
(ix) a Statutory Body.

the Subscriber is deemed to comply with Participation Rule 4.3.1(a).

4.3.1(b) Good Character and Reputation – Principals, Directors, Partners, Officers and Subscriber Administrators

Review Question

This review question is dependent on your response to the previous question *4.3.1(a) If your organisation is not deemed to comply with Participation Rule 4.3.1(a), has it been subject to any of the matters listed in 4.3.1(b)(i) to (v)?*

If your answer was "Yes" or "No", you will be asked:
4.3.1(b) How has your organisation taken reasonable steps to ensure that your principals, directors, partners, officers and Subscriber Administrators are not and have not been subject to any of the matters listed in 4.3.1(b)(i) to (v)?

If your answer was "N/A (My organisation is deemed to comply)", you will not see this question. Per Participation Rule 4.3.3, where the Subscriber's principal, director, partner, officer or Subscriber Administrator is:

(i) an officer or employee of an Authorised Deposit-Taking Institution; or
(ii) an Australian Legal Practitioner; or
(iii) a Licensed Conveyancer; or
(iv) a Public Servant acting on behalf of the Crown in right of the Commonwealth, a State or a Territory; or
(v) a fit and proper Person for the purpose of performing duties in relation to the credit activities authorised by an Australian Credit Licence; or
(vi) a Local Government Officer acting on behalf of a Local Government Organisation; or
(vii) a Statutory Body Officer acting on behalf of a Statutory Body

the Subscriber is deemed to comply with Participation Rule 4.3.1(b) for that principal, director, partner, officer or Subscriber Administrator.

Note: For a body corporate registered under the Corporations Act, 'officer' has the meaning given to it in the Corporations Act.

Requirement

Your organisation has an obligation to ensure its principals, directors, partners, officers and Subscriber Administrators are of good character and reputation.

Purpose

The purpose of this obligation is to ensure that a Subscriber's principals, directors, partners, officers and Subscriber Administrators are of good character and reputation.

Compliance

Your organisation must take reasonable steps to ensure its principals, directors, partners, officers and Subscriber Administrators are of good character and reputation and have not been subject to any of the matters listed below:

(i) an Insolvency Event within the last five years; or
(ii) a conviction for fraud or an indictable offence or any offence for dishonesty against any law in connection with business, professional or commercial activities; or
(iii) disqualification from managing a body corporate under the Corporations Act; or

(iv) any disciplinary action of any government or governmental authority or agency, or any regulatory authority of a financial market or a profession, which may impact on that Person's conduct of a Conveyancing Transaction; or

(v) any refusal of an application to subscribe to an electronic Lodgement service.

Compliance Demonstration

To demonstrate compliance, outline how your organisation has taken reasonable steps to ensure that your principals, directors, partners, officers and Subscriber Administrators have not and are not subject to any of the matters listed above.

If any of your principals, directors, partners, officers and Subscriber Administrators **have** been subject to any of the above, you are required to outline which of the matters in (i) to (v) that they have been subject to and subsequent steps taken to remedy the situation.

Examples of some steps that may be taken by organisations include the completion of a combination of the following:

- Police checks
- Background checks
- Employment screening
- Bankruptcy checks
- ASIC Banned and Disqualified register check

4.4 Insurance Rules – Principal Subscribers and Non-Authorised Deposit-Taking Institutions only

Review Question

4.4 For Principal Subscribers (excluding government bodies) and Non-Authorised Deposit-taking Institutions (where no waiver has been issued) only: Do you hold Professional Indemnity and Fidelity Insurance?

Requirement

Your organisation must hold Professional Indemnity and Fidelity Insurance.

Purpose

The purpose of this obligation is to ensure Subscribers are appropriately insured.

Compliance

You must hold Professional Indemnity and Fidelity Insurance in line with the requirements outlined in Schedule 6 of the MPR.

In general, lawyers and conveyancers are deemed to comply with the Insurance Rules (see section 4, Schedule 6 of the MPR). Authorised Deposit-taking Institutions, the Crown, Local Government Organisations and Statutory Bodies are also deemed to comply with these Insurance Rules (see section 3, Schedule 6 of the MPR).

Compliance Demonstration

If you are deemed to comply as per Schedule 6 of the MPR, select "N/A (My organisation is deemed to comply as per Schedule 6 of the Participation Rules)".

If you are a Non-Authorised Deposit-taking Institution (where no waiver has been issued) or Principal Subscriber (excluding government bodies) and hold Professional Indemnity or Fidelity Insurance, please select "Yes" and provide the certificates of currency for each insurance policy you hold. The certificate must be valid at the time of submission.

If you are a Non-Authorised Deposit-taking Institution (where no waiver has been provided) or Principal Subscriber (excluding government bodies) and do not hold Professional Indemnity or Fidelity Insurance, select "No" and outline the steps you are taking to remedy the situation. In your response you should stipulate the steps you are taking to obtain the relevant insurances as per Schedule 6 of the MPR and provide a reasonable timeframe as to when the certificate of currency will be made available to PEXA.

6.1.1 – User awareness of the terms of the Participation Rules

Question for Information
6.1.1 How many employees within your organisation use the PEXA Exchange?

Purpose
This question is for information purposes only, to inform which additional questions are applicable to your organisation.

Expected Response
Select the number of employees within your organisation that use the PEXA Exchange, either "1" or "Greater than 1".

If you selected "Greater than 1", a subsequent question will prompt you to enter the number of employees within your organisation that use the PEXA Exchange.

Review Question
If you selected "1" to the question above, you will subsequently be asked:
6.1.1 How do you keep yourself aware of the terms of the Participation Rules as appropriate to your use of the PEXA Exchange?

If you selected "Greater than 1" to the question above, you will subsequently be asked:
6.1.1 How does your organisation make Users aware of the terms of the Participation Rules as appropriate to their use of the PEXA Exchange?

Requirement
Your organisation has an obligation to ensure that each User is aware of the terms of the Participation Rules as appropriate to their use of the PEXA Exchange.

Purpose
The purpose of this obligation is to ensure all Users of the PEXA Exchange comply with the Participation Rules.

Compliance
You must ensure all Users are aware of and comply with the Participation Rules.

Compliance Demonstration
To demonstrate compliance, outline how your organisation ensures its User(s) are aware of the Participation Rules as appropriate to their use of the PEXA Exchange. This can include, for example, having in place a formal annual refresher process of the Participation Rules.

Note: Upon completion of this question in the SRP portal, you will be asked to complete the question relating to '**7.2.1(b) – Training in the use of the PEXA Exchange'**. Guidance relating to this question can be found on **page 26**.

6.10 – Protection of Information

Review Question

6.10. Outline the steps your organisation takes to ensure that information provided to your organisation by any other Subscriber, any Client, the Registrar or by PEXA is protected from unauthorised use, reproduction or disclosure.

Requirement

You have an obligation to protect information provided to you from unauthorised use, reproduction or disclosure.

Purpose

The purpose of this requirement is to ensure that all Subscribers take appropriate steps to protect information.

Compliance

Your organisation must take reasonable steps to ensure all information provided by another Subscriber, any Client, the Registrar or PEXA is protected from unauthorised use, reproduction or disclosure.

Compliance Demonstration

Outline the steps your organisation takes to protect information. This can include having an organisational Privacy Policy and training and awareness programs for your Users (as required).

Further guidance on what constitutes reasonable steps to protect information is available through the Office of the Australian Information Commissioner (OAIC) website: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

Note: IT security related processes and procedures will be considered separately in the review questions regarding System Security and Integrity.

6.12 – Subscription to the PEXA Exchange

Review Question
6.12 Has your subscription to the PEXA Exchange been assigned, Novated, transferred or otherwise dealt to you?

Requirement
Subscriptions to the PEXA Exchange must not be assigned, Novated, transferred or otherwise dealt with.

Purpose
The purpose of this requirement is to ensure that all Subscribers have appropriately registered to operate on the PEXA Exchange in accordance with the Participation Rules.

Compliance
Each organisation must maintain its own subscription to the PEXA Exchange, and a subscription cannot be assigned, Novated, transferred or otherwise dealt with.

Compliance Demonstration
If your organisation **has not registered** with PEXA to use the PEXA Exchange (including entering into a Participation Agreement with PEXA), select "Yes". You will then be given an opportunity to outline the steps you are taking to remedy the situation to appropriately register your organisation to operate on the PEXA Exchange.

If your organisation **has registered** with PEXA to use the PEXA Exchange (including entering into a Participation Agreement with PEXA), select "No".

6.15 – Conduct of conveyancing transactions

Review Question

6.15(b) How does your organisation comply with state-based practitioner regulator guidance on who is entitled to electronically sign Registry Instruments?

Requirement

You have an obligation to ensure that your organisation takes reasonable steps to ensure that each Signer complies with the laws of the Jurisdiction regarding who can Digitally Sign Registry Instruments within the relevant states.

Purpose

The purpose of this obligation is to ensure that all Registry Instruments are signed by Signers who are legally entitled in accordance with state-based laws.

Compliance

To satisfy this requirement, Signers within your organisation must comply with the directions issued by ARNECC based on advice provided by practitioner regulators as per below: https://www.arnecc.gov.au/__data/assets/pdf_file/0003/1264125/entitlement-to-sign-registry-instruments.pdf

Compliance Demonstration

To demonstrate compliance, outline the steps your organisation takes to ensure that a Signer complies with state-based laws regarding who can sign Registry Instruments. This can include how you determine who can sign in the PEXA Exchange, for example by ensuring that a User has a conveyancing licence/practising certificate prior to providing a User with signing permission.

7.1(a) - PEXA Subscriber Security Policy

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.2.1 Ensuring Signers sign documents in the PEXA Exchange using their own Digital Certificate.
(i.e. does each Signer have their own Digital Certificate)

Requirement

You have an obligation to ensure that Users with signing permissions sign documents using their own Digital Certificate.

Purpose

The purpose of this obligation is to maintain the security and integrity of the ELN so that all stakeholders have confidence that documents have been appropriately signed by an authorised individual.

Compliance

Each Signer within your organisation must have their own Digital Certificate and only signs documents using their allocated Digital Certificate.

Compliance Demonstration

To demonstrate compliance, outline how you ensure each Signer has their own Digital Certificate and each Digital Certificate is used by the allocated Signer only. This can include referencing process guides used by your organisation that outline necessary steps to be satisfied before a Digital Certificate is used.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.2.3 Having Anti-Virus and Firewall software that aligns with the minimum attributes of 4.2.3. (including outlining what product you use and current version)

Requirement

Anti-Virus software

Viruses and Malware are forms of malicious software introduced into an electronic device such as your computer or mobile device with the malicious intent of causing harm to compromise the confidentiality, integrity or availability of your systems and computer networks or data held on these systems.

You have an obligation to take reasonable steps to implement Anti-Virus software and Malware protection against any unauthorised or uncontrolled access to IT systems and access points that are used by you to access the PEXA Exchange.

You must ensure that the Anti-Virus software and Malware protection meets the following minimum operating requirements:

(i) The ability to identify and remove viruses and Malware (malicious software programs);
(ii) The ability to identify and remove other types of harmful computer software, generally referred to as Malware (or malicious software);
(iii) The ability to automatically receive Anti-Virus updates frequently; and
(iv) The ability to automatically scan for viruses and Malware in documents on servers and workstations and take actions to clean/remove.

Firewall software

You have an obligation to take reasonable steps to provide Firewall protection against any unauthorised intrusions or uncontrolled access to the systems and access points that your organisation may use to access the PEXA Exchange, regardless of whether such access occurs by means of the Internet or some other electronic form of communication.

You must ensure that the Firewall software has the ability to provide Firewall protection either as a standalone device, or on the router and on the built-in software on the device. A properly configured Firewall will inspect all messages entering or leaving your computer through the Firewall, which examines each message and blocks those that do not meet the specified security criteria.

Without limitation, PEXA has identified the following Anti-Virus and Firewall software vendors who provide products that meet the above criteria:

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

Purpose

The purpose of having Anti-Virus software and Malware protection is to protect your IT systems and reduce the risk of data loss. The purpose of a Firewall is to prevent unauthorised access to or from your network.

Compliance

You must have in place:

- Anti-Virus software and Malware protection which meets the four minimum operating requirements set out above under 'Requirements'; and
- A Firewall protection solution either installed on your system or on the network perimeter.

Compliance Demonstration

To demonstrate compliance, you are to provide written confirmation:

- that the Anti-Virus software and Malware protection meets the four minimum operating requirements set out above under 'Requirements';
- advising which Anti-virus software and Malware protection solution and version your organisation uses and the frequency in which the Anti-Virus and Malware scanner is run; and
- advising which Firewall protection solution and version your organisation uses including your organisation's approach to firewall configuration and whether the Firewall is installed on a standalone device/router or is built in software on relevant devices.

If you outsource the management of your IT environment, please request the above details from your managed IT provider.

If you do not have anti-virus software, malware protection and a firewall protection solution installed, please provide a reason as to why this is the case and how you intend on rectifying this going forward.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.2.3 Keeping IT systems up to date which include installing Patches and operating system updates.

Requirement

You have an obligation to keep your IT systems up to date by taking reasonable steps to install Patches and operating system updates (including security specific updates).

Purpose

The purpose of patching and operating system updates is to address vulnerabilities discovered after the release of software. Patches apply to many different parts of an information system including operating systems, servers, routers, desktops, email clients, office suites, mobile devices, firewalls, and other components which exist within a computer network.

Compliance

You are expected to have a software patching schedule or procedure which is run frequently. This must include IT infrastructure such as operating systems, web browsers, endpoint devices that support your ability to access the PEXA Exchange.

Compliance Demonstration

To demonstrate compliance, outline how you address the following:

- Your approach to patching your IT systems and applications;
- Frequency of patching for devices that access the PEXA Exchange;
- Process for validating patching has been applied to all computers in your organisation which access PEXA Exchange; and
- If patching is managed by a 3rd party, the procedures that are in place to validate completion of patching.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.3.1 & 4.3.2 Protecting Access Credentials and Digital Certificates from unauthorised access and use.

Requirement

You have an obligation to ensure that you and your Users protect Access Credentials and Digital Certificates from unauthorised access and use.

In relation to Access Credentials, you must take reasonable steps to ensure Users make passwords as strong as possible. Passwords used to access the PEXA Exchange 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]; and
- Special Characters [e.g. @#$%].

Usernames or personal details must not be used in passwords. You must ensure that passwords, PINs and passphrases used in the PEXA Exchange 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 you or your Users become aware that a particular password, PIN or passphrase has become known or used by someone else;
- 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.

In relation to Digital Certificates, you must install Digital Certificates on Hardware Tokens unless otherwise approved. You must also:

- Ensure that Hardware Tokens are protected by a PIN or passphrase;
- Ensure Digital Certificates are stored in a safe location and removed from a User's computer when no longer accessing the PEXA Exchange;
- Disable Digital Certificates when Users no longer require one;
- Ensure Digital Certificates are not shared between Users; and
- Immediately notify PEXA upon becoming aware of any theft, unauthorised disclosure or improper use of Digital Certificates on PEXA Exchange.

Purpose

The purpose is of this requirement is to mitigate the risk of an IT security breach or fraud in the PEXA Exchange.

Compliance

You must have measures in place to protect Access Credentials and Digital Certificates from unauthorised access and use.

Compliance Demonstration

To demonstrate compliance, outline the processes you have in place to:

- communicate the minimum requirements to Users regarding the types of passwords that can and cannot be used;
- make Users aware of how to protect their Access Credentials and Digital Certificates;
- stop Users from disclosing/sharing their passwords, PINs and passphrases;
- handle any suspected or actual instances of Compromised Access Credentials;
- store Digital Certificates in a safe location;
- ensure Signers disconnect their Digital Certificates from their computer when they are no longer accessing the PEXA Exchange;
- manage Digital Certificates when no longer required by a User;
- ensure that Users only sign documents in the PEXA Exchange using their own Digital Certificate; and
- immediately notify PEXA upon becoming aware of any theft, unauthorised disclosure or improper use of Digital Certificates on PEXA Exchange.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.4.1 & 4.4.4 Ensuring Users understand and are provided training on PEXA's Subscriber Security Policy.

Requirement

You have an obligation to provide a copy of the PEXA Subscriber Security Policy to Users as well as ensuring they understand and comply with this Policy prior to allowing them access to the PEXA Exchange.

Purpose

The purpose of this requirement is to ensure Users are aware of the security requirements that Subscribers and Users must adhere to when using the PEXA Exchange.

Compliance

You are expected to have a process in place that ensures that, prior to a User being provided with access to the PEXA Exchange, the User has:

- been provided with a copy of the PEXA Subscriber Security Policy; and
- demonstrated an understanding of the Policy.

Compliance Demonstration

To demonstrate compliance, you are to confirm that the PEXA Subscriber Security Policy is provided to Users prior to allowing them to access the PEXA Exchange. You must also outline how you confirm your Users are aware of the requirements of the Policy prior to providing access to the PEXA Exchange. Examples of some of the processes that could be in place include:

- Including the PEXA Subscriber Security Policy as part of the employee induction training program.
- Allocating time to review and understand the PEXA Subscriber Security Policy as part of your internal PEXA training program.
- Mandating completion of an assessment (verbal or written) to confirm understanding with a minimum pass mark.

Review Question
7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.4.3 Monitoring User activity for unusual or suspicious activities.

Requirement
You have an obligation to take reasonable steps to monitor the usage of systems and activities of Users who are accessing the PEXA Exchange to identify unusual or suspicious activities.

Purpose
The purpose is of this requirement is to mitigate the risk of fraud in the PEXA Exchange.

Compliance
You are expected to have processes in place to monitor User activity on the PEXA Exchange for unusual or suspicious activities.

Compliance Demonstration
To demonstrate compliance, outline the processes that you have in place to identify unusual or suspicious activity within the PEXA Exchange. Examples of some of the processes that could be in place include:

- Periodically reviewing the list of Users and Signers within the PEXA Exchange.
- Confirming the validity of open and completed Workspaces.
- Undertaking additional validation of financial line items.
- Monitoring the signing of documents and financial line items outside of business hours.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.5.1 Ensuring User profiles and Access Credentials are not shared.

Requirement

You have an obligation to take reasonable steps to ensure that User profiles and Access Credentials are not shared. Access Credentials in this context relate to the PEXA Exchange password and multi-factor authentication passcode.

Purpose

The purpose of this obligation is to maintain the security and integrity of the ELN so that:

- Access to the PEXA Exchange is appropriately managed; and
- All stakeholders have confidence that PEXA Exchange activity is actioned by proper and authorised individuals.

Compliance

Each User of the PEXA Exchange must have their own Access Credentials and these Access Credentials and User profiles must not be shared.

Compliance Demonstration

To demonstrate compliance, outline how you ensure your User profiles and Access Credentials are not shared. Key considerations include having internal processes for:

- setting up each employee as a PEXA Exchange User with their own Access Credentials;
- monitoring employee access to the PEXA Exchange and taking immediate corrective action where an employee who is not an authorised User is accessing the PEXA Exchange;
- managing User access when Users are out of office; and
- promptly removing User access when Users leave the organisation or change roles.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.5.2 Performing User access reviews (at least annually, including validation of permissions) and removing Inactive User profiles.
(for both Access Credentials and Digital Certificates)

Requirement

You have an obligation to, at least annually, review your PEXA account to:

- confirm only authorised Users continue to retain access to the PEXA Exchange;
- confirm only authorised Signers continue to hold a valid Digital Certificate;
- confirm PEXA Exchange permissions are still appropriate for each User (applying the principle of Least Privilege access) as it relates to the duties set-out in their employment agreement; and
- remove Users no longer requiring access to the PEXA Exchange.

Purpose

The purpose of this requirement is to ensure that only authorised Users continue to have access to the PEXA Exchange.

Compliance

You are expected to be performing User access reviews on at least an annual basis.

Compliance Demonstration

To demonstrate compliance, outline the steps you take to perform User access reviews, including validation of permissions and removing Inactive User profiles (for both Access Credentials and Digital Certificates). Your response should include:

- The frequency of reviews;
- What is in scope for each review; and
- Whether this activity forms part of your organisation's overarching user access review process and/or policy (if applicable).

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 4.6.1 Promptly modifying User access privileges as circumstances change.
(i.e. User misconduct, User leaving the organisation or changing roles internally) (for both Access Credentials and Digital Certificates)

Requirement

You have an obligation to promptly modify User access privileges when you no longer want a User to access the PEXA Exchange at all, or in a particular capacity (e.g. Signers and Subscriber Administrators). This also includes where there is User misconduct, when Users leave your organisation or when Users change roles internally.

Purpose

The purpose of this requirement is to ensure that only authorised Users continue to have access to the PEXA Exchange.

Compliance

You are expected to have an operational process in place to promptly modify User access privileges as circumstances change.

Compliance Demonstration

To demonstrate compliance, outline the process you have in place to promptly modify User access privileges as circumstances change. Key considerations include:

- the timeframe in which you modify User access privileges after circumstances change; and
- if the PEXA Exchange is embedded in your human resource offboarding process.

Review Question

7.1(a) Outline how your organisation complies with the following elements of PEXA's Security Policy: 6 Notification to PEXA of breaches of PEXA's Subscriber Security Policy.

Requirement

You have an obligation to immediately, upon becoming aware, notify PEXA of any breach of the PEXA Subscriber Security Policy that may affect the PEXA Exchange or the integrity or security of the ELN.

Purpose

The purpose of this reporting obligation is to protect the integrity or security of the ELN should you identify any breach of the PEXA Subscriber Security Policy within your organisation.

Compliance

You are expected to have processes in place to detect instances of non-compliance with PEXA Subscriber Security Policy. Upon identification of any breaches, you must immediately notify PEXA.

Compliance Demonstration

To demonstrate compliance, outline the processes you have in place for:

- Your Users to report to you all suspected or actual breaches of the PEXA Subscriber Security Policy; and
- Immediate notification to PEXA once you are aware of such a breach.

In order for Users to be able to detect suspected or actual breaches of the PEXA Subscriber Security Policy, it is essential that they aware of the key elements of this Policy. Consequently, section 4.4 of this Policy relating to Training and Monitoring is a prerequisite for compliance with this requirement (section 4.7.3).

7.2.1 (a) – User access to the PEXA Exchange

Review Question
7.2.1(a) Have you created generic/shared User accounts for the purposes of accessing the PEXA Exchange?

Requirement
Your organisation is required to take reasonable steps to ensure that only Users access the PEXA Exchange.

Purpose
The purpose of this requirement is to maintain the integrity of the ELN by ensuring that all Users of the PEXA Exchange are authorised individuals.

Compliance
Your organisation must not have any generic User accounts within the PEXA Exchange.

Compliance Demonstration
If you **have not** created generic/shared User accounts for the purpose of accessing the PEXA Exchange, select "No".

If you **have** created generic/shared User accounts for the purpose of accessing the PEXA Exchange, select "Yes". You will then be prompted to outline the reason why these were created. In providing your rationale, please also include a list of the generic/shared User accounts in place and outline any steps taken to remove these accounts from the PEXA Exchange.

Note: A generic/shared User account is a User profile that is not associated with a particular individual, for example a User profile with the first name being "Office" last name being "Admin".

7.2.1(b) – Training in the use of the PEXA Exchange

Review Question

This review question is dependent on your response to the earlier question *6.1.1 How many employees within your organisation use the PEXA Exchange?*

If your answer was "1", you will be asked:
7.2.1(b) How do you maintain your knowledge of the use of the PEXA Exchange?

If your answer was "Greater than 1", you will be asked:
7.2.1(b) How does your organisation ensure that each User has received training appropriate to their use of the PEXA Exchange?

Requirement

You are required to ensure that each User within your organisation has received training appropriate for their use of the PEXA Exchange.

Purpose

The purpose of this requirement is to ensure all Users of the PEXA Exchange have the necessary knowledge to perform required tasks within the PEXA Exchange.

Compliance

You are expected to have a process in place to ensure all employees of your organisation who access the PEXA Exchange have been provided with training appropriate to their use of the PEXA Exchange.

Compliance Demonstration

To demonstrate compliance, outline the steps your organisation takes to ensure each User has received training appropriate to their use of the PEXA Exchange. This can include a training manual that your organisation uses, induction programs, online webinars, PEXA Certified programs, PEXA Direct training sessions etc. and recording completion of these activities via a training log or register.

7.2.2 – Application to application technology

Review Question

7.2.2 Does your organisation use automation tools (e.g. robotics/artificial intelligence) to access the PEXA Exchange and for data entry? (for both Access Credentials and Digital Certificates)

Requirement

You may use application to application technology for accessing the PEXA Exchange and data entry (e.g. robotics/artificial intelligence) provided that you do not use application to application technology for the function of Digital Signing or for Subscriber Administrator functions.

Purpose

The purpose of this requirement is to limit the use of automation tools within the PEXA Exchange so that core processes are completed by a natural person.

Compliance

Where your organisation uses automation tools, it must not use automation tools for the function of Digital Signing or for Subscriber Administrator functions.

Compliance Demonstration

If you do not use automation tools, select "No".

If you do use automation tools, select "Yes". You will then be required to confirm if this is used for Digital Signing or for Subscriber Administrator functions.

7.4.1 – Signers and background checks

Question for Information
7.4.1 How many employees within your organisation digitally sign in the PEXA Exchange?

Purpose
This question is for information purposes only, to inform which additional questions are applicable to your organisation.

Expected Response
Select the number of employees within your organisation that digitally sign in the PEXA Exchange, either "1" or "Greater than 1".

If you selected "Greater than 1", a subsequent question will prompt you to enter the number of employees within your organisation who digitally sign in the PEXA Exchange.

Review Question
If you selected "Greater than 1" to the question above, you will subsequently be asked:
7.4.1 What is your onboarding/probity process for Signers? (i.e. do you conduct background and police checks?) and
7.4.1 Do you conduct ongoing background and police checks on your Signers?

Requirement
You are required to take reasonable steps to verify the identity of each Signer prior to the initial allocation of a Digital Certificate, and ensure that each Signer is not or has not been subject to:

(i) an Insolvency Event within the last five years; or
(ii) a conviction of fraud or an indictable offence or any offence for dishonesty against any law in connection with business, professional or commercial activities; or
(iii) disqualification from managing a body corporate under the Corporations Act; or
(iv) any disciplinary action of any government or governmental authority or agency, or any regulatory authority of a financial market or a profession, which may impact on a Signer's conduct of a Conveyancing Transaction.

Purpose
The purpose of this requirement is to ensure confidence in the individuals within your organisation that have the authority to sign in the PEXA Exchange.

Compliance
Your organisation must take reasonable steps to ensure that each Signer is not and has not been subject to any of the matters listed above.

Compliance Demonstration
If all Signers are deemed to comply as per Participation Rule 7.4.2, please respond with "N/A – My organisation is deemed to comply".

Where one or more Signers **are not deemed to comply**, you are required to outline how your organisation takes reasonable steps to ensure that each Signer that is not deemed to comply is not and has not been subject to any of the matters listed above.

Examples of some steps that may be taken by organisations include the completion of a combination of the following:

- Police checks
- Background checks
- Employment screening
- Bankruptcy check
- ASIC Banned and Disqualified register checks

7.7.1 – Jeopardised Conveyancing Transactions

Review Question

7.7.1 Have there been any instances where, to your knowledge, information or belief, a Conveyancing Transaction(s) has been Jeopardised?

Requirement

Where, to your knowledge, information or belief, a Conveyancing Transaction has been Jeopardised, you are required to:

(a) where possible, unsign any electronic Registry Instruments and other electronic documents relating to the Conveyancing Transaction immediately; and
(b) where it is not possible to unsign any electronic Registry Instruments or other electronic documents, immediately notify PEXA.

You must also bring to the attention of the other Participating Subscribers any information about the Conveyancing Transaction that it believes to be incorrect, incomplete, false or misleading or that the Conveyancing Transaction has been Jeopardised.

Purpose

The purpose of this requirement is to protect the integrity of the Titles Register.

Compliance

Where, to the organisation's knowledge, information or belief a Conveyancing Transaction has been Jeopardised, you are expected to have followed the required steps to unsign relevant items and inform other participants.

Compliance Demonstration

If there **have not** been any instances where a Conveyancing Transaction(s) has been Jeopardised, select "No".

If there **has** been an instance(s) where a Conveyancing Transaction has been Jeopardised, select "Yes". You will then be prompted to outline what led you to believe there was a compromise, and what action(s) you took in response to the incident.

7.9.1 – Compromise of Security Items

Review Question

7.9.1(a) Have there been any instances where User Access Credentials, passphrases, Private Keys, Digital Certificates, Electronic Workspace identifiers relevant to the PEXA Exchange have been or are likely to have been Compromised?

Requirement

If you become aware that any of the Security Items listed above have been or are likely to have been Compromised, you are required to:

(i) Immediately revoke the User's authority to access and use the PEXA Exchange and prevent the User from accessing and using the PEXA Exchange; and

(ii) For a Digital Certificate:

- Immediately check all Electronic Workspaces in which the Private Key has been used to Digitally Sign any electronic Registry Instruments and other electronic Documents and unsign any electronic Registry Instruments and other electronic Documents in accordance with Participation Rule 7.9.2; and
- Promptly notify the Certification Authority and revoke or cancel the Digital Certificate (including doing everything reasonably necessary to cause the Certification Authority to revoke or cancel it); and
- Promptly notify PEXA.

Purpose

The purpose of this requirement is to ensure appropriate actions are taken in the event Security Items have been or are likely to have been Compromised.

Compliance

Where your organisation has become aware that any of the Security Items listed above have been or are likely to have been Compromised, you must follow the steps outlined above.

Compliance Demonstration

If there **have not** been any instances where User Access Credentials, passphrases, Private Keys, Digital Certificates, Electronic Workspace identifiers have been or are likely to have been Compromised, select "No".

If there **have** been any instances where your User Access Credentials, passphrases, Private Keys, Digital Certificates, Electronic Workspace identifiers have been or are likely to have been Compromised, select "Yes". You will then be prompted to describe the incident and what action(s) you took in response to the incident.

Glossary

Capitalised terms used in these guidance notes have the meanings referenced or set out here or the meanings given to them in the Participation Requirements or ECNL.

Term	Definition
Access Credentials	A User's authentication information—typically a password, a token, or a certificate.
Anti-Virus software	Software utility that detects, prevents, and removes viruses, and other malware from a computer. Most anti-virus programs include an auto-update feature that permits the program to download profiles if new viruses, enabling the system to check for new threats.
Australian Registrars' National Electronic Conveyancing Council (ARNECC)	The body established by the Intergovernmental Agreement to facilitate the ongoing management of the regulatory framework for National Electronic Conveyancing.
Authorised Deposit-taking Institution (ADI)	Financial institutions in Australia are only permitted to accept deposits from the public if they are Authorised Deposit-taking Institutions (ADIs). The ADI's authority is granted by the Australian Prudential Regulation Authority (APRA) under the Banking Act 1959 (Cth).
Certification Authority	A Gatekeeper Accredited Service Provider that issues Digital Certificates that have been Digitally Signed using the Certification Authority's Private Key and provides certificate verification and revocation services for the Digital Certificates it issues.
Council of Australian Governments (COAG)	The peak intergovernmental forum in Australia responsible for managing matters of national significance or matters that need co-ordinated action by all Australian governments.
Compromised	Lost or stolen, or reproduced, modified, disclosed or used without proper authority.
Conveyancing Transaction	A transaction that involves one or more parties and the purpose of which is: a) to create, transfer, dispose of, mortgage, charge, lease or deal with in any other way an estate or interest in land, or b) (b) to get something registered, noted or recorded in the Titles Register, or c) (c) to get the registration, note or record of something in the Titles Register changed, withdrawn or removed.
Digital Certificate	An electronic certificate digitally signed by the Certification Authority which: a) identifies either a key holder and/or the business entity that he/she represents; or a device or application owned, operated or controlled by the business entity; and

	b) (b) binds the key holder to a key pair by specifying the public key of that key pair; and c) (c) contains the specification of the fields to be included in a Digital Certificate and the contents of each.
Digital Signing	In relation to an electronic communication or a document, means create a digital signature for the communication or document.
Electronic Conveyancing National Law (ECNL)	A national application law agreed to be established by Part 8 of the IGA that facilitates the implementation and operation of National Electronic Conveyancing in accordance with the COAG Agreement, as amended from time to time.
Electronic Lodgement Network (ELN)	A network established to create and electronically lodge registry instruments and other electronic documents with the jurisdiction's Land Registry.
Electronic Lodgement Network Operator (ELNO)	The legal entity authorised by a jurisdiction to operate an ELN in that jurisdiction.
Electronic Workspace	A shared electronic Workspace generated by the ELN.
Fidelity Insurance	A form of insurance protection that covers policyholders for losses that they incur as a result of fraudulent acts by specified individuals. It usually insures a business for losses caused by the dishonest acts of its employees.
Firewall software	System designed to prevent unauthorized access to or from a private network. Firewalls prevent unauthorized internet Users from accessing private networks connected to the internet.
Generic User	A User profile that is not associated with a particular individual, for example a User profile with the first name being "Office" last name being "Admin".
Inactive User	A PEXA User who has not logged into the PEXA Exchange over the past 100 days.
Intergovernmental Agreement (IGA)	The Intergovernmental Agreement for a National Electronic Conveyancing Law between the State of New South Wales, the State of Victoria, the State of Queensland, the State of Western Australia, the State of South Australia, the State of Tasmania and the Northern Territory of Australia, that came into operation on 21 November 2011 and as in force from time to time.
Insolvency Event	In relation to a Person, it means any of the following events: a) the Person is, or states that they are, unable to pay all the Person's debts, as and when they become due and payable; or b) the entrance into an arrangement, composition or compromise with, or assignment for the benefit of, all or any class of the Person's creditors or members or a moratorium involving any of them; or c) the appointment of a receiver, receiver and manager, controller, administrator, provisional liquidator or

	liquidator or the taking of any action to make such an appointment; or d) an order is made for the winding up or dissolution of the Person or a resolution is passed or any steps are taken to pass a resolution for its winding up or dissolution; or e) something having a substantially similar effect to (a) to (d) happens in connection with the Person under the law of any Jurisdiction.
Jeopardised	Put at risk the integrity of the Titles Register by fraud or other means.
Key	A string of characters used with a cryptographic algorithm to encrypt and decrypt.
Key Pair	A pair of asymmetric cryptographic Keys (one decrypting messages which have been encrypted using the other) consisting of a Private Key and a Public Key.
Least Privilege	The concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Privilege itself refers to the authorization to bypass certain security restraints.
Malware	Also known as malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware.
Model Operating Requirements (MOR)	A uniform set of requirements determined by ARNECC that are promulgated by the Registrars as Operating Requirements for ELNOs to comply with in their jurisdiction.
Model Participation Rules (MPR)	The Participation Rules in each State and Territory apply to the Subscribers to an Electronic Lodgement Network Operator (ELNO). They determine the rules Subscribers must comply with to be registered as a Subscriber with an ELNO and while continuing to be registered and use the ELNO's Electronic lodgement Network (ELN).
Novated	Substitution of an original party to a contract with a new party, or substitution of an original contract with a new contract
Operating Requirements (OR)	The requirements for ELNOs in a jurisdiction promulgated by that jurisdiction's Registrar and based upon ARNECC's Model Operating Requirements.
Participating Subscriber	For a Conveyancing Transaction, each Subscriber who is involved in the Conveyancing Transaction either directly because it is a Party or indirectly because it is a Representative of a Party.
Participation Rules (PR)	The rules for Subscribers to an ELN in a jurisdiction promulgated by that jurisdiction's Registrar and based upon ARNECC's Model Participation Rules.
Patches	A set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing

	security vulnerabilities and other bugs, and improving the usability or performance.
PEXA	Property Exchange Australia is Australia's online property exchange network. It assists members – such as lawyers, conveyancers and financial institutions – to lodge documents with Land Registries and complete financial settlements electronically.
PEXA's Subscriber Security Policy	Sets out the security requirements that Subscribers must ensure that they and their Users adhere to when using the PEXA Exchange in order to maintain the overall security of the PEXA Exchange.
Principle Subscriber	Has the ability to nominate other Subscribers to act on their behalf for transactions involving Local Government Organisations, Non-Local Government Organisation or Developers.
Private Keys	The Key in an asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation.
Professional Indemnity Insurance	Designed for professionals who provide advice or a service to their customers. It protects against legal costs and claims for damages to third parties which may arise out of an act, omission or breach of professional duty in the course business.
Public Key	The Key in an asymmetric Key Pair which may be made public.
Registrar	The State and Territory officials who have responsibility for each jurisdiction's Land Registry function.
Registry Instrument	For the purposes of the application of the ENCL as a law of a participating jurisdiction, has the meaning given by the application law of the jurisdiction.
Representative	A Subscriber who acts on behalf of a Client.
Security Items	User Access Credentials, passphrases, Private Keys, Digital Certificates, Electronic Workspace identifiers and other items as specified from time to time.
Signer	A user authorised by the Subscriber to Digitally Sign electronic Registry Instruments and other electronic Documents on behalf of the Subscriber
Subscriber	A legal entity registered to use an ELN to complete conveyancing transactions electronically, as or on behalf of, a Transacting Party.
Subscriber Administrator	Does not have access to Subscriber details or financial account information. They do have the ability to: • Create and edit Users • Create and edit Workgroups
Subscriber Manager	Holds the highest level of access to the PEXA Exchange. They have the ability to: • Create and edit Subscriber details • Setup and verify Financial Account information • Create and edit Users

	• Create and edit Workgroups
Subscriber User	Do not have administration rights, but have the ability to transact in the PEXA Exchange based on the rights set up by the Administrators.
Titles Register	The same meaning as Register has in the Transfer of Land Act 1958 (being the Register of land kept under section 27).
User	An individual authorised by a Subscriber to access and use the ELN on behalf of the Subscriber
Workspace	A shared area in PEXA where Subscribers prepare property instruments and settlement documents for a property exchange transaction to effect lodgement and or settlement.

Version Control

Version	Date	Revised by	Brief outline of changes
1.0	May 2019	-	Inaugural version