AUSTRALIAN REGISTRARS NATIONAL ELECTRONIC CONVEYANCING COUNCIL

MODEL PARTICIPATION RULES GUIDANCE NOTE 8

SYSTEM SECURITY & INTEGRITY

1 INTRODUCTION

This guidance note aligns with Version 6 of the Model Participation Rules and explains:

- what system security and integrity obligations are;
- why system security and integrity obligations are necessary;
- when compliance with system security and integrity obligations is required;
- how to comply with system security and integrity obligations; and
- the consequences of non-compliance.

Capitalised terms have the meanings given to them in the Model Participation Rules, Model Operating Requirements or Electronic Conveyancing National Law.

This guide does not constitute legal advice nor does it replace prudent conveyancing practice. Nothing written in this guide overrides the Electronic Conveyancing National Law, Participation Rules, any other relevant legislation or Registrar's Prescribed Requirements.

2 WHAT ARE SYSTEM SECURITY AND INTEGRITY OBLIGATIONS?

The system security and integrity obligations for Subscribers are specified in Model Participation Rule 7 and include obligations related to:

- Protection measures
- Users
- User access
- Digital Certificates
- Notification of Jeopardised Conveyancing Transactions
- Revoking Authority
- Comprised Security Items
- Certifications

3 WHY ARE SYSTEM SECURITY AND INTEGRITY OBLIGATIONS NECESSARY?

System security and integrity obligations help secure the systems used in electronic conveyancing. It is important to have system security and integrity obligations in place to proactively manage the risk of fraud and misuse, and to provide confidence to Subscribers, landowners and the Registrar. Additionally, some security measures are in place to facilitate the efficient operation of systems.

4 WHEN IS COMPLIANCE WITH SYSTEM SECURITY AND INTEGRITY OBLIGATIONS REQUIRED?

Model Participation Rule 3 requires a Subscriber to comply with the system security and integrity obligations at the time of their application to become a Subscriber and at all times while they remain a Subscriber. Model Participation Rule 3(c) requires Subscribers to continue to comply with Model Participation Rule 7.7 (Notification of Jeopardised Conveyancing Transactions) after ceasing to be a Subscriber.

All activity undertaken within an Electronic Lodgment Network is traceable for security reasons.

5 HOW TO COMPLY WITH THE SYSTEM SECURITY OBLIGATIONS?

5.1 Protection Measures

A Subscriber must take reasonable steps to comply with an Electronic Lodgment Network Operator's (ELNO's) security policy. This includes using and maintaining the technology required to enable the Subscriber to access the Electronic Lodgment Network (ELN), including the installation of virus protection software as specified by the ELNO on the Subscriber's computers. The Subscriber must also take reasonable steps to protect Security Items (including Access Credentials and Digital Certificates), and to comply with the ELNO's security policy with respect to training and monitoring of its Users.

A Subscriber must not do anything that it knows or ought reasonably to know is likely to have an adverse effect on the operation, security, integrity, stability, or the overall efficiency of the ELN.

A Subscriber must not fail to do anything within its reasonable control, the omission of which, it knows or ought reasonably to know is likely to have an adverse effect on the operation, security, integrity, stability, or the overall efficiency of the ELN.

The phrase 'ought reasonably to know' is a common legal concept that refers to what a reasonable person in the position of the Subscriber would have known in the circumstances. One example of an action that would likely breach this obligation would be where the Subscriber allocates a Digital Certificate and signing rights to a person known to have been previously involved in property fraud. One example of an omission that may breach this obligation would be where the Subscriber fails to keep its software up to date as software updates often include important security updates.

5.2 Users

A Subscriber must take reasonable steps to ensure that only Users access the ELN. What is reasonable depends on the circumstances and would be based on what steps an ordinarily prudent Subscriber would have taken in the circumstances and in the ordinary course of their business.

A Subscriber must also take reasonable steps to ensure that each of its Users has received training appropriate to their use of the ELN, including cyber security awareness training covering, as a minimum, secure use of the ELN, secure use of the Subscriber's Systems and secure use of email and other electronic communication. Best practice would be to ensure the User completes the training before the User is given access to the ELN.

A Subscriber must also ensure that each of its other principals, Officers, employees, agents and contractors who access the Subscriber's Systems receive cyber security awareness training covering, as a minimum, secure use of the Subscriber's Systems and secure use of email and other electronic communication.

The purpose of requiring this training is to ensure that Users and others who access Subscriber's Systems and the ELN are aware of and avoid risks that could impact the security of the ELN. If any system has a weakness exploited, it could potentially lead to attacks on other systems, including the ELN.

It is for a Subscriber to determine the frequency of the training in light of any requirements in the Subscriber's Participation Agreement with the ELNO, the ELNO's security policy and the frequently changing landscape of cyber security. Model Operating Requirement 7.1(b)(ii)D and 14.6 require an ELNO to make adequate training resources available to Subscribers and Users in relation to their use of the ELN. An ELNO may require training to be completed at specified times within its Participation Agreement or security policy.

A Subscriber must ensure that prior to the initial allocation of a Digital Certificate to a Signer or prior to the appointment of a Subscriber Administrator, a police background check is conducted for that Signer or Subscriber Administrator. The purpose of the police background check is to ensure that the Signer or Subscriber Administrator is not and has not been subject to a conviction of fraud or an indictable offence which may impact on the conduct of a Conveyancing Transaction by the Signer or Subscriber Administrator or any

offence for dishonesty against any law in connection with business, professional or commercial activities.

This requirement helps to protect the integrity of the Titles Register and provides confidence to Subscribers, landowners and the Registrar.

5.3 User Access

A Subscriber must at all times have at least one Subscriber Administrator, and must keep up to date within the ELN:

- its Users' Access Credentials; and
- signing rights linked to those Access Credentials; and
- administrative rights linked to those Access Credentials.

A Subscriber Administrator has an important role to fulfil and should be chosen carefully.

It is important to keep details up to date. When a Subscriber is selected to undertake the Subscriber Review Process, an ELNO may assess compliance with this requirement, as well as related obligations related to sharing of access credentials and misuse of Digital Certificates.

5.4 Digital Certificates

A Subscriber must obtain at least one Digital Certificate and keep it valid. A Subscriber must ensure that all information provided to any certification authority, registration authority or ELNO for the purpose of obtaining a Digital Certificate, is correct, complete and not false or misleading.

A Subscriber must also take reasonable steps to ensure each of the following:

- only Signers Digitally Sign electronic Registry Instruments or other electronic documents;
- a Digital Certificate is only used to Digitally Sign by the Signer to whom it is allocated;
- Signers do not allow any other Person to use their Access Credentials and Digital Certificates;
- Signers keep the Digital Certificate allocated to them safe and secure in the Signer's control;
- Access Credentials are only used to access the ELN by the User to whom the Access Credentials belong; and
- other Users do not allow any other Person to use their Access Credentials.

Using a Digital Signature belonging to another Person can be likened to a forgery of a signature in paper.

It is important for Subscribers, landowners and Registrars to know who has undertaken what action in an ELN. All activity in an ELN is traceable.

The requirement that a Signer keep a Digital Certificate safe and secure and within the Signer's control does not necessarily mean that it must always be within the Signer's possession. The Signer may wish to use other facilities to ensure the Digital Certificate is stored securely, such as locking it in a safe. When a Subscriber is selected to undertake the Subscriber Review Process, an ELNO may assess compliance with this rule.

Subscribers are reminded that jurisdictional regulators have set rules as to who can sign a Registry Instrument or other electronic Document. Refer to https://www.arnecc.gov.au/__data/assets/pdf_file/0003/1264125/entitlement-to-sign-registry-instruments.pdf

5.5 Notification of Jeopardised Conveyancing Transactions

Where to a Subscriber's knowledge, information, or belief a Conveyancing Transaction has been Jeopardised, the Subscriber must, where it is possible to do so, immediately unsign any electronic Registry Instruments and other electronic Documents relating to the Conveyancing Transaction.

The Subscriber must also immediately notify (to the extent permitted by law) the ELNO and the Registrar of the situation.

The Subscriber must also immediately notify (to the extent permitted by law) the other Participating Subscribers of any information about the Conveyancing Transaction that it believes to be incorrect, omitted, false or misleading or that the Conveyancing Transaction has been Jeopardised. Fulfilment of this obligation is important to protect the integrity of the Titles Register.

Each ELNO and Land Registry provides contact information on their websites.

5.6 Revoking Authority

Where a Subscriber no longer intends for a Person to be a User, Signer, or Subscriber Administrator the Subscriber must promptly revoke their access, signing rights and administrative rights for an ELN or ELNs. The Subscriber must also request the Certification Authority to revoke the Signer's Digital Certificate where it is appropriate to do so.

The Subscriber must immediately withdraw its authorisation to Digitally Sign electronic Registry Instruments and other electronic Documents from any Person who ceases to be the employee, agent or contractor of the Subscriber.

If a Subscriber is restricted in its use of the ELN by the Registrar or the ELNO, the Subscriber must Promptly prevent any of its Users from accessing and using the ELN other than in accordance with the restriction.

Prompt revocation of access and use of the ELN where appropriate is essential to protect the integrity of the Titles Register.

5.7 Compromised Security Items

If a Subscriber becomes aware that any Security Items (meaning User Access Credentials, passphrases, Private Keys, Digital Certificates, Electronic Workspace identifiers and other items as specified from time to time) of any of its Users have been or are likely to be Compromised the Subscriber must:

- immediately revoke the User's authority to access and use the ELN and prevent the User from accessing and using the ELN; and
- for a Digital Certificate:
    (i) 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 Model Participation Rule 7.9.2 and as set out below; and
    (ii) 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
    (iii) Promptly notify the ELNO.

If a Subscriber becomes aware or suspects that any of its Private Keys have been used to Digitally Sign any electronic Registry Instruments and other electronic Documents without its authorisation or the authorisation of any Client on whose behalf the electronic Registry Instruments and other electronic Documents are purported to be Digitally Signed:

- where it is possible to do so, the Subscriber must immediately unsign the electronic Registry Instruments and other electronic Documents; or
- where it is not possible to unsign, the Subscriber must immediately notify the ELNO of the situation. Each ELNO provides contact information on their website.

Fulfilment of this obligation is important to protect the integrity of the Titles Register and assists with remedying any issues Promptly.

5.8 What are "reasonable steps"?

"Reasonable steps" is a commonly used legal concept. When applied to Subscribers in this scenario it means the taking of such steps as an ordinarily prudent Subscriber would have taken in the circumstances and in the ordinary course of their business. What reasonable

steps should be taken will be a question of fact dependant on the circumstances of the individual case.

6 WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

Each ELNO is required to monitor compliance as part of its Subscriber Review Process. Failure to comply with these obligations could lead to the removal of the Subscriber's access to the ELN by the ELNO. Failure to comply with an ELNO's Subscriber Review Process is also a Suspension Event in Schedule 7 of the Model Participation Rules. Non-compliance with Model Participation Rule 7 could also be considered a material breach of the Model Participation Rules or could result in the Subscriber being found to be negligent or posing a threat to the operation, security, integrity or stability of the ELN.

7 FREQUENTLY ASKED QUESTIONS

Q1: What type of police background check is required to satisfy Model Participation Rule 7.2.3(b)?

A1: If the Signer or Subscriber Administrator is located within Australia, it is expected that the Subscriber would request a National Police Check. If the Signer or Subscriber Administrator is not located within Australia, it is expected that the Subscriber will request an International Police Check. If a Signer or Subscriber Administrator has recently arrived within Australia, or has lived internationally for a period of time, a Subscriber may choose to obtain an International Police Check in place of, or in addition to, a National Police Check. It is up to the Subscriber to use their judgement of the most appropriate check dependant on the circumstances.

Q2: Is an upfront police background check always required for Signers or Subscriber Administrators, or can the Subscriber leverage existing processes for onboarding staff?

A2: If staff have already been the subject of a police background check, and that was before the initial allocation of a Digital Certificate to a Signer or prior to the appointment of a Subscriber Administrator, then this Model Participation Rule will have been met.

Q3: If a police background check is undertaken on a Signer or Subscriber Administrator and the result shows a disclosable court outcome, who is responsible for determining if the court outcome affects the Subscriber's ability to comply with Model Participation Rule 7.2.3(b)?

A3: It is the responsibility of the Subscriber to determine that the Signer or Subscriber Administrator has not been subject to the matters as shown in Model Participation Rule 7.2.3(b).

Q4: A police background check is undertaken on a Signer or Subscriber Administrator and the result shows a pending charge which, if convicted, would affect the Subscriber's ability to comply with Model Participation Rule 7.2.3(b). Can they continue to be onboarded as a Signer/Subscriber Administrator and what further steps must the Subscriber take?

A4: A Subscriber should use their judgement to determine whether it is appropriate for a Signer/Subscriber Administrator to continue in that role whilst awaiting the outcome of a pending charge. If convicted, the Subscriber must immediately revoke the Signer's ability to Digitally Sign in the ELN or revoke the Subscriber Administrator's role as Subscriber Administrator. The Subscriber must also revoke the Signer's or Subscriber Administrator's access to the ELN as Users. Notice must also be given in writing to the Registrar and the ELNO.