Subscriber Security Policy

Version 4.0

July 2022

Introduction

This Subscriber Security Policy (**Policy**) outlines security obligations that Sympli requires Subscribers and their Users (**Subscribers**) to meet when using the Sympli System.

This Policy has been developed with consideration of:

- ARNECC Model Operating Requirements (MOR) (v6);
- ARNECC Model Operating Requirements Guidance Notes (v6);
- ARNECC Model Participation Rules (MPR) (v6); and,
- ISO 27001:2015 – Information technology – Security techniques - Information Security Management Systems – Requirements.

1 Scope

Subscribers must comply with this Policy as well as the Participation Rules in their relevant jurisdiction. A current version of the Participation Rules each active jurisdiction is available at: https://www.arnecc.gov.au/regulation/participation_rules_by_jurisdiction.

2 Supported Devices

The Sympli System is only compatible with certain systems that meet minimum system configuration requirements.

Subscribers should ensure that devices used to access the Sympli System meet the following minimum specifications:

- Windows computer (Win 10 or later), or Apple Mac Computer (OSX 10.13 or later);
- Google Chrome (preferred), or Mozilla Firefox;;
- Screen resolution of 1280x1024 or higher; and
- Current operating system and browser patch updates to be applied.

Sympli System does not currently support the use of mobile devices such as tablets and smartphones (Android, Apple or Windows Mobile). It may be possible to use these devices; however, some functions will not be available.

4 Requirements

4.1 Digital Certificate Requirements

Digital Certificates are necessary to complete property transactions using Sympli. Subscribers must comply with the Digital Certificate requirements outlined below.

4.1.1 Digital Certificates must meet the Operating Requirements

Subscribers require at least one Digital Certificate in order to sign documents in Sympli. Subscribers must ensure Digital Certificates provided to their Users meet the Operating Requirements.

This includes ensuring:

a. Digital Certificates used are compliant with the Australian Government's Gatekeeper PKI Framework;[1]
b. Digital Certificates are issued by a Gatekeeper Accredited Service Provider;
c. Each Subscriber obtains at least one Gatekeeper Accredited Management Digital Certificate;
d. An additional certificate for each signing User created within the Subscriber's account; and
e. Digital Certificates used in Sympli identify the relevant Subscriber, its ABN, and names the signing User in the Certificate Profile.

Subscribers must ensure that the information they provide for the purpose of obtaining a Digital Certificate is correct, complete and not false or misleading in any way.

4.1.2 Valid Digital Certificates are current

Subscribers must ensure when documents are signed and submitted using Sympli that:

a. any digitally signed document has been executed using a valid Digital Certificate;
b. the Signer has appropriate rights to sign the document; and
c. that the Signer's signing rights are not expired, restricted, suspended or terminated.

4.1.3 Digital Certificates usage

At Sympli's discretion, subscribers will be allowed to use a software-based Digital Certificate to sign within Sympli. This will be based on appropriate information security measures implemented by the Subscriber, which may include compliance with ISO/IEC 27001.

Otherwise, subscribers must ensure that hardware-based Digital Certificates (for instance a Digital Certificate securely stored on a USB driver) are used to sign within Sympli.

4.1.4 Digital Certificates must be stored securely

Subscribers must ensure that their Digital Certificates are stored securely so that they cannot be accessed by unauthorised parties.

a. Required security precautions include:
    i. Hardware-based digital Certificates must be stored on an encrypted and password protected hardware token; (e.g. an encrypted USB);
    ii. Access to the Digital Certificate (Hardware-based or Software-based) is limited to authorised Users; and
    iii. Hardware- based digital Certificates must be physically stored in a secure location when not required (for instance, in a safe or secure filing cabinet).

4.1.5 Digital Certificates must be protected by strong passwords

Digital Certificates must be protected by a strong password.

[1] https://www.dta.gov.au/what-we-do/policies-and-programs/identity/gatekeeper-public-key-infrastructure-framework/

4.1.6 Subscribers to take immediate action where a Digital Certificate is compromised

Subscribers must take immediate action where the security of a Digital Certificate has been, or reasonably believe it will be, compromised by performing the following steps:

a. suspend the relevant User's access to Sympli;
b. revoke the relevant User's Digital Certificate;
c. any documents which were signed using the compromised Digital Certificate are unsigned immediately in accordance with Participation Rule 7.9.2;
d. Sympli is informed of the situation via their Service Team; and
e. access to Sympli for the relevant User is only re-enabled after the above steps have been taken, and actions have been taken to prevent a similar compromise occurring in the future.

If investigations reveal the possibility that a Subscriber's Management Digital Certificate has been compromised, then the time and date of the compromise are to be established. User Digital Certificates approved by the Management Digital Certificate after the time and date of the incident are to be revoked by contacting the Certification Authority. If the time and date of compromise cannot be established with any certainty, establish the last transaction where the Certificate is known to be uncompromised and review all transactions from that point

4.2 Subscriber Management of IT Security

Subscribers must take appropriate security measures to protect their IT environment, particularly concerning devices used to access Sympli. Appropriate security measures include those outlined below.

4.2.1 Operating Systems must be kept up to date

Subscribers must ensure operating systems and applications, specifically those that are used to access Sympli, are kept up to date with the latest security patches.

Enabling 'auto-updates' for operating systems and software is a recommended way to achieve this.[2]

4.2.2 Security software is to be used

Subscribers must ensure that security software is installed on any device used to access Sympli. A good security software solution should:

a. be enabled by default and configured to automatically download and install updates;
b. detect and remove malicious software (malware); and
c. be able to restrict incoming and outgoing connections to an approved list (sometimes referred to as a firewall).

[2] It is also worth subscribing to the Australian Government's 'Stay Smart Online' alert service to be kept up to date with any information about the latest online threats (see https://www.staysmartonline.gov.au/alert-service).

For further information, Sympli recommends consulting the Australian Government's 'Stay Smart Online' service.[3]

4.2.3 Staff are to be provided with cyber security awareness training

Subscribers must ensure their staff have an appropriate level of cyber security awareness, including knowledge of the following:

a. common cyber security threats and distribution mechanisms (such as malware, ransomware, and malicious emails);
b. secure use of the Sympli ELN, including using multi-factor authentication where required;
c. secure use of email and other communication, including common risks such as phishing;
d. basic 'good security hygiene' practices, such as the use of strong individual passwords which are not shared with others; and
e. the security obligations the Subscriber has in accordance with this Policy.

Sympli will make cyber security training resources available: a. during the onboarding process; b. online, through our website (which may include our blog and/or training portal); and c. via email updates. If Subscribers have any queries about their security obligations under this Policy, they should contact the Sympli helpdesk for more information.

The Australian Government's 'Stay Smart Online' service has some additional information and resources available regarding developing security awareness among staff.[4.]

4.3 Subscriber Account Management

Subscribers must ensure that they securely manage their access to Sympli. Subscribers must comply with the account management requirements outlined below.

4.3.1 Subscribers must ensure Users have secure passwords

Subscribers must use strong passwords for accounts used to access Sympli.

The passwords must meet the following requirements:

a. be at least 10 characters in length;[5]
b. use a combination of upper case characters [e.g. ABCD..], lower case characters [e.g. abcd..], numbers [e.g. 1234..] and special characters [e.g. @, #, $..]
c. are unique (e.g. not used across multiple user or system accounts);
d. do not include dictionary words or any business-related words that are easy to guess, or use something obvious such as a person's name, birth date or similar; and

[3] See https://www.staysmartonline.gov.au/protect-your-business/do-things-safely/anti-virus-software-business. For a comparison of specific solutions, this article may also prove useful https://www.tomsguide.com/us/best-antivirus,review-2588-4.html.
[4] See https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/security-awareness
[5] While traditional advice around passwords has focussed on complexity delivered through the use of a combination of special characters, upper and lower case characters and numbers, contemporary views on password security focus on the length of the password being the single most important factor in minimising the potential for a security breach.

e. are not increments of previously used passwords (e.g. “password1”, “password2”).

4.3.2 Passwords are not to be shared

Subscribers must ensure that passwords used for accessing Sympli are not shared.

4.3.3 Subscribers must not cache authentication data

Subscribers must ensure that systems and applications are configured to prevent caching of authentication data used to access Sympli.

4.3.4 Passwords are changed immediately if there is a possible security compromise

Subscribers must ensure that passwords are changed immediately if there is any evidence that they may have been compromised.

4.3.5 Subscribers to regularly review account privileges for Users

Subscribers must regularly review the account access privileges of Users and, where necessary, revoke or modify account privileges.

4.3.6 Subscribers to monitor usage of Sympli

Subscribers must take reasonable steps to monitor the use of Sympli by its Users, in particular to identify any unusual or suspicious activity.

In instances where such activity is observed, the Subscriber must suspend the relevant User account immediately and must notify Sympli as soon as possible. The Subscriber must undertake further investigations to confirm the reason for this activity prior to revoking or re-enabling the User’s account. The Subscriber must inform Sympli as to the findings of any such investigations via the Service Team.

4.3.7 Multi-factor Authentication

Subscribers may be required to use multi-factor authentication to access the Sympli ELN and to Digitally Sign any Electronic Workspace Documents within the Sympli ELN.

4.4 Handling Security Breaches

A potential security breach could have signification impacts on the integrity of property transactions, Subscribers, and Sympli. The actions of Subscribers following a potential breach are critical, and as such, Subscriber must comply with the following requirements.

4.4.1 Subscribers must notify Sympli of any potential security breaches

Subscribers must notify Sympli as soon as they become aware of any potential security compromise. By way of example, this could include:

a. theft, loss, or unauthorised sharing, or use of access credentials in Sympli;
b. theft, loss, or unauthorised sharing of Certificates for Sympli;
b. situations where there is any indication that a document may have been digitally signed without the authority of the Subscriber

Please note, this obligation is in addition to the requirements of Participation Rules 7.7 and 7.9.

4.4.2 Subscribers must take measures to limit a security breach

Subscribers must take all reasonable and appropriate measures to limit the extent of a security breach. Subscribers must inform Sympli of what measures they have taken in immediate response to the breach as well as further prevention measures.

4.5 Subscriber Behaviour

In using the Sympli system, Subscribers are subject to certain conduct requirements. These are outlined below.

4.5.1 Subscribers to avoid omissions or acts which could detrimentally affect the operation of Sympli

Subscribers must not, through act or omission, do anything that they know (or ought to reasonably know) is likely to have an adverse effect on the operation, security, integrity, stability or the overall efficiency of the Sympli ELN.

4.5.2 Sympli able to suspend or terminate Subscriber accounts

Sympli reserves the right to restrict, suspend, or terminate a Subscriber's access to Sympli, as appropriate.

4.6 Subscriber Management of Users

Subscribers are required to take certain steps under this Policy in relation to the conduct of their Users, as described in this section.

4.6.1 Subscribers must provide this Policy to Users

Subscribers must share a copy of this Policy with their Users prior to providing those Users with access to Sympli.

4.6.2 Subscribers must ensure Users understand and comply with this Policy

Subscribers must take reasonable steps to ensure Users:

a. understand the requirements of this Policy; and
b. comply with these requirements.

4.6.3 Subscribers must ensure Users are provided with training to comply with this Policy

Subscribers must take reasonable steps to ensure their Users are provided with appropriate training to enable them to comply with the requirements of this Policy.

4.6.4 Subscribers must comply with Certification Authority Requirements

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

5 Compliance

Sympli reserves the right to review the steps Subscribers have taken to comply with the requirements of this Policy. Subscribers are expected to co-operate with Sympli to determine compliance, if required.

6 Policy Review

Sympli reserves the right to review this Policy and amend it from time to time as necessary, in accordance with the Participation Agreement.

7 Definitions

Defined terms used in this Policy will have the meaning given to them in the Electronic Conveyancing National Law, the Operating Rules, or the Participation Agreement, as applicable.

Appendix A. Glossary

Terms used in this policy which are already defined in the Electronic National Conveyancing Law (ECNL), or associated documents such as the Participation Rules or Model Operating Requirements are taken to have the same meaning as in those documents. These terms have been capitalised in this document and include:

Term	Definition
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.
Certificate Profile	The specification of the fields to be included in a Digital Certificate and the contents of each.
Digital Certificate	An electronic certificate Digitally Signed by the Certification Authority which: • 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; • binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and • contains the specification of the fields to be included in a Digital Certificate and the contents of each.
ECNL	Electronic Conveyancing National Law as adopted or implemented in a jurisdiction, as amended from time to time.
ELN	Electronic Lodgment Network, a network established to create and electronically lodge registry instruments and other electronic documents with the jurisdiction's Land Registry.
ELNO	A person authorised by a jurisdiction to operate an Electronic Lodgment Network.
Gatekeeper	The Commonwealth government strategy to develop PKI to facilitate government online service delivery and e-procurement
Signer	User authorised by the Subscriber to Digitally Sign Registry Instruments and other electronic Documents on behalf of the Subscriber.
Subscriber	A person who is authorised under a participation agreement to use an ELN to complete conveyancing transactions on behalf of another person or on their own behalf.
User	Individual authorised by a Subscriber to access and use the ELN on behalf of the Subscriber.