SPEAR Common Rules

1. ACCESS

Customers may seek access to SPEAR 24 hours a day for every day of the year. However, the Department does not warrant or represent that access to SPEAR will always be available at all times on all days.

2. AVAILABILITY AND SECURITY

2.1 Security of Communications

Subject to any statutory and any express warranties provided in any other terms, the Department does not warrant the security of any information transmitted to or from the Department or any other person using SPEAR and such transmission is at the Customer's risk.

2.2 Interruptions

As electronic services are subject to interruption or breakdown for a variety of reasons, access to SPEAR is offered on an 'as is, as available' basis only.

2.3 Suspension

The Department may alter, suspend or withdraw the availability of SPEAR at any time for any reasonable cause, with or without notice to Customers or Users.

2.4 Delays in processing

The Department and the Relevant Council have no responsibility for, and accept no liability for, any Loss which results from delays in processing any Communication by SPEAR.

2.5 [Deleted]

2.6 Backup

The Department will regularly, and in accordance with the Department's own internal processes, back-up the data and information stored in SPEAR.

2.7 Disaster Recovery

The Department has developed and implemented a reasonable disaster recovery strategy. The key aim of the disaster recovery strategy is the protection and recovery of the data and information stored in SPEAR.

2.8 Protection Measures

The Customer must:

(a) take reasonable steps to comply with the SPEAR Customer Security Policy and the SPEAR User Security Policy; and

(b) provide a copy of the SPEAR Customer Security Policy to each of its Customer Administrators and each other person in the Customer's organisation with responsibility for the protection and security of the Customer's computer system and Security Items; and

(c) provide a copy of the SPEAR User Security Policy to each of its Users before they become Users; and

(d) take reasonable steps to ensure that all its Users comply with the SPEAR Customer Security Policy and the SPEAR User Security Policy.

2.9 Users

The Customer must:

(a) take reasonable steps to ensure that only Users access SPEAR; and

(b) ensure that each of its Users has received training appropriate to their use of SPEAR; and

(c) take reasonable steps to ensure that its Users comply with these Common Rules.

3. FUNCTIONALITY

3.1 Functionality provided by SPEAR

SPEAR will have such functionality and features as the Department determines to provide from time to time having regard to what is reasonably required to enable Customers to lodge, receive and process (as appropriate) Relevant Applications.

3.2 Statutory Provisions

The Department will use its reasonable endeavours to ensure that SPEAR operates in accordance with the Statutory Provisions applicable to SPEAR. However, the Department provides no warranties with respect to the compliance of SPEAR with any Statutory Provision.

3.3 SPEAR updates

The Department may, from time to time, provide updates or new releases of SPEAR. Nothing in these Common Rules shall be construed so as to prevent or limit the type, nature or impact of any updates or new releases which may be provided by the Department.

4. HOW INFORMATION IS PROVIDED BY SPEAR

All Customers agree that where any document or information is to be provided to or by SPEAR:

(a) such document or information will be provided by way of an electronic message to the relevant Customers, giving notice of the document or information having been received into or made available in SPEAR, and

providing the Customer with the URL to access the document or information; and

(b) they accept the electronic notification of the availability of the document or information as provision of the relevant document or information to them by SPEAR.

5. SPEAR RECORDS

5.1 Audit logs

The Department will maintain logs of transactions communicated using SPEAR.

5.2 Timing

Subject to any legislative requirement to the contrary, all Customers agree that the time recorded in SPEAR is the time of entry of a document or information into the SPEAR system, as identified in the SPEAR transaction log.

5.3 Communication

All Customers warrant upon each and every Communication that the Communication is true and correct and contains all relevant information. All Customers warrant and agree that they are authorised to give each Communication given by them.

5.4 Conclusive Proof

All Customers agree that the records maintained by the Department are and will be conclusive evidence, without any further proof, of all actions and transactions communicated through SPEAR and of all information contained in such actions or transactions.

6. OBLIGATIONS UNDER LEGISLATION

All Customers agree that nothing in the Common Rules or any Agreement is to be construed as changing the duties or functions of any party under the *Planning and Environment Act* 1987 or the *Subdivision Act* 1988 or the *Transfer of Land Act 1958* or any other Statutory Provision.

7. [DELETED]

8. CUSTOMER'S OBLIGATION TO UP-DATE DATA

All Customers agree that where any document or information within SPEAR is required to be amended such amended information or document must be changed within SPEAR as soon as reasonably practicable and consistent with all statutory requirements.

9. ELECTRONIC TRANSACTIONS ACT

All Customers agree that any Communication necessary or appropriate for the processing of Relevant Applications may be undertaken by an electronic communication as defined in the Electronic Transactions Act and they each:

(a) consent to the giving of information by electronic communication as provided for under Section 8 of the Electronic Transactions Act; and

(b) agree and acknowledge that where any signature is required to an electronic communication and the applicable security requirements have been met, the signature is valid for the purposes of Section 9 of the Electronic Transactions Act*;* and

(c) agree and acknowledge that where a document is produced by electronic communication, it is valid for the purposes of Section 10 of the Electronic Transactions Act; and

(d) agree and acknowledge that the information recorded in SPEAR is validly retained for the purposes of Section 11 of the Electronic Transactions Act.

10. NO LIABILITY

10.1 The Department and the Relevant Council make no representation or warranty as to the accuracy or completeness of the information contained in or which may be obtained by the use of SPEAR. The Customer and any person using or relying upon SPEAR or information obtained through SPEAR does so on the basis that the Department and the Relevant Council accept no responsibility or liability whatsoever for any errors, faults, defects or omissions in the information, including the absence of or loss of any data.

10.2 Without limiting the generality of clause 10.1 of these Common Rules, each Customer acknowledges and agrees that where the Customer or its Users uploads an ePlan into the SPEAR environment:

(a) the PDF rendered from the uploaded ePlan (and not the ePlan itself) is the Plan for the purposes of the *Planning and Environment Act* 1987 or the *Subdivision Act* 1988 or the *Transfer of Land Act 1958* or any other Statutory Provision; and

(b) the Customer is solely responsible for ensuring that the PDF rendered from that ePlan is checked for any errors, faults, defects and omissions and the Department, the Registrar and the Relevant Council accept no responsibility or liability whatsoever for any such errors, faults, defects or omissions.

10.3 The Customer indemnifies each of the Department, the Registrar and the Relevant Council (each an Indemnified Party) and holds each Indemnified Party harmless against each Loss (including on account of consequential loss or economic loss) directly or indirectly suffered or incurred by the Indemnified Party as a result of any error, fault, defect or omission in any PDF uploaded by the Customer or rendered from an ePlan uploaded by the Customer.

11. LIABILITY EXCLUDED FOR USE OF SPEAR

The liability of the Department and the Relevant Council for:

(a) any failures or delays in availability or functioning of SPEAR due to failure of any communication network (including any internet service provider) or hardware or software used by the Department; or

(b) any breakdown or interruption to any computer system; or

(c) any error, corruption or loss of data which may be caused directly or indirectly through the use of SPEAR,

is limited to the maximum extent permitted by law.

12. LICENCE FOR THE DEPARTMENT TO USE INFORMATION

12.1 All Customers and Users grant to the Department an irrevocable, perpetual, royalty free licence (including the right to sub-licence) to use, copy, provide and publicly display:

(a) all documents submitted with SPEAR for the purpose of the operation of SPEAR or for any other purpose relating to Relevant Applications; and

(b) all information and data provided to SPEAR, including survey data, Plans and field notes and Personal Information,

for the purposes of the operation of SPEAR and for all Authorised Purposes.

12.2 All Customers agree that any documents, information or data submitted by the Customer or its Users, generated by or provided to SPEAR may be accessed and used by other persons who have access to SPEAR for the purposes of a Relevant Application. In particular and without limitation:

(a) any member of the public or third party may access and search the SPEAR system and may obtain documents, information or data relating to a Relevant Application that is publicly available or which has been made available to a Responsible Authority; and

(b) the Responsible Authority may access the SPEAR system and obtain any document, information or data relating to a Relevant Application at any time; and

(c) a Referral Authority may access the SPEAR system and obtain any document, information or data relating to a Relevant Application if the Relevant Application has been referred to the Referral Authority under the Planning and Environment Act 1987; and

(d) other Customers or Users of SPEAR may access the SPEAR system and obtain any document, information or data relating to a Relevant Application where the other Customer or User requires that document, information or data for the purpose of complying with any law or order; and

(e) any Guest may access the SPEAR system if invited by the Customer or its Users and may obtain any documents, information or data relating to a Relevant Application which the Guest has been invited to access.

12.3 All Customers acknowledge that any person who has access to the SPEAR system and who obtains any documents, information or data relating to a Relevant Application may, without limitation:

(a) make any information, document or data contained within SPEAR available to any other person whether or not that other person is a Customer, User, Guest or third party; and

(b) send any information, document or data contained within SPEAR to any other person by electronic transmission or by any other means whether that other person is a Customer, User, Guest or third party; and

(c) reproduce any information, document or data or any part of the information, document or data contained within SPEAR.

12.4 All Customers acknowledge that the documents, information or data referred to in this clause includes documents submitted by the Customer, its Users or Guests and any other Customer or User or Guest and includes information contained within any PDF, attachment, Register Search Statement, survey data and field notes and includes documents created within or generated by SPEAR and any information or data entered into SPEAR by the Customer and any other Customer or User or Guest.

13. PERSONAL INFORMATION

Where a Customer or its Users or Guests supply information or documents to SPEAR and these include Personal Information, such information must only be supplied with the consent of the person to whom the information relates and the Customer (or other person supplying the information) warrants that such consent has been obtained.

14. SPEAR INTELLECTUAL PROPERTY

All Customers agree that where SPEAR creates documents or compiles information (whether in electronic or any other form) by drawing information from Relevant Applications or other information provided to the SPEAR system, the Intellectual Property Rights in that document or compilation of the information is owned by the Department.

15. [DELETED]

16. OBJECTIONS

16.1 Objections to Relevant Applications may be made available in SPEAR by the Relevant Council but, under s. 57(5) of the *Planning and Environment Act*, Customers must rely upon the records of the Relevant Council for details of any objections and the SPEAR record must not be relied on for this purpose.

16.2 The Customer warrants to the Department and to any relevant Responsible Authority each and every time that the Customer lodges an Objection in SPEAR that the Customer is authorised by the persons named in the Objection to make and lodge the Objection.

17. DATA USE

Customers may use the documents and all information in SPEAR for Relevant Purposes but not for any other purpose. Customers acknowledge and agree that the documents and all information which they provide to SPEAR may be used for the Authorised Purposes and as set out in clause 12 of these Common Rules.

18. DIGITAL SIGNATURES

18.1 Subject to this clause 18, a Customer or its Users may satisfy a Signing Requirement in connection with the use of SPEAR by using a Digital Certificate to create a Digital Signature for the relevant Communication or Relevant Application, in accordance with the requirements of the Department.

18.2 Each Customer must promptly disclose to the Department the public key and distinguished name of each Digital Certificate issued to the Customer or its Users which is intended to be used to satisfy a Signing Requirement in connection with the use of SPEAR.

18.3 The Customer must take reasonable steps to ensure that only Signers Digitally Sign relevant Communications or Relevant Applications.

18.4 The Department must ensure that SPEAR does not permit a relevant Communication or Relevant Application to be Digitally Signed unless SPEAR has ensured that the Digital Certificate used for the attempted Digital Signing is valid, has been verified and has not been revoked by the Certification Authority for that Digital Certificate.

18.5 The Department must ensure that SPEAR, before permitting a relevant Communication or a Relevant Application to be Digitally Signed by a Customer or its Users with a Digital Certificate, checks that the Access Credentials for the Key Holder of the Digital Certificate have linked to them rights in SPEAR necessary to perform the Digital Signing at the time it is sought to be done.

18.6 A Digital Signature on a relevant Communication or a Relevant Application is final once the relevant Communication or Relevant Application is Digitally Signed.

18.7 The Customer must ensure that all information provided to any Certification Authority, or to any Registration Authority, is correct, complete and not false or misleading.

18.8 Each Customer warrants in favour of the Department, the Registrar and other Customers that:

(1) each person issued with a Digital Certificate has the authority to legally bind the Customer through the use of the Digital Certificate; and

(2) in respect of any Licensed Surveyor Signing Requirement that is satisfied by using a Digital Certificate, the person who used the Digital Certificate to satisfy that requirement:

(a) is a Licensed Surveyor; and

(b) is the person to whom that Digital Certificate is issued.

18.9 Each Customer indemnifies the Department and the Registrar from and against all Losses incurred by the Department arising out of or otherwise in connection with:

(1) any breach of any of the warranties given in clause 18.8;

(2) any breach of these Common Rules, and any Agreement by the Customer or its Users;

(3) any person using a Digital Certificate of the Customer to satisfy a Licensed Surveyor Signing Requirement where:

(a) the person is not a Licensed Surveyor; or

(b) the Digital Certificate is not issued to that person.

18.10 Each User must not use a Digital Certificate to satisfy a Signing Requirement in connection with the use of SPEAR unless:

(1) the Digital Certificate is a Digital Certificate that is issued to the User; and

(2) the User is authorised to use the Digital Certificate to satisfy that Signing Requirement.

18.11 Reliance on, and repudiation of, Digital Signatures is as follows:

(1) If a Customer's Digital Signature is created for a relevant Communication or Relevant Application then:

(a) unless that Customer repudiates that Digital Signature, that relevant Communication or Relevant Application is to be taken to be signed by that Customer, and

(b) unless that Customer repudiates that Digital Signature, that Digital Signature is binding, in relation to that relevant Communication or Relevant Application, on:

(i) that Customer, and

(ii) all other persons including a Client (if any) for whom that Customer acts with respect to that relevant Communication or Relevant Application, and

(c) unless that Customer repudiates that Digital Signature, that Digital Signature is binding, in relation to that relevant Communication or Relevant Application, for the benefit of:

(i) each of the parties to that relevant Communication or Relevant Application, and

(ii) each Customer, including but not limited to a Responsible Authority or a Relevant Applicant, who acts with respect to that relevant Communication or Relevant Application, and

(iii) any person claiming through or under any person to whom subparagraph (i) applies, and

(iv) the Registrar, once that relevant Communication or Relevant Application is lodged with him or her, and

(v) the Department.

(d) that Customer cannot repudiate that Digital Signature except in the circumstances set out in 18.11(3).

(2) 18.11(1) applies regardless of:

(a) who created the Customer's Digital Signature, and

(b) the circumstances (including fraud) in which the Customer's Digital Signature was created.

(3) Despite 18.11(1) and 18.11(2), a Customer can repudiate the Customer's Digital Signature with respect to a relevant Communication or Relevant Application if the Customer establishes:

(a) that the Digital Signature was not created by the Customer, and

(b) that the Digital Signature was not created by a person who, at the time the Customer's Digital Signature was created for the relevant Communication or Relevant Application:

(i) was an employee, agent, contractor or officer (however described) of the Customer, and

(ii) had the Customer's express or implied authority to create the Customer's Digital Signature for any document or documents, and

(c) that neither of the following enabled the Customer's Digital Signature to be created for the relevant Communication or Relevant Application:

(i) a failure by the Customer, or any of the Customer's employees, agents, contractors or officers, to fully comply with the requirements of the Department; or

(ii) a failure by the Customer, or any of the Customer's employees, agents, contractors or officers, to take reasonable care.

(4) For the purposes of 18.11(3)(b)(ii), it does not matter whether the authority was:

(a) general, or

(b) limited or restricted to documents of a particular class or to a particular document or in any other way.

19. DEFINITIONS

In these Common Rules the following definitions apply:

Access Credentials means a User's identification and password, and any other details, required for a person to access SPEAR.

Agreement means any agreement between the Customer and the Department relating to the use of SPEAR.

Authorised Purpose means the recording and the processing of Relevant Applications and for all documentation and associated purposes (including recording for public access) and includes use in records of Responsible Authorities or Referral Authorities, the Registrar, Crown land records and the digital map base as used and distributed by or on behalf of the State.

Certification Authority means 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.

Client means a person or persons who have appointed a Customer to act on their behalf.

Common Rules means these terms and conditions as set out on the SPEAR web site as amended from time to time which bind Customers of SPEAR.

Communication includes any instruction, request, approval, certification, acceptance, confirmation, information, or document.

Council means a Council as defined in the Local Government Act 1989.

Customer means any person or body who enters into an Agreement with the Department.

Customer Administrator means a person appointed by a Customer to act as an administrator in SPEAR on the Customer's behalf and includes an Administrator as defined in any Agreement.

Department means the Department of Environment, Land, Water and Planning of the State (and its successor under any machinery of Government changes as may be implemented) and any reference to the Department shall be read and construed as a reference to the State.

Digital Certificate means 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) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and

(c) contains the specification of the fields to be included in a Digital Certificate and the contents of each; and

(d) meets the requirements of the Department or the Registrar as specified in writing from time to time.

Digital Signature has the meaning given to it in the Electronic Conveyancing National Law (Victoria).

Electronic Transactions Act means the *Electronic Transactions Act (Victoria*) *2000* (Victoria).

ePlan means an XML (Extensible Mark-Up Language) Plan.

Gatekeeper means the Commonwealth Government strategy to develop Public Key Infrastructure to facilitate Government online service delivery and e-procurement.

Guest means any person authorised by a Customer or its Users to access and use SPEAR for the purposes relating to Relevant Applications.

Intellectual Property Rights means any patents, trademarks or service marks, rights in designs, trade or business names, copyrights, domain names and data base rights (whether or not any of these are registered and including applications for registration of any such thing) and all rights or forms of protection of a similar nature having equivalent or similar effect to any of these in any part of the world.

Key means a string of characters used with a cryptographic algorithm to encrypt and decrypt.

Key Holder means an individual who holds and uses Keys and Digital Certificates on behalf of a Customer, or in his/her own right in the case of a Key Holder who is also a Customer.

Key Pair means 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).

Licensed Surveyor has the same meaning as that provided in the *Surveying Act 2004* (Vic).

Licensed Surveyor Signing Requirement means a Signing Requirement that must be satisfied by a Licensed Surveyor.

Loss means any loss, damage, cost, interest, expense, fee, penalty, fine, forfeiture, assessment, demand, action, suit, claim, proceeding, cause of action, liability or damages incurred by a person and includes:

(1) the cost of any action taken by any person to protect itself from any loss or to preserve any right it has under any Agreement; and

(2) any taxes or duties payable by the person in connection with any Agreement (excluding any tax on assessable income); and

(3) where applicable, all costs actually paid by the person to their own legal representative (whether or not under a costs agreement) and other expenses

incurred by the person in connection with a demand, action, arbitration or other proceeding (including mediation, compromise, out of court settlement or appeal).

Objection means a document to object to an application for a planning permit under section 56 or to object to the grant of a permit under section 57 of the *Planning and Environment Act* 1987 (Vic).

Participating Customer means each Customer involved in a Relevant Application.

PDF means a portable document format file.

Personal Information has the same meaning as that provided in Section 3 of the *Information Privacy Act* 2000 (Vic).

Plan has the same meaning as that provided in section 3 of the *Surveying Act 2004* (Vic).

Private Key means the Key in an asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation.

Public Key means the Key in an asymmetric Key Pair which may be made public.

Public Key Infrastructure (PKI) means Gatekeeper compliant technology, policies and procedures based on public key cryptography used to create, validate, manage, store, distribute and revoke Digital Certificates.

Registrar has the same meaning as that provided in section 4 of the *Transfer of Land Act 1958* (Vic).

Relevant Applicant means the person making the Relevant Application submitted in SPEAR.

Relevant Application means an application to a Responsible Authority or other authorised body and relating to:

(1) a Plan;

(2) approval of the development and use of any land under the *Planning and Environment Act* 1987 (Vic);

(3) the issue of permits under the *Building Act 1993* (Vic);

and includes all activities and documentation associated with such applications.

Relevant Council means the Council (or other statutory appointee or body) which is the Responsible Authority with respect to the Relevant Application.

Relevant Purpose means the purpose of making a Relevant Application, or updating and viewing a Relevant Application or objecting to a Relevant Application and includes use for all associated activities and documentation.

Responsible Authority has the same meaning as it does in the Planning and Environment Act 1987 (Vic).

Security Item means Access Credentials, passphrases, Private Keys, Digital Certificates and other items as specified from time to time.

Signer means the Customer or a Customer's User who is authorised by the Customer to Digitally Sign electronic documents.

Signing Requirement, in relation to a person or class of persons, means any requirement, whether contained in a contract or in any applicable statute, rule, regulation, proclamation, order in council, ordinance or by-law, for any Communication or Relevant Application to be signed, endorsed, certified, issued or authorised by, that person or class of persons.

SPEAR means the computerised system for providing Surveying and Planning through Electronic Applications and Referrals developed by the Department as modified from time to time.

SPEAR Customer Security Policy means the policy set out in Schedule 1, as amended from time to time.

SPEAR User Security Policy means the policy set out in Schedule 2, as amended from time to time.

State means the Crown in right of the State of Victoria.

Statutory Provision means a statute, regulation or provision of a statute or regulation.

User means any person authorised to access and use SPEAR.

Schedule 1 – SPEAR Customer Security Policy

(Version 1 – 15/06/2015)

ABOUT THIS POLICY

This document has been prepared to assist Customers to better understand their obligations to ensure the integrity of SPEAR.

All Customers and their Users must comply with this policy at all times.

Definitions

Access Credentials means a User's identification and password, and any other details, required for a person to access SPEAR.

Agreement means any agreement between the Customer and the Department relating to the use of SPEAR.

Certification Authority means 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.

Client means a person or persons who have appointed a Customer to act on their behalf.

Common Rules means these terms and conditions as set out on the SPEAR web site as amended from time to time which bind Customers of SPEAR.

Communication includes any instruction, request, approval, certification, acceptance, confirmation, information, or document.

Compromised means lost or stolen, or reproduced, modified, disclosed or used without proper authority.

Customer means any person or body who enters into an Agreement with the Department.

Customer Administrator means a person appointed by a Customer to act as an administrator in SPEAR on the Customer's behalf and includes an Administrator as defined in any Agreement.

Department means the Department of Environment, Land, Water and Planning of the State (and its successor under any machinery of Government changes as may be implemented) and any reference to the Department shall be read and construed as a reference to the State.

Digital Certificate means 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) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and

(c) contains the specification of the fields to be included in a Digital Certificate and the contents of each; and

(d) meets the requirements of the Department or the Registrar as specified in writing from time to time.

Digital Signature has the meaning given to it in the Electronic Conveyancing National Law (Victoria).

Gatekeeper means the Commonwealth Government strategy to develop Public Key Infrastructure to facilitate Government online service delivery and e-procurement.

Jeopardised means put at risk the integrity of a Relevant Application by fraud or other means.

Key means a string of characters used with a cryptographic algorithm to encrypt and decrypt.

Key Holder means an individual who holds and uses Keys and Digital Certificates on behalf of a Customer, or in his/her own right in the case of a Key Holder who is also a Customer.

Key Pair means 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).

Participating Customer means each Customer involved in a Relevant Application.

Plan has the same meaning as that provided in section 3 of the *Surveying Act 2004* (Vic).

Private Key means the Key in an asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation.

Public Key means the Key in an asymmetric Key Pair which may be made public.

Public Key Infrastructure (PKI) means Gatekeeper compliant technology, policies and procedures based on public key cryptography used to create, validate, manage, store, distribute and revoke Digital Certificates.

Registrar has the same meaning as that provided in section 4 of the *Transfer of Land Act 1958* (Vic).

Relevant Application means an application to a Responsible Authority or other authorised body and relating to:

(1) a Plan;

(2) approval of the development and use of any land under the *Planning and Environment Act* 1987 (Vic);

(3) the issue of permits under the *Building Act 1993* (Vic);

and includes all activities and documentation associated with such applications.

Security Item means Access Credentials, passphrases, Private Keys, Digital Certificates and other items as specified from time to time.

Signer means the Customer or a Customer's User who is authorised by the Customer to Digitally Sign electronic documents.

SPEAR means the computerised system for providing Surveying and Planning through Electronic Applications and Referrals developed by the Department as modified from time to time.

SPEAR Customer Security Policy means this policy as set out in Schedule 1 of the Common Rules, as amended from time to time.

SPEAR User Security Policy means the policy set out in Schedule 2 of the Common Rules, as amended from time to time.

State means the Crown in right of the State of Victoria.

User means any person authorised to access and use SPEAR.

1. Training

Each Customer must ensure that its Users are adequately trained to participate in SPEAR and are aware of their obligations to protect User Security Items.

Each Customer must:

(a) provide a copy of the SPEAR User Security Policy to each of its Users before they become Users; and

(b) take reasonable steps to ensure that it and all its Users comply with the SPEAR User Security Policy; and

(c) take reasonable steps to ensure that it and all its Users comply with the Common Rules and the terms of any Agreement, policies and practice statements of the Certification Authority relating to the allocation, use and protection of its Digital Certificates which are applicable to them.

2. General protection measures

Each Customer's User details are part of SPEAR. Therefore, SPEAR's integrity is, in part, reliant on the integrity of each Customer's User details and the systems and facilities used to access SPEAR for the Customer.

Each Customer must take reasonable steps to:

(a) ensure that data supplied to SPEAR is free from viruses, corruption and any other condition that may compromise SPEAR or any data stored by, or, passing into or out of, SPEAR; and

(b) prevent, trap, detect and remove any viruses, corruption and any other condition from its systems and data that may damage SPEAR or any data stored by SPEAR; and

(c) establish and maintain appropriate measures to safeguard SPEAR from unauthorised access; and

(d) monitor, and take appropriate action after receiving security alerts from the Department; and

(e) 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 SPEAR; and

(f) 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 or stability of the overall efficiency of SPEAR; and

(g) ensure that its Users access SPEAR only by using computers over which the Customer has sufficient control to ensure compliance with the Common Rules and the terms of any Agreement; and

(h) ensure that it implements reasonable measures to monitor use of SPEAR and Security Items, including to ensure the Customer becomes aware if any of its Security Items have been lost or stolen or reproduced, modified, disclosed or used without proper authority; and

(i) ensure that it adequately protects its computers and other facilities used to access and store its Digital Certificates from unauthorised use or access; and

(j) ensure that it mitigates any loss arising in connection with the theft, loss, unauthorised disclosure or improper use of any of its Security Items.

Each Customer must notify the Department if it becomes aware of anything that is likely to have an adverse effect on the operation, security, integrity or stability of SPEAR.

3. Specific protection measures

The following are specific protection measures that each Customer is required to take. However, these obligations do not limit the obligations set out in clause 2 of this SPEAR Customer Security Policy .

Each Customer must take reasonable steps to ensure that:

(a) any computer used by its Users to access SPEAR does not have caching enabled that would remove the need for the Users to enter passwords or passphrases in accordance with the normal operation of SPEAR; and

(b) all computers used to access SPEAR are protected at all times by up-to-date security software that provides protection from viruses, spyware, key-logging and other security threats.

4. Protection of Access Credentials

Access Credentials allow a User to access SPEAR for the Customer. A failure to properly protect Access Credentials may result in unauthorised access to SPEAR.

Each Customer must take reasonable steps to ensure that:

(a) none of its Users' Access Credentials are easily associated with its User or the Customer (such as a birthday or telephone number); and

(b) each of its Users' Access Credentials are different from any other existing or former User's past or current Access Credentials; and

(c) its Users' Access Credentials are changed at least every 180 days; and

(d) only the User to whom a particular password or passphrase is allocated uses the password or passphrase and that the User does not share them with any other person; and

(e) each of their Users protects its Access Credentials, including by not permitting any other person to see the entry of their Access Credentials into any computer.

5. Digital Certificates

A Customer's Digital Certificate enable the Customer's Signers to Digitally Sign relevant Communications and Relevant Applications on behalf of the Customer. A failure to properly protect Digital Certificates may result in documents and Communications being signed without authority.

Each Customer must take reasonable steps to protect its Digital Certificates. The obligations of Users in relation to Digital Certificates are contained in the SPEAR User Security Policy. Customers must take reasonable steps to ensure that all of their Users comply with the policy.

6. Form of Digital Certificates

Customers must ensure that they and their Users use Digital Certificates only in that form specified in writing by the Department from time to time.

7. Settings of Digital Certificates

Customers must ensure that their:

(a) Digital Certificates are issued in accordance with Gatekeeper rules; and

(b) Digital Certificates are stored on a hard token unless the Department has permitted otherwise; and

(c) not backed up unless the Department has permitted otherwise.

8. Jeopardised relevant Communications or Relevant Applications

Where to the Customer's knowledge, information or belief a relevant Communication or Relevant Application has been Jeopardised:

(a) where it is possible to do so, the Customer must immediately create and Digitally Sign a new version of the relevant Communication or Relevant Application; or

(b) where it is not possible to create and Digitally Sign a new version of the relevant Communication or Relevant Application, the Customer must immediately notify the Department of the situation.

(c) the Customer must bring to the attention of the other Participating Customers any information about the relevant Communication or Relevant Application that it believes to be incorrect, incomplete, false or misleading or that the relevant Communication or Relevant Application has been Jeopardised.

9. Compromised Security Items

If a Customer becomes aware that any of the Security Items of any of its Users has been or is likely to be Compromised, the Customer must:

(a) immediately revoke the User's authority to access and use SPEAR and prevent the User from accessing and using SPEAR; and

(b) for a Digital Certificate:

(i) immediately check SPEAR for any relevant Communications or Relevant Applications which have been Digitally Signed using the User's Private Key and comply with clause 8 of this SPEAR Customer Security Policy; 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 Department.

10. Compromised Signatures

If a Customer becomes aware or suspects that any of its or its Users' Private Keys have been used to Digitally Sign any relevant Communication or Relevant Application without its authorisation or the authorisation of any Client on whose behalf the relevant Communication or Relevant Application is purported to be Digitally Signed:

(a) where it is possible to do so, the Customer must immediately create and Digitally Sign a new version of the relevant Communication or Relevant Application; or

(b) where it is not possible to create and Digitally Sign a new version of the relevant Communication or Relevant Application, the Customer must immediately notify the Department of the situation.

11. Revoking authority

If a Customer no longer intends:

(a) a person to be its User, the Customer must promptly revoke the User's access to and use of SPEAR; or

(b) a person to be a Signer, the Customer must promptly revoke the User's signing rights within SPEAR and, where appropriate, request the Certification Authority to revoke the Signer's Digital Certificate; or

(c) a person to be Customer Administrator, the Customer must promptly request the Department to revoke the User's administrative rights within SPEAR.

When any Signer ceases to be the employee, agent or contractor of the Customer, the Customer must immediately revoke a User's signing rights within SPEAR and, where appropriate, request the Certification Authority to revoke the Signer's Digital Certificate.

.

Schedule 2 – SPEAR User Security Policy

(Version 1 – 15/06/2015)

ABOUT THIS POLICY

This document has been prepared to assist Users to better understand their obligations to ensure the integrity of SPEAR.

All Users must comply with this policy at all times.

Passwords and passphrases

Users must ensure that:

(a) they do not use any facility that enables caching of their SPEAR passwords or Digital Certificate passphrases; and

(b) their passwords and passphrases are not easily associated with them (such as a birth date or telephone number); and

(c) their passwords and passphrases are changed at least every 180 days; and

(d) they do not share their passwords or passphrases with anyone else; and

(e) they do not permit any other person to use their passwords or passphrases; and

(f) they do not permit any other person to see the entry of their passwords and passphrases into any computer; and

(g) their passwords are different from their passphrases.

Protecting Digital Certificates

Users must ensure that:

(a) their Digital Certificate is set to a security level of 'high', which requires entry of a password; and

(b) where the Department has permitted a backup of their Digital Certificate to be made, the backup is protected by a password and stored in a secure location.

Users must ensure that any hard token used to store their Digital Certificate is:

(a) connected to a computer only when the User is using the computer to Digitally Sign in SPEAR; and

(b) stored in a secure location when not in use.

Compromised Digital Certificates

Users must notify a Customer Administrator immediately if they know or suspect that their Digital Certificate has or may have been lost or stolen, or reproduced, modified, disclosed or used without proper authority.

Ask if in doubt

Contact a Customer Administrator if you are uncertain about your obligations under, or terminology used in, this SPEAR User Security Policy.