

|  |
| --- |
| Client incident management system (CIMS)New user - eBusiness registration guideAugust 2020 |
|  |

|  |
| --- |
| Department of Health |

|  |
| --- |
|  |
| To receive this publication in an accessible format phone 1300 650 172, using the National Relay Service 13 36 77 if required, or email CIMS@dhhs.vic.gov.auAuthorised and published by the Victorian Government, 1 Treasury Place, Melbourne.© State of Victoria, Department of Health and Human Services August 2020.Available at [CIMS page](http://providers.dhhs.vic.gov.au/cims) on the Service Providers website: <http://providers.dhhs.vic.gov.au/cims> |
|  |

# Contents

[Contents 3](#_Toc46911924)

[Background 4](#_Toc46911925)

[Purpose 4](#_Toc46911926)

[Security and privacy 4](#_Toc46911927)

[Registration overview 4](#_Toc46911928)

[What is eBusiness? 4](#_Toc46911929)

[Registration - Step by step instructions 5](#_Toc46911930)

[Step 1 - Staff registration for eBusiness and the application 5](#_Toc46911931)

[Step 2 - Organisation Authority approves eBusiness request 12](#_Toc46911932)

[Step 3 – DHHS provides access to the application. 12](#_Toc46911933)

[Step 4 - Confirmation email sent to staff 13](#_Toc46911934)

[Step 5 - Access the eBusiness portal and the application 13](#_Toc46911935)

[Roles and responsibilities 14](#_Toc46911936)

[Organisation Authority 14](#_Toc46911937)

[Application Authority 14](#_Toc46911938)

[Troubleshooting 14](#_Toc46911939)

[Support and contacts 15](#_Toc46911940)

[Appendices 15](#_Toc46911941)

[Appendix 1 – Change of Organisation Authority Form 15](#_Toc46911942)

[Appendix 2 – Organisation Authority Form 16](#_Toc46911943)

[Appendix 3 – eBusiness Access Agreement 16](#_Toc46911944)

# Background

The Client Incident Management System (CIMS) is a web-based application developed by the Department of Health and Human Services (the department) which automates the process of receiving CIMS data (client incident reports) from in-scope service providers.

## Purpose

The purpose of this document is to provide staff who are to be provisioned with specific CIMS user roles, instructions on how to register for an eBusiness account in order to access the CIMS.

## Security and privacy

The CIMS contains sensitive client information; therefore it has a high level of security and user management protocols.

The department has an authentication process called eBusiness which provides staff a mechanism to access the department’s computer systems via the internet on the basis that only registered and authorised persons do so.

Staff are required to provide mandatory details including given name, family name and date of birth to register for an eBusiness account to access the CIMS portal. Staff will be provided with an individual username and password to login to eBusiness.

# Registration overview

Access to CIMS for staff who are to be provisioned with a specific CIMS user role is via the department’s eBusiness portal.

In order to use the eBusiness portal, organisations and their relevant staff must register for an eBusiness account.

Registration to eBusiness is required so that organisations can verify staff identity and their requirement to access the CIMS within their organisation.

All staff requiring access are required to:

* + - register for a **firstname.surname** eBusiness account\*
		- request access to the CIMS application via their eBusiness account.

\*Staff can omit this step if they have an existing **firstname.surname** eBusiness account registered with their current organisation. If staff have an existing eBusiness account under a different organisation, please contact eBusiness Support on 1300 799 470 or via ebiz@dhhs.vic.gov.au to have the account deactivated before registering under the current organisation.

## What is eBusiness?

eBusiness is an online portal, which allows registered and authorised staff access to the department’s computer systems via the internet.

To ensure the security of personal information captured within the CIMS, the application can only be accessed via the eBusiness portal. Staff must register with the eBusiness portal, and log into the application through that portal with an individual username and password.

All organisations have an **Organisation Authority** (OA) to help with eBusiness registrations. The OA in each organisation is responsible for verifying staff identity and authorising them to use the eBusiness environment and the application. (Refer to the Roles and Responsibilities chapter of this document - Pg 14 - for further definition).

The department’s **CIMS Application Authority** grants access to the CIMS application when the staff member’s OA has approved their access in eBusiness. An email is sent to the staff member from eBusiness confirming access has been granted and an eBusiness username and password is provided.

# Registration - Step by step instructions

## Step 1 - Staff registration for eBusiness and the application

Follow [Part A](#_Part_A_–_1) if:

* you do **not** have an existing eBusiness account
	+ you have an eBusiness account with a username in the following format **emur.o15159** (for those using CRISSP)

Follow [Part B](#_Part_B_–) if:

* you have a **firstname.surname** eBusiness account for the organisation you wish to access CIMS with.

Follow [Part C](#_Part_C_-) if:

* you have a **firstname.surname** eBusiness account for a different organisation from which you wish to access CIMS from (ie: Staff who have left their previous organisation and are working for a new organisation; or staff who work for more than one organisation and need to register an eBusiness account for each organisation).

### Part A – Staff who don’t have an eBusiness account (or an account in the format firstname.surname)

1. Go to the [Department of Health and Human Services eBusiness portal](https://hns.dhs.vic.gov.au/dhsportal/wps/myportal): <https://hns.dhs.vic.gov.au/dhsportal/wps/myportal>
2. The eBusiness login screen will appear. Click on the link, ‘I want to register’ on the right-hand side of screen.

Figure 1: image of the eBusiness login screen



The eBusiness Portal application access Request page will open.

This will allow you to register for an eBusiness account and request access to the CIMS portal.

1. In the *Application catalogue* box click on ‘CIMS Production (1.0.0.0)’ from the list and then click on the ‘Select’ button to move the application into the *Selected application* box.

**Figure 2: image of the eBusiness request for registration screen – Application catalogue**



1. When ‘CIMS Production (1.0.0.0)’ is listed in the *Selected application* box, click on the ‘Next’ button.

Figure 3: image of the eBusiness request for registration screen - Selected applications



1. Add your details. Complete all the fields with a red asterisk (at a minimum).

A work email address must be used when registering (do not use a personal email address such as a gmail or hotmail account).

Figure 4: image of the eBusiness request for registration screen – Personal registration details



1. Find your Organisation Name.

Enter all or part of your organisation’s name and click the ‘Search’ button to display matching organisations in the list.

Click on your organisation and press the ‘+select’ button. (If your organisation name appears multiple times you must select the agency with the correct regional location. Do not simply select the agency without a region).

**Figure 5: image of the eBusiness request for registration – Organisational details**

XXXXXXXXXX

7. Select from the drop down list your role in organisation.

**Figure 6: image of the eBusiness request for registration – Role in organisation**



8. Complete all the identity details fields (marked with a red asterisk).

9. Review the *Conditions of Use*, and if you agree, click the ‘Agree’ button. Click on the ‘Register’ button. Your request for the application access is now finished.

Figure 7: image of the eBusiness request for registration screen– Security details



10. Go to [Step 2](#_Step_2_-) on page 12 (Organisational Authority approves eBusiness request).

### Part B – Staff who have an eBusiness account

If you are already using eBusiness for another application within your organisation, such as the Victorian Housing Register Application, and want to request access to the CIMS application under:

the same organisation name, follow the steps below.

a different organisation name or branch/program area within your organisation, go to [Part C](#_Part_C_-).

1. Go to the [Department of Health and Human Services eBusiness portal](https://hns.dhs.vic.gov.au/dhsportal/wps/myportal): <https://hns.dhs.vic.gov.au/dhsportal/wps/myportal>
2. Login to your eBusiness account. Enter your username, password and review the *Conditions of Use* and *Monitoring of Computer Services*. If you agree with the terms, click on the box to display a tick and then click on the ‘Login’ button.

Figure 8: image of the departmental eBusiness login screen



1. Click on the *Additional application* access tab at top of the page.

**Figure 9: image of the eBusiness home screen**



1. Select ‘CIMS Production (1.0.0.0)’ from the *Application catalogue* box and then click on the ‘Apply’ button. Your request for the CIMS application access is now finished.

**Figure 10: image of the eBusiness request additional application access**



Go to [Step 2](#_Step_2_-) on page 12 (Organisational Authority approves eBusiness request).

### Part C - Staff who work for different organisations

##### Scenario 1 – Staff who have left their previous organisation and now work for another organisation.

If a staff member leaves an organisation, and wishes to register for an application from another organisation, they must cancel their previous registration by contacting eBusiness Support on 1300 799 470 or ebiz@dhhs.vic.gov.au. and advise of change of employer. Once cancelled, the new eBusiness registration can then be applied for and processed.

**Scenario 2 – Staff who work for multiple organisations.**

##### Staff who work for more than one organisation will need to register an eBusiness account for each organisation.

1. **If you already have an eBusiness account, follow the steps below to create additional accounts:**Go to the [Department of Health and Human Services eBusiness portal](https://hns.dhs.vic.gov.au/dhsportal/wps/myportal): <https://hns.dhs.vic.gov.au/dhsportal/wps/myportal>
2. Login to your eBusiness account by entering your username and password. Review the *Conditions of Use* and *Monitoring of Computer Services*. If you agree with the terms, click on the box to display a tick and then click on the ‘Login’ button.

Figure 11: image of the eBusiness login screen



1. Click on the *Additional application access* tab at top of the page

**Figure 12: image of the eBusiness home page**



1. Select your organisation for which you want the ‘CIMS Production’ access to apply.
2. Select ‘CIMS Production (1.0.0.0)’ from the *Application catalogue* box and then click on the ‘Apply’ button.

Figure 13: image of the eBusiness request additional application access



6. Go to [Step 2](#_Step_2_-) (Organisational Authority approves eBusiness request).

## Step 2 - Organisation Authority approves eBusiness request

The Organisation Authority (OA)\* will receive an automated email from eBusiness to authorise the staff member’s eBusiness access request.

The OA logs into eBusiness to approve eBusiness/application requests.

\*Refer to the Troubleshooting chapter of this document (pg 14) if your organisation requires a new OA. (A *Change of Organisation Authority* *Form* - Appendix 1 - must be completed and emailed to ebiz@dhhs.vic.gov.au to update the OA details).

It is the organisation’s responsibility to make eBusiness aware if an OA has left the organisation and a new OA is to be appointed.

## Step 3 – DHHS provides access to the application.

DHHS will grant the staff member access to eBusiness and the CIMS application.

This step can only be completed when the staff member’s OA has approved their use of the application in eBusiness.

## Step 4 - Confirmation email sent to staff

A confirmation email is automatically sent from eBusiness to the staff member confirming access to the application. The email contains their eBusiness username and password\*.

*\*Password provided is only to be utilised for new users, existing users are able to log in using their existing password.*

It is important that staff follow the instructions within the email to update their eBusiness password.

## Step 5 - Access the eBusiness portal and the application

1. Go to the [Department of Health and Human Services eBusiness portal](https://hns.dhs.vic.gov.au/dhsportal/wps/myportal): <https://hns.dhs.vic.gov.au/dhsportal/wps/myportal >
2. Login to your eBusiness account by entering your username and password. Review the *Conditions of Use* and the *Monitoring of Computer Services*. If you agree with the terms, click on the box to display a tick and then click on the ‘Login’ button.

Figure 14: image of the eBusiness Login screen



1. Click on the **CIMS Production** link in the Home page. The application will open. You now have access to the CIMS.

**Figure 15: image of the eBusiness home page - list of approved applications for access**



# Roles and responsibilities

## Organisation Authority

An Organisation Authority (OA) is a person designated by the organisation to be the key contact for the department in relation to authorising and maintaining users in the department's technology systems. The OA is determined at the time the organisation enters into the eBusiness Access Agreement with the department and is usually the CEO or other senior member of the organisation. The person nominated for this role must be currently listed as in this role with the department and must be available as they assess and authorise staff for eBusiness applications.

The OA in each organisation is responsible for authorising the staff member’s access to use the eBusiness environment and the application. **OA’s should only authorise access for staff whose role/position within the organisation warrants their use of the application.**

## Application Authority

The department’s Application Authority will provide staff access to the application when the Organisation Authority has approved the staff request in eBusiness.

# Troubleshooting

There are a number of steps in the eBusiness registration process that can cause registration delays. Below provides information on how to overcome the most common registration issues.

#### My request for eBusiness registration or access to the application is not being actioned.

The Organisation Authority (OA) within an organisation must approve all requests related to eBusiness. There are a number of reasons why the request may be delayed from the organisation’s side:

* The OA no longer works for the organisation and can’t approve the eBusiness request.
* The OA is on leave and hasn’t approved the eBusiness request.
* The OA does not know the staff member and cannot confirm their identity.

If the OA no longer works for the organisation, another OA will need to be nominated. The *Change of Organisation Authority* *Form* (Appendix 1) must be completed and emailed to ebiz@dhhs.vic.gov.au prior to staff applying for eBusiness.

#### My organisation’s OA has approved my request but I haven’t received confirmation of my access.

Possible reasons for why a staff member may not have been notified of access include:

An incorrect email address was provided in the eBusiness registration request, therefore the confirmation email bounced or went to an unused destination.

The automated email confirming registration was recognised as SPAM and could be in the staff member’s email Trash/Junk folder.

A yahoo or hotmail email address was provided in the eBusiness registration request. The work email address must be used when registering.

To check the status of your access request, please contact eBusiness Support on 1300 799 470 or email ebiz@dhhs.vic.gov.au

#### I was registered for eBusiness through my old organisation but now work for another organisation.

If a staff member leaves an organisation, and wishes to register for an application from another organisation, they must cancel their previous registration by contacting eBusiness Support on 1300 799 470 or ebiz@dhhs.vic.gov.au. Once cancelled, the new eBusiness registration can then be applied for and processed.

#### A staff member has left the organisation and no longer requires access to eBusiness and/or the CIMS application.

The staff member’s manager needs to send an email to ebiz@dhhs.vic.gov.au and request that the staff member’s access to eBusiness be removed.

Any person in the organisation provisioned as a Senior Delegate in CIMS can update the CIMS user access (by end dating the user account) in CIMS itself. (CIMS has a self-service function which enables organisations to self-manage user provisioning. Step by step instructions on how to manage CIMS user access is in *Chapter 14 - Managing user profiles* of the *CIMS IT Client Incident Register User Manual* available on the Department's CIMS web page: <https://providers.dhhs.vic.gov.au/client-incident-register-user-manual-cims-word> .

**I cannot register for eBusiness as my organisation is not registered for eBusiness.**

Organisations must be registered for eBusiness in order for their staff to then be registered with eBusiness. Registration of an organisation in eBusiness requires the organisation’s duly authorised representative to complete an ‘*Organisation Authority Nomination’* form (Appendix 2) and an ‘*eBusiness Access Agreement*’ form (Appendix 3) to commence the process. Contact eBusiness Support on 1300 799 470 or ebiz@dhhs.vic.gov.au for further instruction of the process. Once the organisation has been registered for eBusiness, staff can then apply for their individual eBusiness registrations.

# Support and contacts

If you have any questions or difficulties with eBusiness registration, please contact eBusiness Support on 1300 799 470 or email via ebiz@dhhs.vic.gov.au .

# Appendices

## Appendix 1 – Change of Organisation Authority Form

The *Change of Organisation Authority form* template is on Pg 17 of this document.

It is to be completed when an organisation has been registered for eBusiness however they are needing to nominate a **replacement** Organisation Authority (OA). A replacement OA is nominated where the primary OA has left the organisation or is no longer able to carry out their responsibilities as an OA.

Please note that there can only be one primary OA per organisation to validate registration requests for staff of that organisation. However, an organisation can nominate a secondary OA to share this responsibility within an organisation. Contact eBusiness support on 1300 799 470 or ebiz@dhhs.vic.gov.au for further information.

## Appendix 2 – Organisation Authority Form

The *Organisation Authority form* template is on Pg 19 of this document.

To be completed when registering a **new** primary Organisation Authority (OA). A new primary OA is nominated where the Organisation is wanting to register for eBusiness. This form must be completed and submitted to the department with the signed eBusiness access agreement form (Appendix 3).

Please note that there can only be one primary OA per organisation to validate registration requests for staff of that organisation. However, an organisation can nominate a secondary OA to share this responsibility within an organisation. Contact eBusiness support on 1300 799 470 or ebiz@dhhs.vic.gov.au for further information.

## Appendix 3 – eBusiness Access Agreement

The *eBusiness Access Agreement* template is on Pg 21 of this document.

An eBusiness Access Agreement states the terms and conditions to be applied when providing organisations access to the department’s eBusiness environment. This Agreement must be completed and submitted to the department together with the signed Organisation Authority nomination form (Appendix 2).

Appendix 1



# Change of Organisation Authority

Organisation:

[As entered on the signed eBusiness Access Agreement]

Authorised by:

[Name of the Organisation’s duly authorised representative who signed the eBusiness Access Agreement]

Signed by Date: ….../...../

[Signature of the Organisation’s duly authorised representative who signed the eBusiness Access agreement]

**Current Organisation Authority’s details**

First Name:

Last Name:

Telephone:

Email:

**Newly Nominated Organisation Authority’s details**

First Name:

Last Name:

Telephone:

Email:

**Organisation Authority Responsibilities – For Information**

**1. Organis**a**tion Authority Role**

The role of the Organisation Authority is to manage user and organisational matters related to their Organisation for access to the DHHS eBusiness Environment. The Department views the Organisation Authority as a key local resource having inherent knowledge and capacity to undertake important tasks relating to access and registration of the organisation’s users.

As part of granting the organisation access to the DHHS eBusiness Environment, the Department will provide the Organisation Authority with access to an Internet based application that permits him or her to fulfil the responsibilities detailed below.

**2. Organisation Authority Responsibilities**

The Organisation Authority has the following responsibilities:

2.1. Verifying the identity of a person applying to be registered as a User of the DHHS eBusiness Environment; (Is the person who they claim to be?) and validating their organisational and role details (Is this the actual job they are doing?);

2.2. Verifying that the employee’s job/position within the Organisation warrants them to have access to the requested eBusiness application (Should this staff member have access to that application?);

2.3. Maintaining the currency of organisational structure and details for their Organisation (for example, add or remove child Organisations or change the Organisation address details); and

2.4. Maintaining the currency of the registered eBusiness Users for their Organisation (for example, advice on de-registering User accounts).

2.5. Ensuring that users’ access rights are reviewed at regular intervals.

**3. Delegation of t**h**e Organisation Authority Role**

The Organisation Authority may delegate the Organisation Authority role to one or more secondary Organisation Authorities. The roles are essentially the same. The value in delegation arises in providing a backup person to the primary Organisation Authority in situations where the primary Organisation Authority is unavailable from time to time.

For further information email eBiz@dhhs.vic.gov.au or call the IT Service Centre, CenITex on **13 17 65.**

|  |
| --- |
| To receive this publication in an accessible format, email eBusiness <eBiz@dhhs.vic.gov.au>Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.© State of Victoria, Department of Health and Human Services, April 2017.Available on the [Service agreements intranet page](https://intranet.dhhs.vic.gov.au/service-agreements) <https://intranet.dhhs.vic.gov.au/service-agreements>  |

**Please scan and email this completed and signed form to:**

**Email:** ebiz@dhs.vic.gov.au

**Subject:** Change toOrganisational Authority Nomination Form

|  |
| --- |
| Organisation authority nomination form |
|  |



Appendix 2

**This form must be completed and submitted to the department with the signed eBusiness access agreement form attached:**

**Organisation**:

*[As entered on the signed eBusiness access agreement]*

**Nominated by:**

*[Name of the organisation’s duly authorised representative who signed the eBusiness access agreement]*

**Signed by:**

*[Signature of the organisation’s duly authorised representative who signed the eBusiness access agreement]*

**Date of agreement:** ….. / ..... / …..

**Nominated organisation authority’s details:**

**First name:**

**Last name:**

**Telephone:**

**Email:**

Organisation authority role and responsibilities

**1. Organisation authority role**

The role of the organisation authority is to manage user and organisational matters related to their organisation for access to the DHHS eBusiness environment. The department views the organisation authority as a key local resource having inherent knowledge and capacity to undertake important tasks relating to access and registration of the organisation’s users.

As part of granting the organisation access to the DHHS eBusiness environment, the department will provide the organisation authority with access to an internet-based application that permits him or her to fulfil the responsibilities detailed below.

**2. Organisation authority responsibilities**

The organisation authority has the following responsibilities:

* verifying the identity of a person applying to be registered as a user of the DHHS eBusiness environment (is the person who they claim to be?) and validating their organisational and role details (is this the actual job they are doing?)
* verifying that the employee’s job/position within the organisation warrants them to have access to the requested eBusiness application (should this staff member have access to that application?)
* maintaining the currency of organisational structure and details for their organisation (for example, add or remove child organisations or change the organisation address details)
* maintaining the currency of the registered eBusiness users for their organisation (for example, advice on de-registering user accounts)
* ensuring that users’ access rights are reviewed at regular intervals.

**3. Delegation of the organisation authority role**

The organisation authority may delegate the organisation authority role to one or more secondary organisation authorities. The roles are essentially the same. The value in delegation arises in providing a backup person to the primary organisation authority in situations where the primary organisation authority is unavailable from time to time.

For further information, email the eBusiness support group <ebiz@dhhs.vic.gov.au> or call the IT Service Centre, CenITex on **13 17 65.**

|  |
| --- |
| To receive this publication in an accessible format, email eBusiness <ebiz@dhhs.vic.gov.au>Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.© State of Victoria, Department of Health and Human Services, June 2017.Available on the [Service agreements intranet page](file:///C%3A%5CUsers%5Cmmag0106%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CIE%5CIVP5KHIR%5CService%20agreements%20intranet%20page) <https://intranet.dhhs.vic.gov.au/service-agreements>  |

**Please scan and email this completed and signed form together with the eBusiness Access Agreement (Appendix 3) to:**

**Email:** ebiz@dhs.vic.gov.au

**Subject:** Organisational Authority Nomination Form


**CIMS AGREEMENT**

Appendix 3

|  |  |
| --- | --- |
| **PARTIES** | The State of Victoria as represented by the Department of Health and Human Services (ABN 74 410 330 756) 50 Lonsdale St, Melbourne, Vic, 3000(‘**Department**’)*and*[Name and ACN/ABN of Organisation] [Address of Organisation](‘**Organisation**’) |

**EXECUTION**

**Executed as an agreement**

|  |  |  |
| --- | --- | --- |
| **Department:****SIGNED** by [name], [position], [branch/division], as authorised representative for theDepartment of Health and Human Services for and on behalf of the **STATE OF VICTORIA** (ABN 74 410 330 756) |  |  |
|  Signature of authorised representative...................................................................Date: |  |  |

**Organisation:**

I, the Organisation’s duly authorised representative, have read this CIMS Agreement and accept the obligations of the Organisation as set out in this CIMS Agreement.

|  |  |
| --- | --- |
| ........................................................................................... |  |
| Name of Organisation’s duly authorised representative |  |
| ......................................................................................... |  |
| Name of Organisation............................................................................................Signature of Organisation’s duly authorised representative |  |

................................................................................

Date:

BACKGROUND

1. The Department has developed the Client Incident Management System IT solution for the purpose of supporting the safety and wellbeing of clients.
2. The Department may grant the Organisation access to CIMS in two different ways, either through;
	1. a web portal to manage Organisation Data (**Portal Access**); and/or
	2. an API gateway for the exchange of Client Incident Information (**API Access**).
3. This CIMS Agreement applies to both types of access to CIMS.
4. The Organisation wishes to have access to CIMS and the Department wishes to grant access to CIMS, on the terms and conditions set out in this CIMS Agreement.

# **DEFINITIONS**

1.1 For the purposes of this CIMS Agreement:

**Business Day** means a day from Monday to Friday (inclusive) that is not a public holiday in Victoria**.**

**Business Hours** means 9 am to 5 pm on a Business Day**.**

**CIMS** means the client incident management system IT solution operated by the Department, including the Portal Access and the API Access.

**CIMS Agreement** means the terms and conditions of this agreement.

**CIMS Commencement Date** means the date on which the Department signs this CIMS Agreement.

**Commissioners Guidelines** means the Office of the Victorian Commissioner for Privacy and Data Protection publication, *Guidelines to protecting the security of personal information: ‘Reasonable steps’ under Information Privacy Principle 4.1 (January 2017)*, as updated from time to time.

**Confidential Information** means all information or data made accessible to the Organisation in relation to CIMS, but does not include:

A. the Organisation Data;

B. information that is, or becomes part of the public domain other than by breach of this CIMS Agreement;

C. information lawfully obtained by the Organisation from another person without any restriction as to use and disclosure; or

D. information in the Organisation's possession prior to disclosure to it by the Department.

**Client Incident Information** means information in relation to client incidents submitted by the Organisation to the Department.

**Health Privacy Principles** means the health privacy principles set out in the *Health Records Act 2001* (Vic).

**Information Privacy Principles** means the information privacy principles set out in the *Privacy and Data Protection Act 2014* (Vic).

**Nominated Purposes** means the management and reporting of client incidents in accordance with the guidance material issued by the Department from time to time, unless otherwise agreed by the Department and the Organisation.

**Organisation Authority** means the person(s) nominated by the Organisation in writing and who will perform the functions set out in clause 5.

**Organisation Data** means any information entered into CIMS by the Organisation, except any Client Incident Information.

**User** means a person employed by the Organisation and registered on CIMS with a valid access account.

**Written Notice** means an email sent by the Department to the Organisation Authority and/or a notice posted to the website of the Department. The Department shall take reasonable steps to bring the notice to the attention of the Organisation.

# **TERM**

* 1. This CIMS Agreement commences on the CIMS Commencement Date and will continue until it is terminated in accordance with clause 6.

# **THE DEPARTMENT**

* 1. The Department grants to the Organisation the right to access and use CIMS for the duration of this CIMS Agreement for the Nominated Purposes on the terms set out in this CIMS Agreement. The way in which the Department grants the Organisation access to CIMS, that is, through Portal Access and/or API Access, shall be agreed by the parties.

# **THE ORGANISATION**

* 1. The Organisation agrees that it will be bound by the Information Privacy Principles and the Health Privacy Principles with respect to any act done in connection with CIMS in the same way as the Department would have been bound had the relevant act been done by the Department. The Organisation agrees that it will ensure that it makes individuals whose information is entered into CIMS aware that:
		1. the Department is an organisation to which the Organisation may disclose their personal information; and
		2. the Organisation may collect and disclose information to the Department for the Nominated Purposes.
	2. The Organisation must take reasonable steps to protect any personal information in connection with CIMS, as described in the schedule to this CIMS Agreement or the Commissioners Guidelines, during the term of this CIMS Agreement.
	3. The Organisation Data may only be accessed or used by the Department for the purpose of the operation and administration of CIMS. The Department may use the Client Incident Information for any purpose of the Department.
	4. The Organisation warrants its computer environment and data transfer protocols will be compatible with CIMS, as varied under clause 4.5.
	5. The Organisation acknowledges that the Department may vary CIMS on 10 Business Days’ Written Notice or other notice period as nominated by the Department and that, in that event, the Organisation must (at its own cost) perform whatever upgrades may be required to its computer environment as may be necessary to ensure it continues to comply with the warranty in clause 4.4.
	6. The Organisation will ensure that neither it nor any person to whom it gives access to the Confidential Information will disclose any of the Confidential Information of the Department to any other person without the prior written consent of the Department unless required by law.
	7. The Organisation must not use the name or branding of the Department in a way that suggests endorsement or association with the Department, without prior written approval.

# **FUNCTIONS OF THE ORGANISATION AUTHORITY**

* 1. The Organisation will ensure that the Organisation Authority manages User and organisational matters related to the Organisation for CIMS, including if applicable to the type of access to CIMS used by the Organisation:
		1. verifying the identity of a person applying to be registered as a User of CIMS and his/her role within the Organisation;
		2. verifying that a prospective User's job/position within the Organisation requires him/her to access CIMS;
		3. periodically reviewing each User's need to access CIMS;
		4. maintaining the currency of organisational details including but not limited to structure and registered address;
		5. maintaining an up to date register of Users, and a record of previous/de-registered Users, who access(ed) CIMS on behalf of the Organisation; and
		6. being available by telephone to the Department at all times during Business Hours with regard to Users and any issues related to User access.

# **TERMINATION**

* 1. Either party may terminate this CIMS Agreement with at least 30 Business Days’ written notice to the other party.
	2. The Department may, by written notice, immediately terminate this CIMS Agreement if, in the reasonable opinion of the Department, the Organisation;
		1. is no longer eligible to access CIMS;
		2. has committed a breach of this CIMS Agreement and failed to rectify the breach within 5 Business Days of receiving written notice from the Department to do so; or
		3. has committed a breach of this CIMS Agreement which is not capable of being rectified.
	3. The Organisation acknowledges that it is responsible for downloading any Organisation Data from CIMS prior to the termination of this CIMS Agreement and record keeping in relation to the Organisation Data thereafter. After the termination of this CIMS Agreement, the Department may delete the Organisation Data after 120 Business Days.

# **LIABILITY**

* 1. To the extent permitted by law, the Department shall have no liability in damages (including special, indirect or consequential damages, which damages will be deemed to include loss of revenue, loss of profit and opportunity loss) in respect of any act or omission of the Department in connection with CIMS, even if the Department has been advised by the Organisation as to the possibility of such losses being incurred.
	2. Subject to clause 7.3, the CIMS is provided on an ‘as is’ and ‘as available’ basis without any express or implied warranties in respect of CIMS.
	3. Pursuant to section 64A of the Australian Consumer Law, this clause applies in respect of any goods or services supplied under this agreement which are not of a kind ordinarily acquired for personal, domestic or household use or consumption, provided that this clause will not apply if the Customer establishes that reliance on it would not be fair and reasonable. Liability for breach of a guarantee conferred by the Australian Consumer Law (other than those conferred by sections 51 to 53 of the Australian Consumer Law) is limited:
		1. to the supplying of the services again; or
		2. to the payment of the cost of having the services supplied again.
	4. The Organisation acknowledges that CIMS shall not be error free or without interruption.

# **ACCEPTABLE USE**

* 1. The Organisation must not use CIMS in a manner that;
		1. breaks or circumvents any of the technical, administrative or security measures;
		2. disrupts the performance or degrades the performance of CIMS; or
		3. attempts to exceed or circumvents limitations on volume or otherwise in a manner that exceeds reasonable volumes or volumes specified in a Written Notice.
	2. The Organisation may use the Client Incident Information retrieved through the API Access in any third party applications at its own risk. The Organisation must rely on its own inquiries and judgement as to the suitability of the Client Incident Information for use in any third party application.

# **9. GENERAL**

9.1 If a court finds that any part of this CIMS Agreement is void, unenforceable, or otherwise legally ineffective (“Ineffective”) in any jurisdiction, then the offending part will be read and interpreted in a manner that would not render it Ineffective. If an Ineffective part cannot be read in a way that ensures it is not Ineffective, then the offending part will be deleted from this CIMS Agreement and the remainder of this CIMS Agreement will be construed in a manner so as to ensure the remaining parts continue in force to the greatest extent possible.

9.2 The Organisation acknowledges and accepts that no right under this CIMS Agreement is waived or deemed to be waived except by Written Notice.

9.3 In the event of a change in policy of the Department then the Department may amend this CIMS Agreement by Written Notice to implement the change in policy.

# **10. GOVERNING LAW**

10.1 The laws of the State of Victoria govern this CIMS Agreement. The Organisation agrees to the non-exclusive jurisdiction of the courts in the State of Victoria.

**SCHEDULE – REASONABLE STEPS TO PROTECT PERSONAL INFORMATION**

1. The Organisation must anticipate and take necessary precautions to address foreseeable security risks based on current common cyber security issues.
2. The foreseeable security risks include but not limited to:
	* Lost or stolen laptops and USB storage devices;
	* Accidental exposure and loss of data caused by administrator misconfiguration;
	* Use of insecure legacy IT;
	* Targeted attacks caused by malicious emails and web based malware;
	* Lack of Network segmentation and isolation of confidential data; and
	* Inadequate cyber security incident response plans.
3. The Organisation should access and use two free Commonwealth Government services that provide current and ongoing guidance to mitigate common cyber security threats;
	* <https://www.asd.gov.au/infosec/mitigationstrategies.htm>
	* <https://www.staysmartonline.gov.au/alert-service>
4. The advice from ASD is a pdf that explains how to implement basic IT security controls that will mitigate in excess of 85% of common targeted cyber security attacks.
5. Stay Smart online is a subscription service that provides timely notifications of critical software and operating system security patches
6. To address the most common current cyber security risks, the Organisation should, at a minimum:
	* Use encryption on all laptops and portable storage devices;
	* Only use sanctioned cloud file sharing services - https://www.asd.gov.au/infosec/irap/certified\_clouds.htm;
	* Regularly test IT infrastructure to identify and address misconfiguration;
	* Only use current and supported IT systems and operating systems;
	* Take reasonable steps to implement the ASD Essential Eight - https://www.asd.gov.au/infosec/mitigationstrategies.htm
	* Where applicable, implement network segmentation and isolate confidential data - https://www.asd.gov.au/publications/protect/network\_segmentation\_segregation.htm
7. The Organisation should subscribe to and implement in a timely manner the regular security updates issued by the Stay Smart Online service;
	* https://www.staysmartonline.gov.au/alert-service
8. The Organisation should subscribe to the Commonwealth Government’s Stay Smart online service also issues a more detailed Small Business Guide that can assist small organisations implement basic cyber security hygiene controls. <https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay-Smart-Online-Small-Business-Guide_0.PDF>
9. For a more detailed information concerning “reasonable steps” to protect personal information, the Organisation should refer to the Commissioners Guidelines.