**Type: Guidelines**

**Name: Guidelines for the use of Cloud Software Services**

**Purpose**

These Guidelines support the CCDHB Cloud Framework and are to be used when purchasing or subscribing to Cloud Software services for use at CCDHB.

**Definitions**

**Cloud Services** are software services supplied from an external data centre. They may be sold as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS)

**CISO** Chief Information Security Officer

**In Confidence** is the classification used for information that requires protection from unauthorised access during processing, transfer, or while at rest.

Examples are personal health information, identifiable staff information not intended for the public domain, and commercially sensitive information that needs protection from unauthorised access, such as customer payment details.

**IPSG** Information Privacy and Security Governance Committee

**Personal Information** means any information about an identifiable living individual.

**Restricted** adversely affect the internal stability or economic wellbeing of New Zealand or friendly countries.

**Sensitive** endanger the safety of any person

**Special Handling Subject Matter** is the classification for information that requires higher access standards to ensure the ‘need to know’ principle is maintained.

subject matter that is considered to require special handling includes mental health information, sexual diseases, abuse, etc.

**Guidelines Content**

1. *Introduction*
2. *Process Outline*
3. *Classify the Information*
4. *Pre-approved services*
5. *Assess Base Risk*
6. *No Risk Evident*
7. *Some Risk Evident*
8. *Significant Risk Evident*
9. *Significant Risk Presumed*
10. *Extreme Risk Presumed*
11. **Introduction**

* Staff are encouraged to make use of Cloud Software services where these are available and appropriate.
* Because these services are a “contract for supply”, staff are expected to adhere to the CCDHB governance requirements applicable to such purchases.
* When these services involve passing personal and or health information, it is important to ensure that the cloud service takes an appropriate level of care of the information with respect to privacy and security.
* it is important that sufficient diligence is undertaken when selecting a service and entering into an agreement.
* Staff are reminded to be particularly wary of free cloud services as any offers or guarantees made by the supplier may not be enforceable.
* Staff are reminded that ability of 3DHB ICT to provide assistance with issues arising from cloud services are limited.

1. **Process overview**

* The process is a risk management activity.
* The amount of diligence for any proposal is determined by the amount of risk that becomes evident during the process.
* Proposals for cloud services where there is no risk evident are self-assessed and proceed with the minimum of governance.
* Where risk becomes evident, the amount of diligence required increases accordingly and 3DHB ICT and CCDHB Legal will be engaged to assist the process automatically.
* 3DHB ICT and CCDHB Legal may be approached directly at any time during the process.

3DHB ICT Security email here

CCDHB Privacy email here

Process flow chart here



1. **Classify the Information**

* Classify the information according CCDHB information classification guidelines.

Use the form [here](file:///\\ad\depts\HIQ\Architecture\Security\3DHB_ICT_Information_Classification_guide_HISF.docx)

If your classification indicates that your information requires special handling, please skip to the **Significant Risk Presumed** section of this guideline.

The CCDHB policy on information classification is here

1. **Pre-preapproved services**

**Approval:** these proposals do not require approval

* Some cloud services have already been approved for use and these may be used provided any remaining CCDHB governance requirements have been met. The cloud service may be approved subject to certain guidelines. It is important that staff adhere to the guidelines if they use the service.

A list of pre-approved services and guidelines for their use is here

1. **Assess the base risk**

* Use the cloud assessment tool to establish the base risk category for the proposal.

The Cloud Assessment tool is [here](file:///\\ad\depts\HIQ\Architecture\Security\cloud%20computing\SaaS\3DHB_ICT_Cloud_Questionnaire.docx)

* Whether patient or personal information can be de-identified is an important factor when assessing risk.

Guidance on de-identifying information can be found here

* If you **can** answer every question with a “yes”, your proposal has no evident risk and you may proceed to utilise this service upon completing any remaining CC DHB governance requirements.
* If you **cannot** answer every question with “yes”, your proposal has evident risk and further diligence is required.

1. **No Risk Evident**

**Approval:** these proposals are approved by the Service wanting to use the Cloud Service**.**

* If you answer every question with a “yes”, your proposal has no evident risk and you may proceed to utilise this service upon completing any remaining CC DHB governance requirements.

Send your assessment to [IT.ServiceDesk@ccdhb.org.nz](mailto:IT.ServiceDesk@ccdhb.org.nz)

* If you cannot answer every question with “yes”, your proposal has evident risk and further diligence is required. Proceed to **Some Risk Evident**.

1. **Some Risk Evident**

**Approval:** these proposals are approved by 3DHB ICT and CCDHB Legal

* Complete the Brief Cloud Security Assessment form and the Brief PIA form.

The Brief Cloud Security Assessment form is [here](file:///\\ad\depts\HIQ\Architecture\Security\cloud%20computing\3DHB_ICT_Brief_Cloud_Security%20Assessment.docx)

* Most reputable vendors will publish their Privacy Policy and their “Terms and Conditions” or some form of Service Level Agreement on their website. It is important that you familiarise yourself with these so that you understand what you can you can expect from the vendor.
* Use the information from the vendor to answer the questions in the vendor section of the Brief Cloud Security Assessment form.
* “Unsure” is an acceptable answer if you cannot answer a question from the vendor’s information.
* When carrying out the assessments, you may become aware of some risks and how they might be managed. Please include this information in your assessments.
* Send your assessments and the information you obtained from the vendor to [IT.ServiceDesk@ccdhb.org.nz](mailto:IT.ServiceDesk@ccdhb.org.nz)
* The Service Desk will create a task on your behalf and forward your assessments to 3DHB ICT and CCDHB Legal for prioritisation and review.
* If the risks to be managed fall within the delegation of 3DHB ICT and CCDHB Legal, they will prepare a response which may include recommendations and approval to implement.
* If the risks to be managed fall outside the delegation of 3DHB ICT and CCDHB Legal, they will escalate the proposal to the IPSG committee for consideration under the **Significant Risk Evident** process.
* In either case you will be advised of advised of the outcome.
* If your proposal is approved you may proceed to utilise this service upon completing any remaining CCDHB governance requirements.

1. **Significant Risk Evident**

**Approval:** these proposals are approved by IPSG

* 3DHB ICT and CCDHB Legal will conduct an assessment proportionate to the level of risk evident.
* Their assessment and any recommendations will be referred to the IPSG for consideration.
* The IPSG will prepare a response which may include recommendations and approval to implement.
* You will be advised of the out come.
* If your proposal is approved you may proceed to utilise this service upon completing any remaining CCDHB governance requirements.

1. **Significant Risk Presumed**

**Approval:** these proposals are approved by IPSG

* Complete the Brief Cloud Security Assessment form and the Brief PIA form.
* Most reputable vendors will publish their Privacy Policy and their “Terms and Conditions” or some form of Service Level Agreement on their website. It is important that you familiarise yourself with these so that you understand what you can you can expect from the vendor.
* Use the information from the vendor to answer the questions in the vendor section of the Brief Cloud Security Assessment form.
* “Unsure” is an acceptable answer if you cannot answer a question from the vendor’s information.
* When carrying out the assessments, you may become aware of some risks and how they might be managed. Please include this information in your assessments.
* This category of risk requires evidence of appropriate “special handling” measures. Please consider these and include them, if any, with your assessment.
* Send your assessments and the information you obtained from the vendor to [IT.ServiceDesk@ccdhb.org.nz](mailto:IT.ServiceDesk@ccdhb.org.nz)
* 3DHB ICT and CCDHB Legal will conduct an assessment proportionate to the level of risk evident.
* Their assessment and any recommendations will be referred to the IPSG for consideration.
* The IPSG will prepare a response which may include recommendations and approval to implement.
* You will be advised of the out come.
* If your proposal is approved you may proceed to utilise this service upon completing any remaining CCDHB governance requirements.

1. **Extreme Risk Presumed**

**Approval:** these proposals are approved by the CEO

This is a special category of risk and applies where the information is classified **above** “in confidence”.

* If your proposal involves information which you believe is classified as “restricted” or “sensitive”, contact the CISO directly.

Disclaimer: This document has been developed by Capital & Coast District Health Board (CCDHB) specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and CCDHB assumes no responsibility whatsoever.