Cloud Services

CATHOLIC ARCHDIOCESE OF PERTH

Policy Category	Archives and Information Governance
Policy Sub-category	Records Management
Approving Authority	Executive Director, Finance and Administration
Approval Date	14 November 2022
Review Schedule	16 December 2025

Table of Contents

Cloud Services

Background and Purpose

Cloud Services technology provides the Catholic Archdiocese of Perth (the Archdiocese) with the ability to store data in offsite geographically remote facilities.

The use of cloud -based services enables the Archdiocese to move away from on-premise hardware and to utilise the increased scalability, reliability, and functionality provided by cloud services.

Taking advantage of cloud services requires the Archdiocese to implement appropriate data security controls including with respect to the management of cloud service arrangements with providers.

The purpose of this policy is to:

- Provide an outline of the different types of cloud services;
- Outline the potential risks of using cloud services and the risk mitigation strategies to be put in place;
- Set out roles and responsibilities with respect to engagement with cloud service providers (CSPs); and
- Ensure that the Archdiocese complies with applicable laws, regulations and standards.

Scope

This policy applies to:

- Employees and Volunteers; (referred to in this Policy as Staff/Staff Members)
- All Archdiocese-owned agencies, offices and organisations belonging to the Roman Catholic Archbishop of Perth Corporation Sole, who create, capture, store and use records and data in the Archdiocese.

Principles

- 3.1 The Archdiocese is committed to ensuring that the use of cloud-based services:
  - a. Supports the strategic and operational objectives of the Archdiocese's Information Governance Strategy and the requirements of the National Catholic Safeguarding Standards;
  - b. Enhances the Archdiocese's information governance and management systems;
  - c. Is governed by appropriate risk mitigation strategies and practices to protect the Archdiocese's data, operations and reputation from exposure to risks associated with using cloud services; and
  - d. Complies with applicable laws, regulations and standards.

Cloud Service Models

- 4.1 Cloud services are provided via three (3) cloud service models:
  - 4.1.1. **Infrastructure as a Service** (IAAS) which involves the vendor providing physical computer hardware including CPU processing, memory, data storage and network connectivity. The vendor may share their hardware among multiple customers referred to as ‘multiple tenants’ using virtualisation software. IAAS enables customers to run operating systems and software applications of their choice. Typically the vendor controls and maintains the physical computer hardware. Typically the customer controls and maintains the operating systems and software applications. an example IAAS vendor service is Amazon Elastic Compute Cloud (EC2).
  - 4.1.2. **Platform as a Service** (PaaS) involves the vendor providing infrastructure as a service plus operating systems and server applications such as web servers. PaaS enables customers to use the vendor’s cloud infrastructure to deploy web applications and other software developed by the customer using programming languages supported by the vendor. Typically the vendor controls and maintains the physical computer hardware, operating systems and server applications. Typically the customer only controls and maintains the software applications developed by the customer.
  - 4.1.3. **Software as a Service** (SaaS) which involves the vendor using their cloud infrastructure and cloud platforms to provide customers with software applications. Example applications include email and an environment for users to collaboratively develop and share files such as documents and spreadsheets. These end user applications are typically accessed by users via a web browser, eliminating the need for the user to install or maintain additional software. Typically the vendor controls and maintains the physical computer hardware, operating systems and software applications. Typically the customer only controls and maintains limited application configuration settings specific to users such as creating email address distribution lists. Example SaaS vendor services include Customer Relationship Management, Google Docs, Google Gmail and Microsoft 365.
- 4.2. The service utilised by the Archdiocese is **Software as a Service** (SaaS).

Methods of Deployment

- 5.1 There are four cloud service deployment models:
  - 5.1.1. **Public cloud** which involves an organisation using a vendor's cloud infrastructure which is shared via the internet with many other organisations and other members of the public. This model has maximum potential cost efficiencies due to economies of scale. However, this model has a variety of inherent security risks that need to be considered.
  - 5.1.2. **Private cloud** involves an organisation's exclusive use of cloud infrastructure and services located at the organisation's premises or offsite, and managed by the organisation or a vendor. Compared to the public cloud model, the private cloud model has reduced potential cost efficiencies. If the private cloud is properly implemented and operated, it has reduced potential security concerns. A well architected private cloud properly managed by a vendor provides many of the benefits of a public cloud, but with increased control over security. A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the vendor, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud vendors.
  - 5.1.3. **Community cloud** involves a private cloud that is shared by several organisations with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a private cloud by several departments of the same government.
  - 5.1.4. **Hybrid cloud** involves a combination of cloud models. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data, which interacts with sensitive data stored or processed in a private cloud.

[1] Australian Cyber Security Centre: Cloud Computing Security Considerations October 2021 https://www.cyber.gov.au/

Cloud Service Risk Management

- 6.1. Engaging in an arrangement with a CSP is not without risk. For example:
  - i. The act of sending or storing data outside a State, Territory or Country might be, in itself, a breach of local laws;
  - ii. The cloud service provider might fail to comply with legislation or standards of the local jurisdiction;
  - iii. Data may be subject to legislation and other requirements of the storage jurisdiction;
  - iv. There may be risks associated with unauthorised access to data;
  - v. There may be a risk of a loss of access to data;
  - vi. There may be a risk of data destruction or loss;
  - vii. The evidential value of the data may be damaged; and
  - viii. The service provider may cease operation.[3]
- 6.2. Regardless of the service model (Clause 4) or method of deployment chosen (Clause 5), relevant risks must be identified, mitigated and managed.

- 6.3. To ensure that the Archdiocese is protected the following mechanisms must be in place:
  - 6.3.1. A risk assessment and analysis shall be performed on all cloud services before commencement of service.
  - 6.3.2. The analysis shall identify any risks to the Archdiocese, business unit, process, security, and/or data stored, including:
    - a. The cloud service has appropriate stability or performance levels that satisfy or exceed the business requirements;
    - b. Data is owned by the Archdiocese and is not sold or transferred to another party;
    - c. Data is stored in Australia, except publicly available information (e.g. front-end websites), which is permissible to be stored outside of Australia;
    - d. The cloud service and CSP abide by all Commonwealth, State and Territory legislation;
    - e. At the end of the contract, data is destroyed and recovered/transferred to an alternative CSP; and
    - f. The cloud service includes appropriate mechanisms that satisfy or exceed the security and privacy requirements for the Archdiocese systems and data.
  - 6.3.3. When undertaking the risk assessment as indicated in clause 6.3.2(f) above, the security and privacy mechanisms of the CSP must include the following:
    - a. The cloud solution and CSP meet the Archdiocese's IT security best practices;
    - b. The CSP are accredited against major Australian Commonwealth (Federal) and international security standards (e.g. ISO 27001 and Australian Federal Government's Information Security Manual);
    - c. Secure data in transit between the organisation and the CSP is implemented. This includes secure network protocols and cryptography, two factor authentication and accounts lockouts and logging traffic and activities; and
    - d. Secure data in transit between the organisation and the CSP is implemented. This includes secure network protocols and cryptography, two factor authentication and accounts lockouts and logging traffic and activities; and
  - 6.3.4. An annual risk assessment review shall be performed on all cloud services and CSPs to ensure ongoing compliance with the terms of this Policy.

[3] State Records Office of South Australia Cloud Computing and Records Management June 2015

Roles and Responsibilities

- 7.1. Employees and Volunteers must adhere to instructions or restrictions of this policy and alert the Information Technology Manager to issues that may be either direct or indirect breach of this policy.
- 7.2. The Responsible Officer is the Director of Archives and Information Governance who:
    - 7.2.1. Maintains and updates the policy and advises the Governing Authority and Executive Team of potential breaches of this policy.
    - 7.2.2. Issues instructions and restrictions as required, to ensure compliance with this Policy.
- 7.3. Governing Authority and Executive Team:
    - 7.3.1. Oversees the collective management of information security within the Archdiocese.
    - 7.3.2. Ensures and enforces compliance with this Policy.

Breach of Policy

The Archdiocese will take all alleged breaches of the policy seriously. Alleged breaches may be investigated, and disciplinary action may be taken against a person who is found in breach of this policy, in accordance with legislation, Canonical Law, and Archdiocesan policies.

[4] Based on Department of Local Government, Sport and Cultural Industries Policy

GOVERNANCE FRAMEWORK

Serving the Church in the Digital Age: The Archdiocese of Perth's Information Governance Strategy

SUPPORTING PROCEDURES

National Catholic Safeguarding Standards

RELATED POLICIES

Information Governance Suite of Policies

RELATED PLANS

Business Continuity Plan
IT Disaster Recovery Plan
Risk Management Plan

RELEVANT LEGISLATION AND STANDARDS

Australian Consumer Law (ACL):
Schedule 2 of the Competition and Consumer Act 2010 (Cth)
Parts 6 and 7 of the Competition and Consumer Regulations 2010 (Cth)
Corporations Act 2001 (Cth)
Privacy Act 1988 (Cth)

RESPONSIBLE OFFICER

Director of the Archives and Information Governance Office
Tel: 6104 36 25
Email: archives@perthcatholic.org.au

Version	Date Issued	Approved By	Amendments Undertaken
1.0	16.05.23		Align visual style with other documents, minor text changes, Text changes, removal and adding of pages

For enquiries or more information, please contact:

ODHRAN O'BRIEN
Director of the Archives and
Information Governance Office
Tel: 6104 3625
Email: archives@perthcatholic.org.au

Location: Archives and Information Governance Office,
193 Harold St, Mt Lawley WA 6050

Postal Address: 40A Mary St, Highgate WA 6003

Before referencing this document, please ensure you
have the latest version from the Archdiocesan Intranet.
Printing of this document is not recommended.