Definitions

Cloud computing: Is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.

Public cloud: Is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

Private Cloud: Is based on the standard cloud computing model but uses a proprietary architecture at an organization's in-house facilities or uses an infrastructure dedicated to a single organization.

Financial information: Is any data for {COMPANY-NAME}, its employees, members, or other third parties.

Intellectual property: Is any data that is owned by {COMPANY-NAME} or provided by a third party that would not be distributed to the public.

Other non-public data or information: Are assets deemed the property of {COMPANY-NAME}.

Other public data or information: Are assets deemed the property of {COMPANY-NAME}.

Personally Identifiable Information (PII): Is any data that contains personally identifiable information concerning any members, employees, or other third parties.

Overview

Cloud computing would allow {COMPANY-NAME} to take advantage of technologies for storing and/or sharing documents and other files, and virtual on-demand computing resources. Cloud computing can be beneficial in reducing cost and providing flexibility and scalability.

Purpose

The purpose of this policy is to ensure that {COMPANY-NAME} can potentially make appropriate cloud adoption decisions and at the same time does not use, or allow the use of, inappropriate cloud service practices. Acceptable and unacceptable cloud adoption examples are listed in this policy. All other cloud use cases are approved on a case-by-case basis.

Policy Detail

It is the policy of {COMPANY-NAME} to protect the confidentiality, security, and integrity of each member’s non-public personal information. {COMPANY-NAME} will take responsibility for its use of cloud computing services to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of {COMPANY-NAME}.

This policy acknowledges the potential use of diligently vetted cloud services, only with:

- Providers who prove, and can document in writing, that they can provide appropriate levels of protection to {COMPANY-NAME} data in categories that include, but are not limited to, transport, storage, encryption, backup, recovery, encryption key management, legal and regulatory jurisdiction, audit, or privacy
- Explicit procedures for all handling of {COMPANY-NAME} information regardless of the storage, sharing or computing resource schemes

Cloud Computing Services

The category of cloud service offered by the provider has a significant impact on the split of responsibilities between the customer and the provider to manage security and associated risks.

- Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The customer is responsible for the operating system and the entire software stack necessary to run applications and is responsible for the customer data placed into the cloud computing environment. This means most of the responsibility for securing the applications and the data falls onto the customer.
- Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider, since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the Service Level Agreement (SLA).
- Platform as a Service (PaaS) is a cloud computing service that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Responsibility is likely shared between the customer and provider.

Privacy Concerns

There are information security and data privacy concerns about use of cloud computing services at {COMPANY-NAME}. They include:

- {COMPANY-NAME} may be limited in its protection or control of its data, potentially leading to a loss of security, lessened security, inability to comply with various regulations and data handling protection laws, or loss of privacy of data due to aggregation with data from other cloud consumers.
- {COMPANY-NAME}'s dependency on a third party for critical infrastructure and data handling processes.
- {COMPANY-NAME} may have limited SLAs for a given provider's services and the third parties that a cloud vendor might contract with.
- {COMPANY-NAME} is reliant on vendors' services for the security of the computing infrastructure.

Diligence

In evaluating the potential use of a particular cloud platform, {COMPANY-NAME} will pay particular attention to the foregoing, and other privacy concerns, in addition to its documented vendor due diligence program.

Exit Strategy

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. {COMPANY-NAME} must determine how data would be recovered from the vendor.

Examples

The following table outlines the data classifications and proper handling of {COMPANY-NAME} data.

Data Classification	Public Cloud Computing, Storage or Sharing*	Private Cloud and On-premise Computing or Storage User access restricted by username and password or another authentication
Financial Information	Not Allowed	Allowed No special requirements, subject to any applicable laws
Intellectual Property	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Other Non-Public Data	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Other Public Data	Allowed	Allowed No special requirements, subject to any applicable laws
Personally Identifiable Information (PII)	Not Allowed	Allowed No special requirements, subject to any applicable laws

*See Policy 20 Cloud Computing Adoption Appendix A for approved and non- approved services.

Cloud Computing Adoption

Appendix A

Rev. April 01, 2021

Approved Public Cloud Services

This listing is not represented to be exhaustive and is meant to serve as a point-in-time list of approved or disapproved public cloud services as of the revision date in this appendix. Any cloud service not explicitly listed as approved should be assumed to be not approved until documented otherwise.

Services Approved for {COMPANY-NAME} Use	Services Not Approved for {COMPANY-NAME} Use

**Limited by user and intended use. See restrictions on data classification use in the main policy body*

***Approval under review as of the date of this revision*