CATALYST

WORKPLACES THAT WORK FOR WOMEN

CLOUD VENDOR MANAGEMENT STANDARD

Effective: September 1, 2020

Cloud computing is a method of delivering Information Technology (IT) services where the customer pays to use, rather than own, the resources. These services are typically provided by third parties via the Internet. The widely-accepted definition of cloud computing provided by the US National Institute of Standards and Technology (NIST), is adopted for convenience.

At present there are four widely accepted service delivery models:

- Infrastructure as a Service (IaaS);
- Software as a Service (SaaS);
- Platform as a Service (PaaS);
- Network as a Service (NaaS).

Cloud services are provided via four deployment models:

- Private cloud – where services are provided by an internal provider, i.e. IT;
- Public cloud – where services are provided by third parties, i.e. external companies or entities, over the public Internet;
- Community cloud – where services are provided by external company(s) or entity(s) for a specific community of users with common interests;
- Hybrid cloud – where services are provided partly by an internal provider in a private cloud and partly provided by an external company(s) or entity(s) in the public or community cloud.

Cloud services can provide a significant range of benefits to individuals and organizations including increased solution choice and flexibility, faster time to solution, and reduced total cost of ownership.

Purpose of Standard

This Standard is intended to ensure that all of Catalyst's legal, ethical and standard compliance requirements are met in the procurement, evaluation and use of cloud services.

Application of Standard

This Standard applies to all staff and vendors or organizations acting for, or on behalf of, Catalyst in the evaluation, procurement or use of cloud services.

Standard

Criteria for all cloud services

All Cloud Services must:

1. Be fit for the purpose they are designed to support;
2. Comply with all relevant legislation and regulations (i.e. GDPR, PCI, SHIELD);
3. Comply with all existing Catalyst Policies and Standards;
4. Respect the intellectual property rights of others and not breach copyright;
5. Comply with the relevant professional ethics and with Catalyst's ethical principles; and
6. Not relinquish any Catalyst data ownership rights.

Procedure to procure, evaluate, and use cloud services

All staff and vendors acting for or on behalf of Catalyst must ensure that the following steps are adhered to:

1. The proposed cloud service is suitable for the classification of data which is to be stored or processed in the cloud.

Data Classification	**Cloud Service Deployment Model**	
	Vendor with formal privacy and security policies	**Vendor without a guarantee of security or privacy**
Confidential	Yes	No
Internal	Yes	No
Public	Yes	Yes

2. Approval to use data or information: Where a cloud service is proposed to host Catalyst data or information, appropriate written sign-off must be received from the Information Steward.
3. Approval that information can be hosted in the cloud: Following approval from 2., and evaluation against 1., a cloud service proposed to host personal information, must, before entering into a cloud service agreement, be reviewed, tested as appropriate, and approved to ensure that confidential data can be processed and stored securely. Multiple business units must indicate their approval.
4. For a new cloud service: contact Finance at the start for procurement advice and/or information on existing cloud agreements in place.

5. Contact IT for advice at the evaluation stage. Catalyst places great emphasis on the need for integration and interoperability of systems. These requirements must be considered and documented, and all Catalyst policies, procedures and project prioritization must be adhered to.

6. Backup / Retention / Business Continuity / Disaster Recovery: The service selected must ensure that the data and information is secure at all times and that an adequate backup and recovery plan is in place to ensure that data and information can be retrieved in a timely manner to meet business needs. For more critical systems, the service must be built with high availability, and with a business continuity and disaster recovery plan appropriate to Catalyst's business needs. Where a cloud services is being considered to provide a business-critical IT system, contact IT for advice and sign-off in advance.

7. An appropriate formal contract must be signed with the cloud service provider. It is generally not appropriate to simply accept the third parties' generic terms and conditions. Catalyst's Legal Department must be consulted and provide written sign-off in advance to ensure that appropriate contract law, procurement legislation and Catalyst policies are adhered to.

Standard compliance and handling of Standard breaches

1. Catalyst's VP, Information Technology or Legal Department reserve the right to refuse Catalyst staff or vendors permission to use any new cloud service or to enforce the discontinued use of an existing cloud service if it is deemed to be unsuitable.

2. Catalyst's VP, Information Technology or Legal Department must be notified in writing of all cloud services procured and in use by staff or vendors that hold Catalyst data and information or that have been procured on behalf of Catalyst.

3. Where it is alleged that a breach of this Standard or data has occurred, the matter should be reported to Catalyst's VP, Information Technology immediately. Thereafter, Catalyst's Incident Response Team will establish an investigation to ascertain the facts, mitigate risks and/or make other recommendations.

Violations of Standard

- **Non-Compliance.** An employee who violates this Standard may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Data Classification

- Incident Response

Definitions and Terms

- None

Administration of this Standard

- **Questions.** You are encouraged to ask any questions you may have about this Plan. To learn more, please contact secure@catalyst.org.

- **Reporting.** It is important that you immediately report any suspected violation of this Plan by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Plan will be fully and confidentially investigated.

- **Exception to Plan.** Limited exceptions to the Plan may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Plan. Any request for an exception to the requirements of this Plan must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Plan applies globally unless contrary to local laws and regulations. Operations in different countries may have more stringent policies or implementing procedures where required by local law. In the event of a conflict, these more stringent policies or implementing procedures will take precedence.

Revision History

Date	Name	Description	Responsibility
09/01/2020	James Mbassa	Initial release.	Owner