THE UNIVERSITY OF BRITISH COLUMBIA
Information Technology

Service Level Agreement

Hybrid Cloud Service

Version 0.91 DRAFT
2023-08-24

Document Information

Version History

Version	Date	Description	Author(s)
0.0	2022-01-10	*Formerly 1.0.* Initial draft of Service Level Agreement	Mario Angers
0.1 0.2 0.3 0.4	2022-02-08 2022-03-03 2022-03-04 2022-07-25	*Formerly 1.1, 1.2, 1.3 and 1.4.* Draft. Updates	Mario Angers
0.5	2022-08-02	*Formerly 1.5.* Draft. Updates, including document template and addition of Security Requirements section	Aaron Heck Vanessa Lomas Jagmeet Randhawa
0.6	2022-08-09	*Formerly 1.6.* Draft. Updates incorporating feedback from Safety and Risk Services	Aaron Heck Susan Johnson Robert Tremonti
0.7	2022-08-10	Draft. Updates to stakeholders, period review and service agreement sections.	Mario Angers Aaron Heck Vanessa Lomas Jagmeet Randhawa
0.8	2023-06-16	Draft. Reviewed MLE comments from November '22. Updates to Licensing and Dispute process. Added Termination and Exit Strategy section.	Sanja LeBlanc Brent Dunington Aaron Heck Lee Wang Michael Lonsdale-Eccles
0.9	2023-08-10	Draft. Reviewed Erica Brimacombe's comments and updated sections for clarity.	Sanja LeBlanc Erica Brimacombe
0.91	2023-08-24	Draft. Incorporated Michael Berdan's feedback. Moved Cost and Fee sections to section 5, just above Privacy and Security sections.	Sanja LeBlanc Michael Berdan
0.X	2023-XX-XX		

1.0	2023-XX-XX	Initial version	Mario Angers Erica Brimacombe Brent Dunington Aaron Heck Susan Johnson Sanja LeBlanc Vanessa Lomas Michael Lonsdale-Eccles Jagmeet Randhawa Robert Tremonti Lee Wang

Document Approval

By signing below, all Stakeholders agree to the terms and conditions outlined in this Agreement.

Name	Role	Signed	Date Signed
Mario Angers	Senior Manager, Systems, UBC IT		
Stephen Lamb	Deputy CIO, UBC IT		
Aarti Paul	Director, Engagement Services, UBC IT		
Don Thompson	CISO		
Matthew Smith	Manager, Research Systems, Advanced Research Computing		

Table of Contents

1. Services Covered

This Service Level Agreement (this "SLA" or "Agreement") is an agreement between the consumer of the Services (the "Client") and UBC IT Systems as the provider of the Services (the "Service Owner")(collectively, the "Parties"), which defines the responsibilities and expectations for use of the Services. The Client must adhere to the standards and policies set out in this Agreement with respect to any usage of the Services. This SLA applies separately to each Client using the Services.

1.1. Included Services

The Services are hybrid cloud services that consist of service offerings from the following Public Cloud Vendors:

- **Amazon Web Services** (AWS) (portfolio of services and offerings);
- **Microsoft Azure** (portfolio of services and offerings);

And the following management portal:

- **CloudBolt Cloud Cost and Security Optimization.**

All service offerings from each Public Cloud Vendor are included in the Services and covered by this Agreement. Additional Vendors will be added as their usage is approved by the university and Service Owner. Services may be removed from the scope of this Agreement at the discretion of the Service Owner or Vendor

With respect to the Services, the Service Owner will provide the Client with the following support, as applicable:

- onboarding to and access to the Services;
- service request fulfilment;
- support escalation and handoff to Vendor;
- advance maintenance notification;
- Cloud Migration Assessment assistance (if required by Service Owner or requested by Client);
- cloud design and architecture consulting and support;
- cloud security consultation; and

- cloud deployment review and recommendation.

2. Definitions

- **Agreement** – this Service Level Agreement ("SLA") document, including any appendices
- **Stakeholders** – individuals in the UBC positions listed under section 3 "Stakeholders"
- **Client** – consumer of the Services
- **Cloud Migration Assessment** – framework for defining readiness of service or team moving to cloud
- **Parties** – the Client and the Service Owner
- **Public Cloud Vendor** – the public cloud vendor(s) represented in this Agreement, as listed under section 1.1 "Included Services"
- **Service Owner** – UBC IT Systems as provider of the Services
- **Services** – all services that are part of the Hybrid Cloud Service, as defined under 1.1 "Included Services"

3. Stakeholders

The following represent the primary Stakeholders associated with this Agreement:

- Senior Manager, Systems, UBC IT
- Deputy Chief Information Officer, UBC IT
- Director, Engagement Services, UBC IT
- Chief Information Security Officer
- Manager, Research Systems, Advanced Research Computing

4. Agreement Overview

This Agreement represents a Service Level Agreement between the Parties for the access, consumption and management of the Services.

This Agreement remains valid until superseded by a revised Agreement endorsed by the Stakeholders, or the cancelation of the Services by either Party.

This Agreement does not supersede current polices, processes and procedures unless explicitly stated herein.

This Agreement incorporates by reference the terms of UBC's agreements with the Public Cloud Vendors listed as part of the Services.

For more information on Public Cloud Vendors Customer Agreements, see the linked information below:

- **AWS** - https://aws.amazon.com/agreement/
- **Azure** - https://azure.microsoft.com/en-us/support/legal/
- **GCP** - https://cloud.google.com/terms

4.1. Periodic Review

This Agreement may be reviewed and updated by the Service Owner after consultation and approval from the Stakeholders. Changes to the Agreement will be communicated to the Client.

5. Fees and Payment

Service Owner will pay the monthly bill for Client's usage to the Public Cloud vendor on Client's behalf and will issue a chargeback to Client's worktag on a monthly basis through Workday.

The Client must provide a valid **worktag** during onboarding for monthly billing through Workday. Authorized signatory with financial responsibility will provide their approval in writing, accepting all fees and charges incurred by the Client.

All fees and charges associated with the Client's account(s), including provisioned services, vendor marketplace charges, and Service Owner brokerage fees, are the Client's responsibility. Service Owner may assess a consultancy fee depending on Client's requirements. Those costs will be communicated in advance and are the responsibility of the Client.

If there is a change in the payment **worktag**, the Client must notify the Service Owner within 14 days and update the payment method accordingly.

If the Client negotiates credits with the Vendor, the Client is responsible for applying the credits to their account. The credits will not be retroactively applied to the Client's account.

In the event of insolvency, the Client's Administrative Head of Unit will be responsible for paying any outstanding charges. If fees remain unpaid for over 30 days, the Service Owner reserves the right to suspend or terminate the Client's account, as outlined in the "Termination" section.

5.1. Cost Dispute Process

Any payment disputes must be submitted within 30 days of billing. Client is responsible for initiating the cost dispute process through the UBC's IT Central Services ticketing system, ServiceNow.

The process for initiating a cost dispute is as follows:

1. The Client submits a ServiceNow ticket and details the reasons for the dispute.
2. The UBC IT Service Centre (ITSC) triages the ticket and assigns it to the Service Owner.
3. The Service Owner contacts the Client and clarifies the details of the dispute.
4. The Service Owner engages with the Public Cloud Vendor regarding the dispute according to the Public Cloud Vendor's cost dispute procedures.
5. The Service Owner manages dispute resolution with Public Cloud Vendor, with the assistance and support of the Client.

The Client is responsible for adhering to the decision of the Public Cloud Vendor regarding the dispute and remains responsible for paying the outstanding amount to the Service Owner even if the Client disagrees with the outcome. If billing inaccuracies are attributable to the Public Cloud Vendor, the Service Owner will work with the Public Cloud Vendor to credit the Client appropriately.

Public cloud usage carries a potentially significant cost risk. It is highly recommended that Clients regularly review cloud spend and set budget alerts to prevent cost overrun.

The Service Owner will assist the Client in managing disputes with the Public Cloud Vendor, but ultimately the Public Cloud Vendor will assess the dispute. The Client or Client's Administrative Head of Unit will be held responsible for all outstanding costs.

6. Termination of Service and Exit Strategy

Either Party may terminate this Agreement for convenience or inability to fulfill obligations in this Agreement. The termination notice will be provided in writing and delivered through the ServiceNow self-service portal as a Service Request with a tracking number. The termination notice must be delivered 30 days in advance of the termination of Services, unless otherwise agreed upon by both Parties in writing.

If the Client is terminating this Agreement, the Client is responsible for providing the Service Owner with a detailed list of all Services that are to be decommissioned and the effective date for Services termination, and is responsible for settling all outstanding charges and fees with the Service Owner.

In the event of non-payment issues, the Service Owner will make a reasonable attempt to contact the Client or Client's department prior to terminating an account. The Client's Administrative Head of Unit is accountable for paying any outstanding charges, and may request the Services remain active if fees are paid.

The Client will remain responsible for all fees and charges that have been incurred through the termination date and is responsible for any fees and charges incurred during the post-termination period.

6.1. Data Ownership and Portability

The Client is responsible for extracting and migrating the Client's data to another platform prior to account termination. If requested by the Client, the Service Owner, at its discretion and if capable, may assist the Client with data extraction or migration. The Service Owner may require a fee for this service.

Determining and setting the effective date for account termination is very important. Once your account is deleted, all data and services are purged as of the date the account is terminated. **The account and data associated with it will no longer be recoverable as of this date.**

7. Security and Privacy Requirements

7.1. "In" the cloud vs. "of" the cloud

The Client is responsible for the security "in" the cloud. The Service Owner or Public Cloud Vendor is responsible for all security "of" the cloud itself.

"In" the cloud refers to the workloads or services which are deployed by the Client in the cloud, or the specific Client-controlled configuration of cloud-based services that they use. **"Of" the cloud** refers to the infrastructure and services offered by a Public Cloud Vendor or, in some cases, the Service Owner.

For example, in the case of EduCloud, the Service Owner is responsible for the security of EduCloud itself (i.e. **"of" the cloud**), but the Client is responsible for the security of workloads or applications deployed within EduCloud (i.e. **"in" the cloud**).

Customer	Responsible for security **in the cloud**	UBC ISS compliance; Privacy Impact Assessment(s); Identity and access management; Data management and protection; Security controls
Service Owner	Responsible for security **of the cloud**	UBC ISS compliance; Identity and access management; Secure connectivity; Service management
Public Cloud Vendor	Responsible for security **of the cloud**	Public cloud infrastructure; Physical security

7.2. Baseline controls and services

When workloads are deployed in non-public cloud vendors such as UBC/BCNET EduCloud, or on-premises at UBC, there are centralized baseline UBC controls and services that provide automated background protection, monitoring and logging. These include, but are not limited to:

- automated scheduled backups (EduCloud);
- inbound internet traffic scanning and protection;
- Centralized Network Monitoring and Logging;
- DNS Firewall;
- hardened OS images; and
- vulnerability alerting.

These controls and services are not available, or in some cases available but not automatically provisioned, for workloads deployed in Public Cloud Vendors. As such, it is the Client's responsibility to consider these controls, or Public Cloud Vendor specific equivalents, in their design of workloads that make use of Public Cloud Vendors.

7.3. Privacy Impact Assessments

All workloads, services or data that are provisioned in, or migrated to, a Public Cloud Vendor must undergo a Privacy Impact Assessment (PIA). British Columbia's *Freedom of Information and Protection of Privacy Act (FIPPA)* requires public bodies such as UBC to conduct a PIA for all new or substantially modified system, process, program or activity that supports University business. See the Privacy Matters website for more information and exceptions to the process.

If you are running an academic research project, you may not need to conduct a PIA. Please refer to https://privacymatters.ubc.ca/frequently-asked-pia-questions for further information.

7.4. Security and Privacy Areas of Responsibility

Area of Responsibility	Client	Service Owner	Public Cloud Vendor
Compliance with UBC's Information Security Standards for all data and deployed workloads, as required by UBC Policy SC14. This includes, **but is not limited to**: EDR, backups, logging, vulnerability management, and patching	✓		
Completion of Privacy Impact Assessments (PIAs), including a cybersecurity consult if required, prior to implementation of any cloud-based applications or services, or a move of data into the cloud	✓		
Identity and access management of applications, workloads, Public Cloud Vendor services, and/or Public Cloud Vendor accounts/tenants (use of UBC's Identity Provider can greatly simplify this responsibility)	✓		
Data classification, encryption (at rest and in-transit), monitoring and integrity. See UBC Information Security Standard U5 for specific guidance on Public Cloud encryption requirements.	✓		
Application security controls (i.e. controls within deployed applications)	✓		
Implementation of Public Cloud Vendor service-specific security controls and security best practices (consult with Cybersecurity for specific guidance)	✓		
Infrastructure and endpoint security controls and connectivity	✓		
Hybrid Cloud Service (UBC specific components) compliance with UBC's Information Security Standards		✓	
Identity and access management of Hybrid Cloud Service		✓	

Area of Responsibility	Client	Service Owner	Public Cloud Vendor
Secure connectivity of UBC campus Private IP networks to all Public Cloud Vendors		✓	
Cloud management portal administration and management		✓	
Public Cloud Vendor infrastructure, including physical security			✓

Up to date version of this table is published on the Hybrid Cloud Service documentation page.

8. General Requirements and Responsibilities

8.1. Client

The Client must:

a) agree to and comply with all of the terms and conditions of this Agreement;

b) provide the Service Owner with a pre-approved workday tag for monthly billing;

c) agree to pay for all Services costs incurred by the Client on a monthly basis;

d) make a reasonable attempt to resolve issues prior to escalating the issue to Service Owner; and

e) be reasonably available to resolve Services related incidents or requests.

8.2. Service Owner

The Service Owner will, with respect to the Services, make best efforts to:

a) provide support to the Client as detailed in section 7;

b) employ knowledgeable and friendly staff;

c) manage the availability and performance of management portal;

d) manage incidents and support requests made by the Client;

e) provide the Client with an escalation path to the Public Cloud Vendor and support the Client to a resolution;
f) provide the Client with detailed consolidated cost planning, management, analysis and optimization support;
g) notify the Client for all scheduled and unscheduled maintenance;
    i. minor maintenance (workload non-impacting) will be communicated 48 hours prior to maintenance;
    ii. major maintenance (workload impacting) will be communicated one business week prior to maintenance;
h) ensure the Services are available twenty-four hours a day, seven days a week;
i) communicate changes to Services to Clients and Stakeholders;
j) perform scheduled maintenance every two weeks (as new releases of cloud management portal are available and required);

The Service Owner is not responsible for the response or quality of support provided by the Public Cloud Vendor.

9. Service Management and Support Levels

9.1. Support Availability

Support for the Services will be available through the Service Owner as follows, based on priority:

Low	Regular office hours 8 a.m. – 5 p.m. PT, contact ITSC
Medium	Regular office hours 8 a.m. – 5 p.m. PT, contact ITSC
High	Regular office hours 8 a.m. – 5 p.m. PT, contact ITSC After hours, contact ITSC and ITSC to escalate to Service Owner

Critical	Regular office hours 8 a.m. – 5 p.m. PT, contact ITSC After hours, contact ITSC and ITSC to escalate to Service Owner and/or Code 3 Coordinator

Incidents may be evaluated for their impact and urgency, and priority may be changed.

9.2. Support for Privacy Impact Assessments and Cybersecurity Assessments

A Privacy Impact Assessment (PIA) is a risk management and compliance review process used to identify and address potential information privacy and security issues, thus avoiding costly program, service, or process redesign and minimizing exposure to potential privacy breaches.

British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) requires public bodies such as UBC to conduct a PIA for all new or substantially modified initiatives. An "initiative" refers to an enactment, system, project, program, or activity that supports University business.

Website: https://privacymatters.ubc.ca/privacy-impact-assessment

Request a PIA *(CWL login required)*

Request a Cybersecurity consult *(CWL login required)*

E-mail: privacy.matters@ubc.ca

9.3. Support Process

Support requests must be initiated by the Client through existing support methods as outlined on the UBC IT Service Catalogue.

9.4. Response Time

In support of the Services, the Service Owner will respond to service-related incidents and/or requests submitted by the Client within the following time frames:

Priority	Incident Acknowledgement (*upon diagnosis and assessment)	Request Fulfillment Acknowledgement and Initial Assessment
Low	1 Business Day	< 5 Business Days
Medium	4 Business Hours	< 3 Business Days
High	< 30 minutes	< 2 Business Days
Critical	Immediately	1 Business Day

9.5. Vendor Support, Performance and Availability

The Service Owner has no control over the performance and availability of the services provided by the Public Cloud Vendors, as such, makes no guarantees for the service levels provided by the Public Cloud Vendors.

Public Cloud Vendors

For more information on service levels provided by the Public Cloud Vendors, see the linked information below:

- AWS - AWS Service Level Agreements (amazon.com)
- Azure - Service Level Agreements – Home | Microsoft Azure
- GCP - Google Cloud Platform Service Level Agreements

Up to date information with respect to available Vendor Service Level Agreements and Vendor contact methods are available on the Hybrid Cloud Service catalogue page (Insert link when available).

9.6. Cloud Migration Assessment and Consults

The Service Owner will provide access to the Cloud Migration Assessment self-assessment document as part of onboarding the Client to the Services. A detailed engagement can be requested (or may be required) for Clients who are seeking complex or enterprise-level Services. The Service Owner will outline any additional fees that may be incurred by the Client as a result of the additional consult and implementation engagement.

Cloud migration readiness assessment is a critical step before moving your applications, services, and data to a cloud environment. It involves evaluating your organization's existing infrastructure, applications, processes, and people to determine how well-prepared you are for the migration. A thorough assessment helps identify potential challenges, risks, and opportunities for optimization, ensuring a smoother and more successful transition to the cloud.

9.7. Licensing in Public Cloud

The Client acknowledges that the use of certain software and operating systems in the public cloud may require valid licenses from the software vendors or licensors. The Client is responsible for ensuring compliance with all applicable software agreements, terms and conditions, including obtaining the necessary licenses for software deployed in the public cloud environment. Portability of software licenses between on-premises and public cloud is to be validated by the Client.

Software licensing in the cloud requires careful attention and understanding from Clients. It is crucial to not assume that software licenses obtained for on-premises use automatically extend to the public cloud environment.

Clients should review and comply with software license agreements to ensure compliance in the public cloud.