STORAGE OF AND ACCESS TO CUSTOMER DATA POLICY

1. Scope

1.1 This '*Cyferd – Storage of and Access to Customer Data Policy*' (this "**Policy**") applies to the storage of and access to Customer Data within the Cyferd Perimeter and the provision of the Database Services. This Policy is made in connection with the provision by Cyferd Inc. ("**Cyferd**") of Access to the Cyferd Product to its customers (including those whose Access to the Cyferd Product is/ was procured through a Cyferd Partner) (in this Policy each a "**Customer**").

1.2 In this Policy the "**Agreement**" means, in respect of the Customer in question, the master services agreement known as '*Cyferd – MSA (A) – 1 August 2024'* entered into/ accepted by that Customer. The online version of the Agreement where accepted being found at https://cyferd.com/cyferdcomm/us.

1.3 This Policy is a Cyferd Policy and applies to, forms part of and is supplemental to the Agreement. The terms of Agreement shall apply to this Policy and are incorporated herein, *mutatis mutandis*, to this Policy.

1.4 For each Customer, this Policy together with the applicable Order Form, the Agreement, the other Cyferd Policies and any other applicable document that forms part of and/or is supplemental to the Agreement from time to time, applies to the subject matter of that Order Form and that Customer's Access to the Cyferd Product.

1.5 Unless otherwise noted or where the context otherwise requires, all capitalized terms used herein shall have the meanings set forth in the Agreement and the definitions document known as '*Cyferd – Definitions re MSA (A) – 1 August 2024*' (https://cyferd.com/cyferdcomm/us).

1.6 In addition, in this Policy the following words and expressions shall have the following meaning unless the context otherwise requires:

"**the Annexure**"	the document annexed to this Policy at '*the Annexure*' which is an '*Overview of how the 'Cyferd Platform' operates*' as amended from time to time by Cyferd
"**Cyferd Perimeter**"	the boundaries of the Cyferd Product (namely the '*Cyferd platform*') within which Cyferd takes responsibility (on the terms and subject to the conditions of the Agreement with each Customer) to provide service to Customers (namely Access to the Cyferd Product via Tenancy(ies)) further details of which are set out below in this Policy, **the Annexure** and Cyferd's **Hosting Policy** (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended by Cyferd from time to time)
"**List of Sub-Processors**"	means the latest version of the list of Sub-Processors used by Cyferd, as amended from time to time by Cyferd, which as at Order Acceptance is available at https://cyferd.com/cyferdcomm/us

1.7 The following terms defined in Cyferd's **Data Protection Policy** (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended by Cyferd from time to time) shall have the same meaning in this Policy: "**Controller**", "**Hosting/ Data Storage Arrangements**", "**process**", "**processing**", "**Processor**", "**Protected Data**", "**Site Reliability Engineering**", "**Sub-Processor**".

2. Last Updated

This Policy was last updated on 1 August 2024. For previous versions of this Policy see https://cyferd.com/cyferdcomm/us.

3. Changes to this Policy

3.1 ***For any person who is not a Customer at the time of such posting*** - Cyferd shall, at its absolute discretion, be entitled to amend this Policy or any part of it by posting an updated version of this Policy at https://cyferd.com/cyferdcomm/us and such updates will be effective upon such posting or, if later, the 'Last Updated' date specified in such updated version of this Policy.

3.2 ***For any person who is a Customer at the time such Update Notification is made*** –Cyferd may at its absolute discretion make, and notify the Customer of, updated versions of this Policy by notifying the Customer of any such Update(s) by way of Update Notification in accordance with the Agreement. Such Update(s) will be effective in respect of the Customer in question in accordance with the applicable provisions of the Agreement.

3.3 If Cyferd makes any amendments to this Policy, it will change the 'Last Updated' date in **paragraph 2** above in such updated version of this Policy.

4. The Database Services

4.1 Subject to any special provisions in any Order Form(s) which relate to a Customer's Agreement, the Agreement contains Cyferd's obligations to provide the Database Services. In particular the provision of the Database Services:

4.1.1 will be performed with reasonable care and skill by Cyferd;

4.1.2 are subject to the terms and conditions of this Policy; and

4.1.3 (to the extent applicable) are subject to the **Hosting Policy**, the **Data Protection Policy** and any other relevant Cyferd Policy (https://cyferd.com/cyferdcomm/us),

and time shall not be of the essence in respect of the provision of the Database Services.

4.2 Refer to **the Annexure** for details as to how storage of Customer Data works within the Cyferd Perimeter (including the Hosting/ Data Storage Arrangements). Storage related details appear in most sections of **the Annexure** so it is recommended to read the whole of **the Annexure** in this regard. By way of summary it provides:

4.2.1 The Cyferd Product uses several technologies to store managed data for the Customer in respect of each of that Customer's Tenancies. These are also implemented in a multi-tenant manner using shared storage infrastructure.

4.2.2 Each '*Primary Datacenter*' and '*Secondary Datacenter*' includes a 'storage' segment where the Customer Data (in respect of each Tenancy) and other data is stored.

4.2.3 The Customer is responsible for providing the authentication service for its Authorized Users.

4.2.4 Cyferd manages the availability of Customer Data of a Customer (for that Customer's Tenancy(ies) in question) within the Cyferd Perimeter.

4.2.5 Within the '*Tenant Catalog'*, the details of each Customer's '*DataStore'* (for that Customer's Tenancy in question) are recorded. Each '*DataStore*' is implemented as a separate database with its own '*Credentials*' that permit access only to that database and not to any other Customer's database or any other database in respect of any other Tenancy

4.2.6 Authorized Users can access these '*DataStores'* only via the '*Compute Tier'* interfaces. Cyferd staff are not permitted to access the content of the '*DataStores'* unless authorized by the Customer in question as an Authorized User

4.2.7 The '*DataStores'* are stored on volumes that are encrypted using '*Industry common practices within Cloud-hosted Infrastructure*'. Data '*at Rest'* is encrypted

4.2.8 Various technologies are used to manage Customer Data of a Customer (for that Customer's Tenancy(ies) in question). **The Annexure** contains a list in this regard.

4.2.9 To provide '*Resilience'* against failure of infrastructure *within* the '*Primary Datacenter*' location, the '*DataStore'* technologies have been implemented in '*Clusters'* that retain 2 (two) copies of data at the '*Primary Datacenter*' location, and a replica in the '*Secondary Datacenter*' location in case of any Cyferd decision to initiate a '*Disaster Recovery'* scenario.

4.2.10 The '*Image/Document* (*BLOB*)' storage is implemented with bidirectional replication between the '*Primary Datacenter*' and '*Secondary Datacenter*' locations, so that uploaded '*Images/Documents'* and the nightly '*Backups*' are available for restoration from both locations.

4.3 In this regard, details of and the roles of third parties used by Cyferd in connection with the provision of the Hosting/ Data Storage Arrangements (including the Site Reliability Engineering, the provision of infrastructure, the supplier of virtual hardware used for the delivery of the Cyferd Product, the provision of managed services for communication between Cyferd microservices, the provision of '*Databases*', the provision of '*BLOB storage*', storing and inspecting diagnostic logs) are set out in:

4.3.1 the **List of Sub-Processors** (in that regard such applicable third parties also being Sub-Processors); and

4.3.2 **the Annexure**.

4.4 The **Data Protection Policy** applies to the basis on how Cyferd (as Processor) will process Protected Data for a Customer (as Controller) in connection with Cyferd providing Access to the Cyferd Product to that Customer pursuant to the Agreement relating to that Customer. Processing of Protected Data is also relevant in terms of the provision of the Hosting/ Data Storage Arrangements (and hence the Database Services) and the applicable provisions of the **Data Protection Policy** apply in respect of the same.

4.5 The **Hosting Policy** applies to the hosting/ delivery of the Cyferd Product (as defined below) (including a Customer's Tenancy(ies)) and the provision of the Hosting Services (which includes/ is relevant to the Hosting/ Data Storage Arrangements) by or on behalf of Cyferd and the applicable provisions of the **Hosting Policy** apply in respect of the same.

5. Customer Data – additional provisions

5.1 In respect of a Customer, the Agreement applies in respect of:

5.1.1 Cyferd not having any ownership of any Customer Data.

5.1.2 Except to the extent Cyferd has direct obligations under data protection laws, Cyferd not having any control over any Customer Data hosted or stored by Cyferd nor will Cyferd actively monitor or have access to the content of the Customer Data.

5.1.3 It is the Customer's responsibility to ensure (and is exclusively responsible for) the accuracy, quality, integrity and legality of the Customer Data and that its use (including use in connection with the Cyferd Product) complies with all applicable laws and Intellectual Property Rights.

5.1.4 Cyferd routinely undertakes regular backups of the Cyferd Product (including all Tenancy(ies) (which may include Customer Data) for its own business continuity purposes and/or to comply with applicable laws/ regulatory requirements. The Customer acknowledges that such steps do not in any way make Cyferd responsible for ensuring the Customer Data does not become inaccessible, damaged or corrupted. Subject to its direct obligations under data protection laws and to the provisions of this Policy, to the maximum extent permitted by applicable law, Cyferd shall not be responsible (under any legal theory, including in negligence) for any loss of availability of, or corruption or damage to, any Customer Data.

5.2 In respect of a Customer and without prejudice to its rights under the Agreement, if Cyferd becomes aware of any allegation that any Customer Data (of that Customer) may not comply with the **Acceptable Use Policy** (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended by Cyferd from time to time), this Policy, or any other part of the Agreement relating to that Customer, Cyferd shall have the right request the permanent deletion of the same by the Customer or otherwise remove or suspend Access to any such Customer Data from that Customer's Tenancy(ies). Where Cyferd (as a PaaS provider) has other obligations imposed on it by law where compliance with the same requires it to do any other act, deed or thing or omit from doing any other act, deed or thing in connection with any such allegation and/or offending Customer Data, then Cyferd shall comply with such obligations imposed on it by law and the Customer irrevocably and unconditionally consents to and permits the same. Where reasonably practicable and lawful Cyferd shall notify the Customer before taking such action.

6. Failure to comply with/ breach of this Policy by the Customer

Without limiting anything else herein or in the Agreement, if Customer fails to comply with and/or otherwise breaches any term(s) of this Policy, then such failure to comply/breach will be considered to be a material breach by the Customer of the Agreement, and for which Cyferd shall be entitled to, without limitation, exercise all available rights and remedies under the Agreement.

[End of Policy]

THE ANNEXURE

There is annexed hereto an '*Overview of how the 'Cyferd Platform' operates*'.

This document provides an overview of how the Cyferd Platform operates and is intended to be supplemental to and clarify some of the content of the *'Cyferd - Data Protection Policy'*, the *'Cyferd – Hosting Policy'*, the *'Cyferd - Privacy Policy'* and the *'Cyferd – Storage of and Access to Customer Data Policy'*.

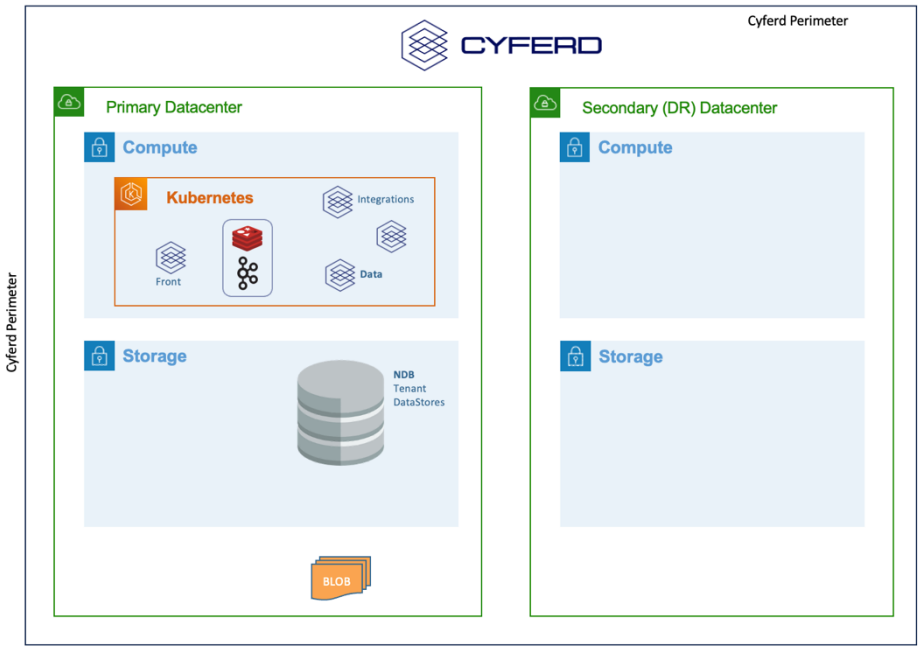
In this document "**Administrator**", "**Access**", "**Authorized User**", "**Customer Data**", "**Cyferd Product**", "**Tenancy**", "**Tenancies**", "**Tenancy(ies)**" have the meanings given to them the definitions document known as '*Cyferd – Definitions re MSA (A) – 1 August 2024*' (https://cyferd.com/cyferdcomm/us).

In this document "**Customer**" has the same meaning given to it in the applicable policy referred to above.

In this document "**Cyferd Platform**" has the same meaning as the Cyferd Product.

Cyferd Perimeter

The "**Cyferd Perimeter**" describes the boundaries of the Cyferd Platform, within which Cyferd Inc. ("**Cyferd**") takes responsibility to provide service to Customers (namely Access to the Cyferd Platform via its Tenancy(ies)) by using and managing many technologies deployed in tiered and secured network segments, operating in several Cyferd-managed locations.

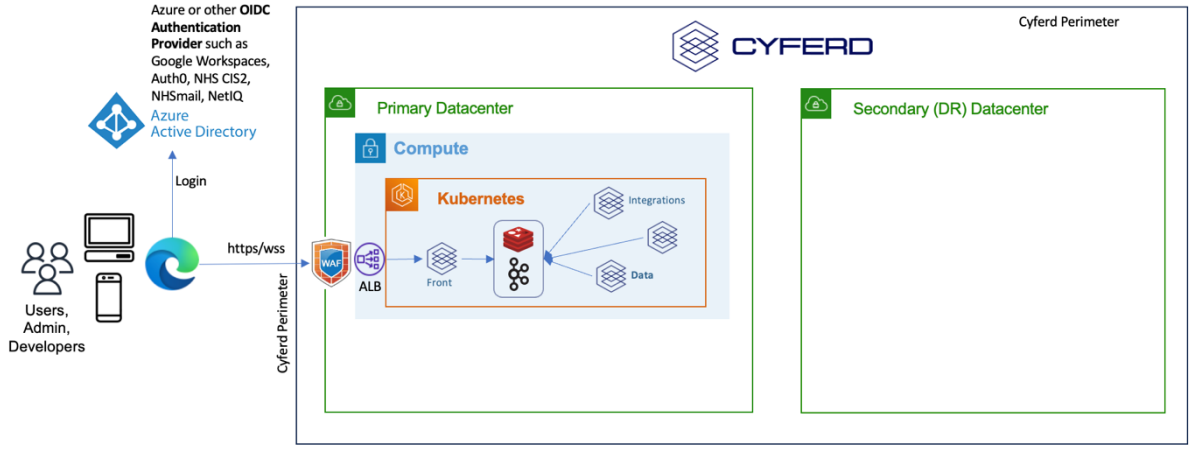


Here we can see that there are two Datacenters, implemented in different locations: the Primary Datacenter is where service is primarily delivered from, containing a 'compute' segment where the Cyferd Platform microservices operate in a Kubernetes cluster, and a 'storage' segment where the Customer Data (in respect of each Tenancy) and other data is stored; the Secondary Datacenter contains similar infrastructure that is maintained in a state of readiness to resume customer service in case (albeit very remote possibility) the Primary Datacenter becomes inaccessible or unsafe to use.

All services *outside* the Cyferd Perimeter are the responsibility of the Customer in question to provide, e.g. Authorized User authentication, and access to other datasources.

Ingress

The Cyferd Perimeter has only one Ingress for any Tenancy. Whether using an HTML5 compliant browser from a desktop (Windows, MacOS) or from a mobile device (iOS, iPadOS, Android), the Cyferd Mobile clients for Android/iOS, or programmatic interactions with the Cyferd Platform from another solution, all traffic is encrypted in transit, and terminated at the edge of the Cyferd Perimeter.



When a Customer's Authorized User browses to that Customer's Tenancy at https://tenant.cyferd.cloud/ the traffic traverses a *Web Application Firewall* (WAF) that performs validation of well-formed https requests and passes it on to an *Application Load Balancer* (ALB) that terminates the Transport Layer Security (TLS aka SSL) encrypted connection before forwarding the user request to a front-end Cyferd Platform microservice running within the Kubernetes cluster.

The initial response to attempting to connect is to redirect the Authorized User to the Authentication Provider that is configured for that Customer's Tenancy. Cyferd requires that the Customer supplied or approved Authentication Provider supports Open ID Connect (OIDC) to provide the authenticated Authorized User's identity to the Cyferd Platform. Popular OIDC Authentication Providers include Microsoft Azure Entra ID, Google Workspaces, Okta/Auth0, ADFS, and several niche providers such as NHS CIS2 and NHSmail (ADFS) are also supported.

The Customer is responsible for providing the authentication service for its Authorized Users.

Upon successful authentication and redirection to the Customer's Tenancy, a 'session' is established and traffic between the browser and the Cyferd Platform continues using a Secured Websocket. Data in transit through the Cyferd Perimeter is encrypted.

Programmatic interactions with the Cyferd Platform follow the same path of connectivity, however authentication may use an API Token that is created and managed within the Tenancy by an appropriately authorized Authorized User, and a RESTful API is supported instead of the Websocket.

Compute & Storage

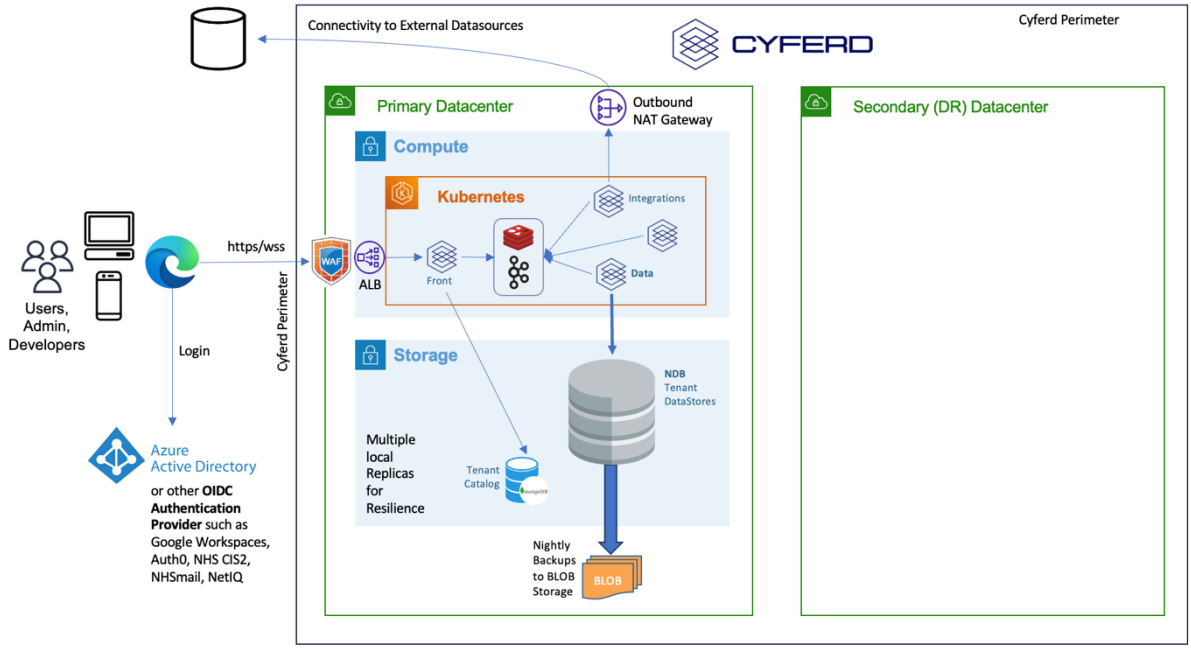
The Cyferd Platform is *multi-tenant*, meaning service to many Tenancies is delivered from shared infrastructure; individual Tenancies do not have individual installations.

Tenant Catalog

All Customers are described in the *Tenant Catalog*, which distinguishes multiple Tenancies by their HTTP Origin **tenant.cyferd.cloud** as used when connecting to the Cyferd Platform. Details in the *Tenant Catalog*, for each Customer (per Tenancy), include:

- the OIDC *Authentication Provider* properties:
    - Issuer Base URL
    - Client ID
    - Client Secret
- Identification of the Administrator of that Customer (*Super Users*) which must be valid identities provided by the *Authentication Provider* above
- *DataStore* properties (for several database technologies used by the Cyferd Platform
    - Database Name
    - Credentials
    - Optional URI if hosted in an irregular location
- *BLOB Storage* properties (used for uploaded *Documents*/*Images* and Backups)
    - Storage Type
    - Bucket Identifier
    - Access Key
    - Access Secret
    - Optional Region if in an irregular location

Cyferd manages the availability of Customer Data of a Customer (for that Customer's Tenancy(ies) in question) within the Cyferd Perimeter.



Compute

Authorized User interactions are enqueued to a pair of components (*Kafka & Redis*) which Cyferd calls "**Rex**" that provide loose coupling and horizontal scalability of the Cyferd Platform microservices.

Each microservice reads specific classes of work from Rex, and either provides a direct service (e.g. data manipulation, notification delivery) or interacts with another resource to query, modify or create data before responding to Rex.

For example (in respect of a Customer and each of that Customer's Tenancies):

- the **Front-End** microservice is the point that Authorized User interactions are submitted through, manages *User Session*, provides *Websocket* connectivity, and submits work to Rex. It also provides the response from Rex to the Authorized User through the *Websocket*.
- the **Data** microservice performs almost all interactions with that Customer's configured *DataStores* (for that Customer's Tenancy in question) – to search, list, modify, create, or delete data.
- the **Channels** microservice performs delivery of *Messages* to Authorized Users as *Mobile Notifications*, *Emails*, and within the Cyferd Platform user interface (for that Customer's Tenancy in question).
- The **Integrations** microservice provides connectivity to datasources or microservices *outside* the Cyferd Perimeter, as configured within that Customer's Tenancy in question, e.g. *Foreign Currency Exchange Rates*, *User Properties* in an external directory.
  Access to publicly accessible datasources is via an *Egress NAT Gateway* on the Cyferd Perimeter; access to private datasources inside the Customer's own '*Perimeter*' requires deployment of the *Cyferd Remote Agent* inside that '*Perimeter*' to implement a *Tunnel* that provide a network access path to those datasources.
- Other microservices perform a variety of utility functions within the Cyferd Platform. Cyferd may, in respect of the Cyferd Platform, redistribute work amongst existing or new microservices and add further optional capabilities at any time without obligation or notification.

Storage

The Cyferd Platform uses several technologies to store managed data for the Customer in respect of each of that Customer's Tenancies. These are also implemented in a multi-tenant manner using shared storage infrastructure.

Within the *Tenant Catalog*, the details of each Customer's *DataStore* (for that Customer's Tenancy in question) are recorded. Each DataStore is implemented as a separate database with its own Credentials that permit access only to that database and not to any other Customer's database or any other database in respect of any other Tenancy.

> *Think of each Customer's DataStore as a book on a shared bookshelf. Ownership of the book is recorded in the Tenant Catalog, and access to open the book requires the credentials that are recorded in the Tenant Catalog. Only Cyferd (as the librarian in this example) has access to the Tenant Catalog.*

Authorized Users can access these *DataStores* only via the *Compute Tier* interfaces. Cyferd staff are not permitted to access the content of the *DataStores* unless authorized by the Customer in question as an Authorized User.

The *DataStores* are stored on volumes that are encrypted using '*Industry common practices within Cloud-hosted Infrastructure*'. Data *at Rest* is encrypted.

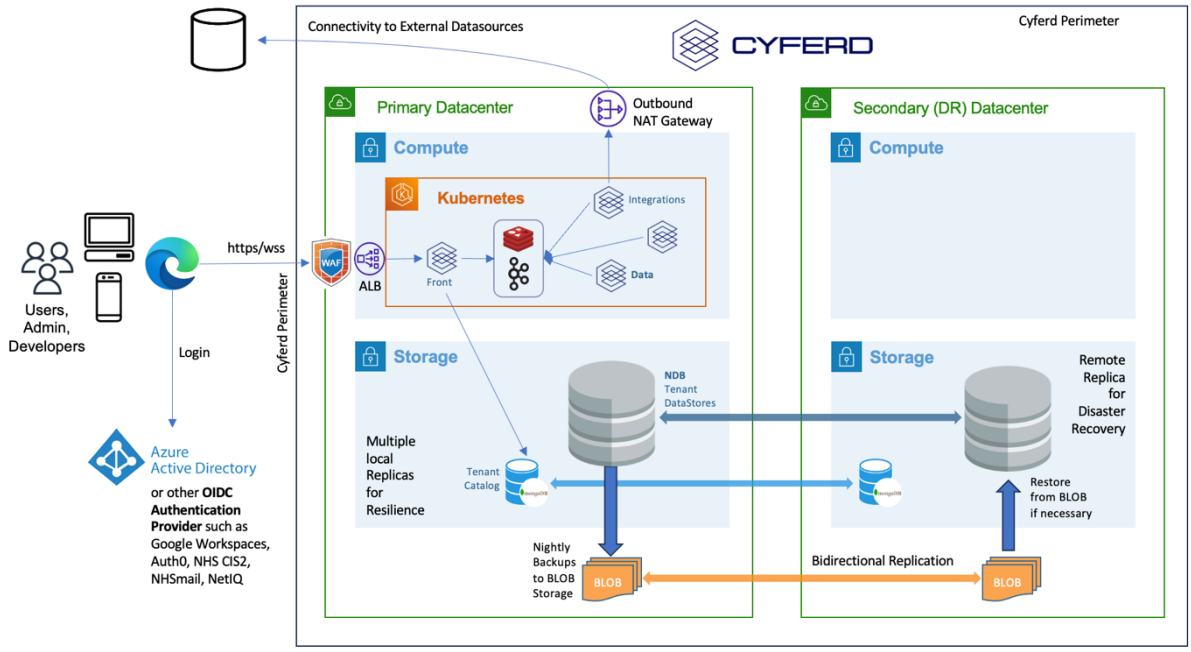
Various technologies are used to manage Customer Data of a Customer (for that Customer's Tenancy(ies) in question). This list describes the main classes of data, but may be modified by Cyferd at any time without notification or obligation:

- **JSON Document**
    - Authorized User *Session* tokens
    - *Transaction Logs* that record *CRUD* operations on managed datasets
    - *Lookup* datasets (values such as Country, Currency, and other categorizations that may be offered in the *User Interface* to be recorded into managed collections of data)
- **Graph & Relational Tables**
    - **Metadata** of objects defined within and used by a Tenancy
        - *Collections* of managed data
        - *Relationships* between *Collections*
        - *Views* that customize the interactions with a *Collection*
        - *Flows* that implement *Business Logic* when interacting with *Collections*
        - *Integrations* – connectivity and authentication details for external datasources that are relevant to the Tenancy in question but not part of the Cyferd Platform
    - **Administrative Data**
        - Properties of Authorized Users who have authenticated into the Tenancy in question or been invited to use it
        - *User Assignments* and *Access Rights*
    - **Cyferd-managed Data**
        - *Collections* (tables)
        - *Relationships* (~ amongst tables)
- **BLOB Storage**
    - *Images* or *Documents* (up to 20MB each) that are uploaded and attached to records in *Collections*
    - Nightly Backups of other *DataStores* within the Tenancy in question

Resilience & Disaster Recovery

Resilience describes the ability to continue service without interruption and may also be known as *High Availability*. When a member of a clustered service must be restarted (e.g. security patches) or replaced (e.g. resized to a larger or newer machine) as part of normal *System Operations* then a resilient configuration provides continuous service without interruption or reconfiguration of clients using that service.

Disaster Recovery (DR) is a process of recovering service to a failover host or environment but is initiated as a consequence of an *interruption of service* due to dramatic failure of connectivity or integrity.



Compute

The *Compute Tier* microservices are implemented in multi-host *Kubernetes clusters* that provide dynamic *Horizontal Pod Autoscaling* based on resource (RAM) utilization. Under heavy utilization, *Kubernetes* will replicate the microservices so that more instances are available to service requests that are on the *Queue*.

A *Kubernetes cluster* can be instantiated in the Secondary Datacenter to leverage local data and restore interrupted customer service in case Cyferd determines or decides that the Primary Datacenter location is inaccessible or compromised.

Storage

To provide *Resilience* against failure of infrastructure *within* the Primary Datacenter location, the *DataStore* technologies have been implemented in *Clusters* that retain two copies of data at the Primary Datacenter location, and a real-time replica in the Secondary Datacenter location in case of any Cyferd decision to initiate a *Disaster Recovery* scenario.

Similarly, the *Image/Document* (*BLOB*) storage is implemented with bidirectional replication between the Primary Datacenter and Secondary Datacenter locations, so that uploaded *Images/Documents* and the nightly Backups are available for restoration from both locations.