<Azure basic operation rules>

Site Administrator (and really as Global Administrator: we don't have a formal Cloud Architect nor DevOps manager, thus site administrator) makes all major decisions on Azure operations - Compute, Storage, Network - within major connection with relative parties and organizational decision chain.

Based on those decisions, operations run with IT Azure support Administrator and that team will have delegated/sub-managing role.
Virtual Network Gateway, Site Gateway, AD- AAD connection (i.e., AAD Cloud Sync), Network, VM, Storage related tasks/jobs and maintenance all under Site Admin's design with IT Azure team communication, management/maintenance.

There are three strong autonomy areas that require its own management rules (and access chain) - Database, App, Data Analytics (CL does not have eligible members on Data Analytics yet)

Azure SQL: Data Architect will make all major decisions. Sr. level Data Engineers will have near full control (except User/APP permission/access level/monitoring setup - this is Azure SQL DBA job)

APP: In Azure APP and Web APP areas (relevant jobs like APP backup plan, application gateway included), Application Manager/Sr. APP Engineer will make all major decisions within connection with Data Architect

Data Analytics: CL would not have cloud data analytics service in near future, but when Databricks is up, then Manager or Sr. level Data Analyst will have autonomy within connection with Data Architect.

BI report: as long as CL BI app is Tableau (not Tableau online), not much change. In due time, review by Data Architect will happen, but Azure SQL - Tableau connection is a major job in short term.

<Azure Dev/Test subscription policy>

- Region: US East (not US East2) and no other region unless a permitted reason exists, but like below, for learning purpose short time (within a few hours) creation is fine

- Resource: for learning purposes, internal data staff will have authorization to make/delete these.
However, remember 2 things:
First, do not waste budget on higher/premium services unnecessarily and remove all relative test resource when done if it was just for learning/testing (cleanup)
so that no more cost incurred unless it's not just for learning, but for persistent development usage.
Second, if it's permanent change, ask before making a change: example) Databricks cluster creation

- Especially expensive services such as Databricks, (Cosmos DB - up to small scale/free range is ok), Azure SQL (in any form except real dev MI given), Synapse Analytics
: 'for personal learning' is not allowed. These things in real environment will come to reality in time, but this is not yet. If you want to learn Databricks, Azure SQL (new), Synapse Analytics, let Data Architect know. That would be encouraged actually.
In Azure subscription policy, Databricks, new Azure SQL and Synapse Analytics will be prohibited. Also, some fundamental resources - including Azure SQL MI - will have resource lock (delete lock and read lock). I want to give as much freedom as possible in Dev environment, but some restrictions are necessary.

- Tags: must be entered for resource group AND each resource (Tags are not inherited from RG to each Resource)
(1) environment: development / test
(2) project: database / app / learning / testing other
(3) creator: Jin (or some degree to identify)
(4) Department: your department (this is optional initially because only Data Team and APP team in dev)

- Naming convention
Virtual machine: cl-vm-test01
VNet: cl-vnet-dev01
Resource group: cl-rg-test01
Storage account: cladlstest01, clblobstdev01, clmsgstdev02
Data factory pipe: cl-adf-pipe-uas-test01
APP service plan: cl-asp-dev02
APP service: cl-app-dev02
Recovery service vault: cl-rsv-dev03

<Azure Permission/Role setup>

There are two types of roles in Azure: AAD roles and RBAC on subscription/resource group/resource hierarchy roles.

1) CLAzureGlobalAdmin@centerlight.org (global admin): Site Administrator, Director/Manager of IT Azure support will have access, but limited way ONLY when global admin rights are needed (example: AAD - AD sync, Management group creation, subscription creation). Unless that, do not use this - keep in safe vault.

2) User Administrator: Site Administrator, Director/Manager of IT Azure support and support team

3) Network Administrator: Site Administrator, Director/Manager of IT Azure support and support team

4) Cloud Device Administrator: Site Administrator, Director/Manager of IT Azure support and support team

5) Security Administrator: Site Administrator, Director/Manager of IT Azure support and support team

6) Azure SQL Administrator (this is not built-in AAD role, formally): Data Architect, Data Manager

7) Application Administrator: Application manager, Sr. APP Engineer

8) Subscription Owner: Data Architect, Site Administrator, Director/Manager of IT Azure support

9) Under subscription, Resource group, each Resource and all access permission management is based on Site administrator's decision, IT support can execute (delegated management), but IT support itself cannot make authorization decisions.

<Azure Resource/service management (therefore, Cost tied)>

Everything in Cloud service is a resource (Azure SQL is a resource, Network is a resource, Data storage is a resource). Therefore, resource management is directly tied to cost.
This means, Resource management is about 'what kind of service(resource) we consume/use' to make business run efficiently, but not only that, how much this (and entire services) costs us? type question and budget tied.

Entire budget is set by company rules - that part we cannot arbitrarily change.
However, within budget limit, 'how are we going to use that?' is a value-type question (is it worth? kind)

Below are basic rules on resource management.

1) Cloud Architect/Site administrator is the Organizational Azure designer, therefore, makes all the fundamental decisions (compute, network, storage) on resources (creation, removal, change) in cooperation with IT Azure support and relative staff in hierarchy of organization chain.

2) Data, Data analytics, APP areas have autonomy as stated previously, but they do not make decisions on 'resource' management in production environments. Resource requests can be made, and Site administrator collects/evaluates.

3) When user requests for Azure resource (for example, storage usage), no matter what the path was (email, talk, chat, IT support request...), go to Site Admin and evaluation process.

4) Resource policies will be made by Site admin. This includes Resource groups, each Resource management policies. IT support can execute (delegated management), but IT support by itself cannot make resource creation/deletion/management decisions.