C3 AI Operational Controls Description

This C3 AI Operational Controls Description describes the roles and responsibilities of You ("**Customer**") and Us ("**C3 AI**") in the deployment of the C3 AI Software, Customer Applications, and Customer Extensions. In the event of a conflict between the terms of this C3 AI Operational Controls Description and the C3 AI End User License Agreement or other agreement with Us governing Your use of the C3 AI Software (the "**Agreement**"), the terms and conditions of this C3 AI Operational Controls Description apply, but only to the extent of such conflict. Capitalized terms used but not defined herein shall have the meaning(s) set forth in the Agreement.

Objective

C3 AI delivers a comprehensive platform as a service (PaaS) for rapidly developing and operating big data, predictive analytics, machine learning, and AI software as a service (SaaS) applications. C3 also offers a family of configurable and extensible SaaS products developed with and operating on its PaaS.

C3 AI offers the ability for Customer to deploy in a dedicated virtual private cloud in a C3 AI managed cloud account, a private cloud deployment where the C3 AI Platform is deployed in Customer's cloud account (e.g. AWS, Azure, GCP), a hybrid cloud deployment where the C3 AI Platform is deployed in Customer's data center and leverages cloud services in Customer's cloud account, or an on-premise deployment where the C3 AI Platform is installed on hardware deployed in Customer's data center.

Irrespective of a private cloud deployment, on-premise deployment, hybrid cloud deployment, or a C3 AI cloud deployment, C3 AI is responsible and accountable for the management, provisioning, system performance monitoring, system availability monitoring, assisting with system and data security monitoring, patching, and continuous content updates (e.g. weather data, documentation, geospatial) of the C3 AI Platform and C3 AI Applications through the term of the contract.

This document details the roles and responsibilities of Customer operations and C3 AI operations teams irrespective of the type of cloud deployment.

C3 AI and Customer Operations Responsibilities

The following RACI (Responsibility, Accountability, Consultation, and Information) matrix summarizes Customer and C3 AI responsibilities for the C3 AI Platform, C3 AI Applications, and Customer Developed Applications.

A RACI matrix indicates responsibility (R), accountability (A), consultation (C), and information (I) by deployment type and task.

Customer-Managed (Private Cloud) Deployment

A private cloud deployment enables Customer to deploy the C3 AI Platform in Customer's cloud account (e.g., AWS, Azure, GCP).

If the C3 AI Platform is deployed in a Private Cloud Deployment model where Customer prefers to manage the cloud infrastructure, the following conditions apply.

1) Customer is required to create the necessary infrastructure as detailed in C3 AI's "Installation Guide" in a dedicated, C3AI-specific, subaccount to which C3 is provided administrative access to Kubernetes cluster to manage the C3 AI Platform.
2) Customer is required to provide hardware (Compute, Storage) and networking infrastructure to meet initial and on-going SLA requirements of operating the C3 AI Platform.
3) C3 manages and operates C3 AI Platform components, C3 AI Platform incident management, provisioning, and upgrades of the C3 AI Platform.
4) C3 AI Operations monitors all components of the C3 AI Platform through its monitoring solution to help optimize and tune the C3 AI Platform. The C3 AI monitoring components are necessary for the C3 AI Platform to function.
5) Customer must provide network access to C3 AI and content providers to enable continuous content updates (e.g., weather, geospatial, documentation).

The below are the operational responsibilities for C3 AI personnel and the Customer in this model.

	C3 AI Operations	**C3 AI Support**	**Customer**	**C3 AI Access level Req'd**
Infrastructure as a Service	C, I	C, I	R, A	No Access
IAM (Identity and Access Management)	C, I	C, I	R, A	End-user Access per below
Network	C, I	C, I	R, A	Access path for business use
Kubernetes as a Service	C, I	C, I	R, A	Edit privileges to C3 AI namespaces
Storage	C, I	C, I	R, A	Debug Break Glass Read-only Access
PostgreSQL RDBMS Service	R, C, I	C, I	R, A	DBA Access
Optional Repositories (conda,pip,npm)	C, I	C, I	R, A	Read-only Access
C3 AI Platform				
Deployment	R, A	I	I	Cluster Admin

Patches & Upgrades	R, A	I	C, I	Cluster Admin
Backup & Restoration	R, A	I	I	Infrastructure Admin
Incident Management	R, A	I	I	Infrastructure Admin
System Performance Monitoring	R, A	I	I	Infrastructure Admin
System Availability Monitoring	R, A	I	I	Infrastructure Admin
System and Data Security Monitoring	R, A	I	R, I	Infrastructure Admin
C3 AI Applications				
System and Performance Monitoring	R, A	C, I	I	Cluster Admin
Incident Management	R, A	C, I	C, I	Cluster Admin
Deployment	R	A, C	I	Cluster Admin
Patches & Upgrades	R	A, C	I	Cluster Admin
Customer Developed and C3 AI Extended Applications				
Performance Monitoring	C, I	C, I	R, A	None
Incident Management	C, I	C, I	R, A	None
Deployment	C, I	C, I	R, A	None
Patches & Upgrades	C, I	C, I	R, A	None
App Admin (e.g., user & content management)			R, A	
Data Classification & Access Control		I	R, A	

Table 1 – C3 AI Application and C3 AI Platform Operating Responsibilities

	C3AI Responsibility	**Customer Responsibility**
C3 AI Platform		
Infrastructure-as-a-Service	C3 AI is responsible for: • Communicating Infrastructure, hardware, network, and storage requirements • Kubernetes Helm charts and container images for the C3 AI Platform and related software components	Customers are responsible for: • Infrastructure virtualization and hardware per C3 AI specifications • Network/subnet configuration per C3 AI specifications • Operating system patches for Kubernetes nodes

		• A file system that C3 AI can use for file storage. For AWS deployments, S3 is used as the file system. For Azure deployments Blob storage is used as the file system. For GSP Google Cloud Storage Service (GCS)is used. • Kubernetes configuration per C3 AI Installation Guide. • Kubernetes cluster administrative access • PostgreSQL RDBMS Database as a service with data backup and disaster recovery setups per C3 AI and Customer requirements • Creating roles and identities for C3 AI personnel (e.g., Ops, COE (Centre of Excellence), Support) that requires access • Repositories that will host C3 AI helm charts, C3 AI container images, conda, pip, npm artifacts. Or internet access to other repositories for those purposes.
C3 AI Platform Installation and Configuration	C3 AI Operations is responsible for the installation and configuration of the C3 AI Server and related software components.	
Upgrades and Patches	C3 AI targets quarterly releases of the C3 AI Platform. C3 AI Operations may also need to apply patches out of cycle to correct or prevent critical system issues. Patching and upgrades are performed on the C3 AI Server and related software. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact. Where possible, C3 AI will provide Customer with lead time consistent with their software license agreement (SLA).	
Monitoring	C3 AI Operations provides 24x7 system monitoring. Monitoring of the C3 AI Platform includes system availability and capacity monitoring.	
Backup and Restoration	Daily backups of data stores including: the key value store, relational, and multi-dimensional data stores.	Daily backups of data stores including: the key value store, relational, and multi-dimensional data stores.

Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventative maintenance. Incident tickets are used to track and assign priority and severity to all incidents.	
C3 AI Applications		
Application Deployment	C3 AI Operations is responsible for the deployment of C3 AI applications.	
Patching and Upgrades	C3 AI targets quarterly releases of the C3 AI applications. C3 AI Operations may also need to apply patches out of cycle to correct or prevent critical system issues. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact. Where possible, C3 AI Operations will provide Customer with lead time consistent with their software license agreement (SLA).	
Monitoring	C3 AI Operations provides 24x7 system monitoring for applications it manages on behalf of its s. Monitoring of C3 AI Applications includes: • Application availability • Data loading and remediation of any data load failures • Work queue monitoring	Customer provides access to C3 AI's cloud monitoring environment.
Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventive maintenance. Incident tickets are used to track and assign priority and severity of all incidents.	
Customer Developed and C3 AI Extended Applications		
Deployment		Customers are responsible for providing and deploying applications they develop or C3 AI applications they have extended.

Patching and Upgrades		Customers are responsible for managing and coordinating their application upgrades and patch releases.
Monitoring		Customers are responsible for the monitoring of applications they develop and deploy on the C3 AI Platform. Monitoring of C3 AI Applications includes but is not limited to: • Application availability • Application response time • Data load activities and remediation of any data load failures • Work queue management
Incident Management		Customers are responsible for the tracking and resolution of issues and incidents for the applications they develop or the C3 AI applications they extend.
Application Administration		Customers are responsible for the management and administration of: • Application users (app users, developers, and administrators) • Application security configuration (permissions, roles, admin groups)
Data Classification and Access Control		Customer is accountable to ensure their solution and its data are securely identified, labeled, and correctly classified to meet any compliance obligation. Distinguishing between sensitive Customer Data and content designed to be private or personally identifiable must be done by Customer. Customer's accountability for data classification and management should be acknowledged as an essential part of the planning process. In such solutions, Customer needs to configure and establish processes to protect both the data and the solution's feature set that protects their data.

C3 AI Managed Private Cloud Deployment

A private cloud deployment enables Customer to deploy the C3 AI Platform in Customer's cloud account (e.g., AWS, Azure, GCP).

If the C3 AI Platform is deployed in a Private Cloud Deployment model where Customer prefers C3 AI to manage the cloud infrastructure, the conditions below apply.

1) Customer is required to create a dedicated C3 AI-specific sub-account to which C3 AI is provided administrative access.
2) Customer is required to provide hardware (Compute, Storage) and networking infrastructure to meet initial and on-going SLA requirements of operating the C3 AI Platform.
3) C3 AI manages and operates the infrastructure, backup, incident management, provisioning, patches, and upgrades of the C3 AI Platform.
4) C3 AI monitors all components of the C3 AI Platform through its centralized monitoring solution to help optimize and tune the C3 AI Platform. The C3 AI centralized monitoring component resides in the C3 AI cloud environment and is necessary for the C3 AI Platform to function.
5) Customer must provide network access to C3 AI and content providers to enable continuous content updates (e.g., weather, geospatial, documentation).

The below are the operational responsibilities for C3 AI personnel and Customer in this model.

	C3 AI Operations	**C3 AI Support**	**Customer**	**C3 AI Access level Req'd**
Infrastructure as a Service	C, I	C, I	R, A	Admin level access
IAM	R, I	C, I	R, A	End-user Access
Network	R, I	C, I	R, A	Access path for business use
Kubernetes as a Service	R, I	C, I	C, A	Edit privileges to C3 namespaces
Storage	R, I	C, I	C, A	RW access
PostgreSQL RDBMS Service	R, I	C, I	C, A	DBA Access
Optional Repositories (conda,pip,npm)	C, I	C, I	R, A	Read-only Access
C3 AI Platform				
Deployment	R, A	I	I	Cluster Admin
Patches & Upgrades	R, A	I	C, I	Cluster Admin
Backup & Restoration	R, A	I		Infrastructure Admin
Incident Management	R, A	I	I	Infrastructure Admin

Infrastructure Monitoring	R, A	I	I	Infrastructure Admin
System Performance Monitoring	R, A	I	I	Infrastructure Admin
System Availability Monitoring	R, A	I	I	Infrastructure Admin
System and Data Security Monitoring	R, A	I	R, I	Infrastructure Admin
C3AI Applications				
System and Performance Monitoring	R, A	C, I	I	Cluster Admin
Incident Management	R, A	C, I	C, I	Cluster Admin
Deployment	R	A, C	I	Cluster Admin
Patches & Upgrades	R	A, C	I	Cluster Admin
Customer Developed and C3 AI Extended Applications				
Performance Monitoring	C, I	C, I	R, A	None
Incident Management	C, I	C, I	R, A	None
Deployment	C, I	C, I	R, A	None
Patches & Upgrades	C, I	C, I	R, A	None
App Admin (e.g., user & content management)			R, A	
Data Classification & Access Control		I	R, A	

Table 2 – C3 AI Application and C3 AI Platform Operating Responsibilities

	C3 AI Responsibility	**Customer Responsibility**
C3 AI Platform		
Infrastructure-as-a-Service	C3 AI is responsible for: • Communicating Infrastructure, hardware, network, and storage requirements • Network/subnet configuration • A file system that C3 AI can use for file storage. For AWS deployments, S3 is used as the file system. For Azure deployments Blob storage is used as the file system. • Kubernetes configuration	Customers are responsible for: • Infrastructure virtualization and hardware per C3 AI specifications • AMI, Virtual images, and Operating system patches • Provide C3 AI with administrative access to the environment.

	• PostgreSQL-compatible RDBMS Database as a service with data backup and disaster recovery s • Creating roles and identities for C3 AI personnel (e.g., Ops, COE, Support) that requires access • Internet access to repositories that will host C3 AI helm charts, C3 AI container images, conda, pip, npm artifacts. • Kubernetes Helm charts and container images for the C3 AI Server and related software components	
C3 AI Platform Installation and Configuration	C3 AI Operations is responsible for the installation and configuration of the C3 AI Platform and related software components.	
Upgrades and Patches	C3 AI targets quarterly releases of the C3 AI Platform. C3 AI Operations may also need to apply patches out of cycle to correct or prevent critical system issues. Patching and upgrades are performed on the C3 AI Server and related software. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact. Where possible, C3 AI Operations will provide Customer with lead time consistent with their software license agreement (SLA).	
Infrastructure Monitoring	C3 AI Operations provides 24x7 system monitoring. Monitoring of the C3 AI Platform includes system availability and capacity monitoring.	
Backup and Restoration	Daily backups of data stores including: the key value store, relational, and multi-dimensional data stores.	
Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventative maintenance. Incident tickets are used to track and assign priority and severity to all incidents.	
C3 AI Applications		

Deployment	C3 AI Operations is responsible for the deployment of C3 AI Applications.	
Patching and Upgrades	C3 AI targets quarterly releases of the C3 AI Applications. C3 AI Operations may also need to apply patches out of cycle to correct or prevent critical system issues. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact. Where possible, C3 AI Operations will provide Customer with lead time consistent with their software license agreement (SLA).	
Monitoring	C3 AI Operations provides 24x7 system monitoring for applications it manages on behalf of its customers. Monitoring of C3 AI Applications includes: • Application availability • Data loading and remediation of any data load failures • Work queue monitoring	Customer provides access to C3 AI's cloud monitoring environment hosted and managed in a C3 AI production VPC and account.
Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventive maintenance. Incident tickets are used to track and assign priority and severity of all incidents.	
Customer Developed and C3 AI Extended Applications		
Deployment		Customers are responsible for providing and deploying applications they develop or C3 AI Applications that they have extended.
Patching and Upgrades		Customers are responsible for managing and coordinating their application upgrades and patch releases.

Monitoring		Customers are responsible for the monitoring of applications they develop and deploy on the C3 AI Platform. Monitoring of C3 AI Applications includes but is not limited to: • Application availability • Application response time • Data load activities and remediation of any data load failures • Work queue management
Incident Management		Customers are responsible for the tracking and resolution of issues and incidents for the applications they develop or the C3 AI Applications they extend.
Application Administration		Customers are responsible for the management and administration of: • Application users (app users, developers, and administrators) • Application security configuration (permissions, roles, admin groups)
Data Classification and Access Control		Customer is accountable to ensure their solution and its data are securely identified, labeled, and correctly classified to meet any compliance obligation. Distinguishing between sensitive Customer Data and content designed to be private or personally identifiable must be done by Customer. Customer's accountability for data classification and management should be acknowledged as an essential part of the planning process. In such solutions, Customer needs to configure and establish processes to protect both the data and the solution's feature set that protects their data.

C3 AI Cloud Account

In a C3 AI managed cloud account the cloud services are contracted for by C3 AI and the C3 AI Platform and Applications are operated on behalf of Customer in a virtual private cloud or multi-tenant cloud on Customer's behalf. Customer may be deployed in a multi-tenant environment (shared VPC) or in a private environment (Customer-dedicated VPC).

If the C3 AI Platform is deployed in a C3 AI Cloud Account, the below conditions apply.

1) C3 AI creates a virtual private cloud for Customer.
2) C3 AI manages and operates the infrastructure, backup, incident management, provisioning, patches, and upgrades of the C3 AI Platform.
3) C3 AI monitors all components of the C3 AI Platform through its centralized monitoring solution to help optimize and tune the C3 AI Platform.
4) C3 AI provides continuous content updates (e.g., weather, geospatial, documentation).

Below are the operational responsibilities for C3 AI and Customer in this model.

	C3 AI Operations	**C3 AI Support**	**Customer**	**C3 AI Access level Req'd**
Infrastructure as a Service	R, I	C, I	I	Admin level Access
C3 AI Platform				
Deployment	R, A	I	I	Cluster Admin
Patches & Upgrades	R, A	I	C, I	Cluster Admin
Backup & Restoration	R, A	I		Infrastructure Admin
Incident Management	R, A	I	I	Infrastructure Admin
Infrastructure Monitoring	R, A	I	I	Infrastructure Admin
System Performance Monitoring	R, A	I	I	Infrastructure Admin
System Availability Monitoring	R, A	I	I	Infrastructure Admin
System and Data Security Monitoring	R, A	I	R, I	Infrastructure Admin
C3 AI Applications				
System and Performance Monitoring	R, A	C, I	I	Cluster Admin
Incident Management	R, A	C, I	C, I	Cluster Admin
Deployment	R	A, C	I	Cluster Admin

Patches & Upgrades	R	A, C	I	Cluster Admin
Customer Developed and C3 AI Extended Applications				
Performance Monitoring	C, I	C, I	R, A	None
Incident Management	C, I	C, I	R, A	None
Deployment	C, I	C, I	R, A	None
Patches & Upgrades	C, I	C, I	R, A	None
App Admin (e.g., user & content management)			R, A	
Data Classification & Access Control			R, A	

Table 3 – C3 AI Application and C3 AI Platform Operating Responsibilities

	C3 AI Responsibility	**Customer Responsibility**
C3 AI Platform		
Infrastructure-as-a-Service	C3 AI is responsible for: • Communicating Infrastructure, hardware, network, and storage requirements • Infrastructure virtualization and hardware • Network/subnet configuration • A file system that C3 AI can use for file storage. For AWS deployments, S3 is used as the file system. For onpremises deployments, HDFS is the file system. • Secure administrative access to the environment	
C3 AI Platform Installation and Configuration	C3 AI Operations is responsible for the installation and configuration of the C3 AI Server and related software components.	

Upgrades and Patches	C3 AI targets quarterly releases of the C3 AI Platform. C3 AI Operations may also need to apply patches out of cycle to correct or prevent critical system issues. Patching and upgrades are performed on the C3 AI Server and related software. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact. Where possible, C3 AI Operations will provide Customer with lead time consistent with their software license agreement (SLA).	
Infrastructure Monitoring	C3 AI Operations provides 24x7 system monitoring. Monitoring of the C3 AI Platform includes system availability and capacity monitoring.	
Backup and Restoration	Daily backups of data stores including: the key value store, relational, and multi-dimensional data stores.	
Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventative maintenance. Incident tickets are used to track and assign priority and severity to all incidents.	
C3 AI Applications		
Deployment	C3 AI Operations is responsible for the deploymentof C3 AI Applications.	
Patching and Upgrades	C3 AI targets quarterly releases of the C3 AI applications. C3 AI Operations may also need to apply patches out of cycle to correct or prevent critical system issues. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact. Where possible, C3 AI Operations will provide Customer with lead time consistent with their software license agreement (SLA).	

Monitoring	C3 AI Operations provides 24x7 system monitoring for applications it manages on behalf of its s. Monitoring of C3 AI Applications includes: • Application availability • Data loading and remediation of any data load failures • Work queue monitoring	
Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventive maintenance. Incident tickets are used to track and assign priority and severity of all incidents.	
Customer Developed and C3 AI Extended Applications		
Provisioning		Customers are responsible for providing and provisioning applications they develop or C3 AI applications that they have extended.
Patching and Upgrades		Customers are responsible for managing and coordinating their application upgrades and patch releases.
Monitoring		Customers are responsible for the monitoring of applications they develop and deploy on the C3 AI Platform. Monitoring of C3 AI Applications includes but is not limited to: • Application availability • Application response time • Data load activities and remediation of any data load failures • Work queue management
Incident Management		Customers are responsible for the tracking and resolution of issues and incidents for the applications they develop or the C3 AI Applications they extend.

Application Administration		Customers are responsible for the management and administrations of: • Application users (app users, developers, and administrators) • Application security configuration (permissions, roles, admin groups)
Data Classification and Access Control		Customer is accountable to ensure their solution and its data are securely identified, labeled, and correctly classified to meet any compliance obligation. Distinguishing between sensitive Customer Data and content designed to be private or personally identifiable must be done by Customer. Customer's accountability for data classification and management should be acknowledged as an essential part of the planning process. In such solutions, Customer needs to configure and establish processes to protect both the data and the solution's feature set that protects their data.

Content Updates

The C3 AI Platform and AI Applications have prebuilt integrations, including pre-defined integrations.

Content Type	Data Elements	Frequency
Weather	Temperature Humidity 7-day forecast	Daily
Google	Geocoding and Maps	On-demand
C3 AI Documentation	C3 AI provides monthly documentation updates	Monthly
Developer Tips and Community	C3 AI provides licensed customers access to a community content site providing tips, Q&A, and developer responses.	Monthly