

Second AMENDMENT

This Amendment made and entered into this 5th day of April, 2022, by and between Pinellas County, a political subdivision of the State of Florida, hereinafter referred to as "County," and Carousel Industries of North America, Inc., Exeter, RI hereinafter referred to as "Contractor," (individually referred to as "Party", collectively "Parties").

WITNESSETH:

WHEREAS, the County and the Contractor entered into an agreement on January 12, 2021, pursuant to Pinellas County Contract No. 156-0302-M (hereinafter "Agreement") pursuant to which the Contractor agreed to provide maintenance and repair services of 9-1-1 equipment for County; and

WHEREAS, Section twenty-one (21) of the Agreement permits modification by mutual written agreement of the parties; and

WHEREAS, the County and the Contractor now wish to modify the Agreement in order to provide for additional WAN managed services for network monitoring, at the same prices, terms, and conditions;

NOW THEREFORE, the Parties agree that the Agreement is amended as follows:

1. Incorporate the attached proposal to the Agreement as Attachment G for additional WAN managed services for network monitoring
2. In the event of conflict or inconsistency between the terms and conditions set forth in Attachment G and the terms and conditions set forth in the Agreement, the term and conditions of the Agreement will govern and control.
3. Attachment G will increase the contract by \$116,226.00 for a revised not-to-exceed sum of \$4,344,255.41.
4. The effective date is from March 1, 2022 and the Contractor will provide the services within Attachment G for twenty-two months through December 31, 2023.
5. Except as changed or modified herein, all provisions and conditions of the original Agreement and any amendments thereto shall remain in full force and effect.

Each Party to this Amendment represents and warrants that: (i) it has the full right and authority and has obtained all necessary approvals to enter into this Amendment; (ii) each person executing this Amendment on behalf of the Party is authorized to do so; (iii) this Amendment constitutes a valid and legally binding obligation of the Party, enforceable in accordance with its terms.

IN WITNESS WHEREOF the Parties herein have executed this Second Amendment as of the
day and year first written above.

PINELLAS COUNTY, FLORIDA
by and through its County Administrator



Barry A. Burton, County Administrator

CONTRACTOR:

Carousel Industries of North America, Inc.



Santhosh Daniel (Mar 7, 2022 15:35 EST)

Authorized Signature

Santhosh Daniel

Printed Authorized Signature

VP, Controller

Title Authorized Signature

APPROVED AS TO FORM

By: 

Office of the County Attorney

Managed
Services

ATTACHMENT G

Carousel Managed Services WAN Managed Services

Statement of Services

This document provides a high-level service definition for:
Pinellas County

Effective Date: 3/1/2022

Proposal #: 623827

Presented to: Judith Weshinskey-Price

Presented by: Adam Wright

Architected by: David DeGenova

Disclaimer

This documentation might include technical or process inaccuracies or typographical errors and is subject to correction and other revision without notice. Carousel GIVES YOU THE CLIENT THIS DOCUMENTATION "AS IS." EXPRESS OR IMPLIED WARRANTIES OF ANY KIND ARE NOT PROVIDED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states or jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Table of Contents

Managed Services Agreement	4
Services Overview.....	4
Service Transition	4
Steady State Delivery	5
List of Exhibits in this Agreement.....	5
Pricing	6
One Time Charges (OTC).....	6
Monthly Recurring Charges (MRC)	6
Pricing Assumptions	6
Out of Scope and Service Limitations	7
Signatures	8
Exhibit A – Service Delivery Gateway (SDG)	9
Carousel Secure Service Delivery Gateway	9
Connectivity	9
Infrastructure Requirements.....	9
Connectivity Requirements	11
A Day in the Life of a Managed Services Engineer	11
Remote Access	11
Password Vaulting.....	12
Data Security and Management.....	13
Types of Data Carousel Does Not Collect	14
The Carousel Commitment	16
Exhibit B – Service Transition Details	17
B.1. Planning Phase	17
B.2. Execution Phase	18
B.3. Quality Assurance/Testing Phase	18
B.4. Tuning Phase	19
B.5. Steady State Phase	19
Exhibit C – Steady State Entitlements.....	20
C.1. Monitoring.....	20
C.1.1. Reachability Monitoring	20
C.1.2. Incident & Performance Monitoring	20
C.2. Reporting & Portals	20
C.3. Configuration Management	20
C.3.1 Network Backup.....	20
C.4. Event Management	20
C.4.1 Service Desk	20
C.4.2 Event Capture, Validation and Recording	21
C.4.3 Event Correlation & Suppression	21
C.5. Incident Management (<i>Optimize ONLY</i>)	21
C.5.1 Incident Notification.....	21

C.5.2	Triage & Troubleshooting (<i>Optimize Only</i>)	22
C.5.3	Complex Resolution (<i>Optimize Only</i>)	22
C.5.4	Bug Resolution (<i>Optimize Only</i>)	22
C.5.5	Carrier Management (<i>Optimize Only</i>)	22
C.5.6	Vendor Management (<i>Optimize Only</i>)	22
C.5.7	Incident Escalation (<i>Optimize Only</i>)	23
C.6.	Problem Management (<i>Optimize Only</i>)	23
C.6.1	Root Cause Analysis (<i>Optimize Only</i>)	23
C.6.2	Chronic Problem Management (<i>Optimize Only</i>)	23
C.7.	Patch & Release Management (<i>Optimize Only</i>)	23
C.7.1	Server Patch Management (<i>Optimize Only</i>)	24
C.7.2	Network Device Release Management (<i>Optimize Only</i>)	24
C.7.3	Application Release Management (<i>Optimize Only</i>)	24
C.8.	IT Asset Change Management (<i>Optimize Only</i>)	24
C.8.1	Standard Change Request (<i>Optimize Only</i>)	25
C.8.2	Emergency Change Request (<i>Optimize Only</i>)	25
C.8.3	Complex Change Request (<i>Optimize Only</i>)	25
C.9.	Health Checks (<i>Optimize Only</i>)	26
C.9.1	Security (<i>Optimize Only</i>)	26
C.10.	Continuous Service Improvement	26
Exhibit D –	Service Level Agreement	27
Exhibit E –	Supported Items	29

Managed Services Agreement

This Statement of Services Agreement (the "Agreement") is entered into between Carousel Industries of North America, Inc. ("Carousel"), with an office at 659 South County Trail, Exeter, RI 02822 ("Carousel") and Pinellas County ("Client") at 10750 Ulmerton Road, Largo, FL 33778, United States. The effective date of this Agreement is 3/1/2022 (the "Effective Date"). Where the Effective Date is not defined above, this Agreement will be effective on the date that Carousel countersigns this Agreement.

This Agreement defines Carousel's IT Managed Services ("Managed Services") based upon the Carousel's 7x24 Service Delivery Platform which is driven by tight ITIL alignment from Carousel's US (primary support) and India (secondary support) service delivery centers. For this agreement, Carousel will provide a services transition plan, steady-state services to augment the client's ongoing day-to-day network operations and reduce the internal resources needed to provide operational support.

Carousel is providing Managed Service for a twenty two (22) month term length (3/1/2022-12/31/2023), which includes four (4) weeks of service transition. This term is designed to co-term with the PS Essential and Staffing master agreement.

The infrastructure and services herein are structured to support the Client's current locations, with committed pricing to scale based upon growth or Carousel assuming increased responsibilities at the Client's discretion. Future grow, expansion, or contraction of this agreement can be facilitated through our Change Request (CR) process.

Services Overview

Carousel will provide a services transition plan and steady-state services to augment the Client's ongoing day-to-day IT operations and reduce the internal resources needed to provide operational support.

Service Transition

Carousel will manage and perform the following transition phases in which activities required for delivery are planned, designed and implemented:

- **Planning Phase** —a detailed data-gathering including a series of internal reviews culminating with a transition kick-off meeting.
- **Execution Phase**— quickly get supported items loaded and configured in the monitoring tool, validate connectivity and response
- **Quality Assurance/Testing Phase** - a full quality and testing review of the proposed solution with refinement and enhancements
- **Tuning Phase** - tuning of the environment to eliminate noise, false positives and ensure that the monitoring and reporting functions are optimized and working as expected. Additionally, Carousel will finalize all delivery process and procedures
- **Steady-State Phase**— Carousel will deliver the services specified in this Statement of Services and provide regular reports on performance against agreed upon SLA metrics.

Estimated Service Transition Timeframe

Carousel estimates the entire service transitioning process will be completed within 4 weeks. The estimated timeframe begins when Carousel receives the client required information (inventory details, passwords, response procedures, etc.) Upon engagement of Carousel's Managed Services, we will work collaboratively with your team throughout the service transition process toward steady state support from Carousel's Support Centers. The following high-level schedule and process overview will provide you an understanding of the transition process:

Phase	Weeks			
	1	2	3	4
Planning Phase				
Execution Phase				
QA/Testing Phase				
Tuning Phase				
Steady State (Go Live)				

Please see Exhibit B for detailed service transition description

Steady State Delivery

Carousel offers a bundled approach to service delivery, with the most common services bundled together. The bundles aligned to your agreement are as follows:

- **OBSERVE** – Proactive Monitoring, Event Management, Network Configuration Management and Quality Assurance Reviews
- **OPTIMIZE** – Proactive Monitoring, Event Management, Incident Management, Problem Management, Network Configuration Management, Patch Management, Change Management and Quality Assurance Reviews

Please refer to Exhibit C for Steady State Entitlement Details

List of Exhibits in this Agreement

Exhibit #	Description	Acknowledgement	
Exhibit A	Service Delivery Gateway (SDG)	Initials:	
Exhibit B	Service Transition Details	Initials:	
Exhibit C	Steady State Entitlements	Initials:	
Exhibit D	Service Level Agreement	Initials:	
Exhibit E	Supported Items	Initials:	

Pricing

One Time Charges (OTC)

Service Description	Quantity	Charge	Notes
Managed Services Transition Charges	1	\$ 14,168.00	Due at Contract Signing
Included in above: CI-SDG-MEDIUM - Physical Server (Gateway 1 & 2)	1		
Total: One Time Charge		\$ 14,168.00	

Monthly Recurring Charges (MRC)

Service Description	Months	Monthly Rate	Notes
Steady State Managed Services <ul style="list-style-type: none"> Recurring Monthly Charge 	22	\$ 4,639.00	Managed Services charges commence on 3/1/2022
Total: Twenty-Two (22) Month Recurring Charge		\$ 102,058.00	

Payments are due Net 30. Local, state and federal taxes are not included in the numbers listed above and will be added at time of invoice.

Pricing Assumptions

Carousel's pricing is based on our current understanding of the Client environment, the scope defined in this support agreement, and the assumptions stated below. If during the course of this engagement any of these assumptions prove to be invalid, both parties will agree to execute a change order and revisit the scope of this support agreement.

- Quoted pricing is based upon a 22-month agreement
- Quoted pricing is based on Monthly billing via the Client's purchase order/invoice process.
- All work will be performed remotely from Carousel Operation Centers located in the United States and India.
 - NOTE: If onsite is required, the client currently has an onsite engineer with Carousel via another agreement. While onsite agreement is in place, this engineer will be leveraged for any/all onsite services.**
- Any desk side assistance required to diagnose or resolve infrastructure issues will be performed by Client.
- Client is responsible for ensuring that manufacturer's maintenance and support contracts are maintained for all software and hardware components managed by Carousel.
- Performance issues or application failure due to faulty hardware or improperly configured or faulty software caused by Client is outside the scope of the services agreement and will be the responsibility of Client to remedy. Carousel will make reasonable efforts to work with Client to troubleshoot and rectify problems.
- This proposal is based on a system configuration list and specifications contained within this Statement of Services. Any changes to these specifications may result in new requirements or price changes for this program.

Out of Scope and Service Limitations

- Any project-based work is not included in this Statement of Services.
- We assume that all solutions under this agreement are designed, configured, and implemented correctly and any redesign, reconfiguration, or re-implementation are out of scope.
- We assume that all solutions covered in this agreement are operational and performing at an optimal level and any additional remediation efforts are not covered under the agreement.
- This agreement is a remote managed service offering and by default does not provide on-site support, engineering, and consulting. Any on-site requirements are out-of-scope unless clearly defined in Exhibit C (Steady State Entitlement Details).
- Any custom errors, logs, and/or parameters to monitoring.
- Any customizations to Carousel standard monitoring templates.
- Investigation and analysis of root cause of problems for P3 and P4 issues if applicable.
 - **NOTE: This can be provided on P3 cases as requested by the client**

Signatures

Signature below indicates Client has read and agrees to all Terms and Exhibits of this Statement of Services.

Accepted By: (Client Authorized Signature)

Accepted By: (Carousel Authorized Signature)

On:

Mark Moretti/VP Managed Services

On:

Bill to Address:

Address:

659 South County Trail

Exeter, RI 02822

ATTN:

ATTN:

Service Contracts Dept.

800-401-0760

maintenanace@carouselindustries.com

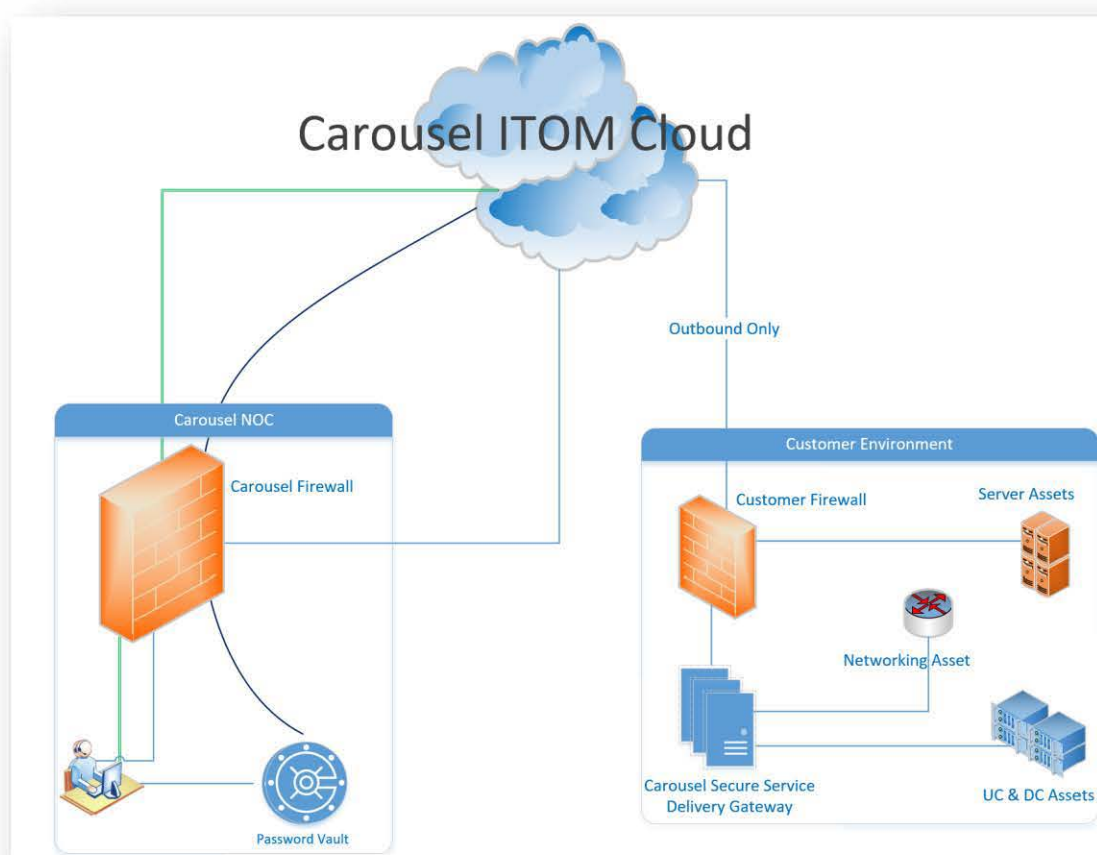
Exhibit A – Service Delivery Gateway (SDG)

Carousel Secure Service Delivery Gateway

The delivery of Carousel's Managed Services requires the implementation of our Service Delivery Gateway (SDG). The SDG is architected to provide device auto-discovery, monitoring, performance management, secure remote access, device level authentication, and tools for improved diagnostic capabilities.

The SDG is deployed with a secure abstraction layer between Carousel's Network Operation Center and the Client's environment ensuring the confidentiality, integrity, and availability of the Client's critical data. Our National Institute of Standards and Technology (NIST) based architecture guarantees the highest levels of authentication, access control, auditability, availability, and scalability.

The Service Delivery Gateway allows Carousel's managed services team to obtain alert, alarms, and performance information from The Client's environment. As abnormal, degraded, and service affecting conditions occur Carousel's service personnel can securely authenticate to the support devices, and investigate, evaluate, diagnose, and resolve detected incidents. In addition, our SDG maintains an audit trail of all access and records all session for detailed auditability.



Connectivity

Carousel's Service Delivery Gateway requires a minimum of two (2) virtual machines for secure connectivity, performance data collection and our managed services support tools. Carousel may also choose to install additional Gateways, Agents or Master Agents for increased services, capabilities and visibility to assets, based on the defined support requirements.

Infrastructure Requirements

NOTE: Within the One-time Charges (OTC), a single physical server platform that will support Service Delivery Gateway number 1 & 2 in a virtual capacity has been included.

Carousel will provide all licensing for the all monitoring and diagnostic tools for the supported environment. In addition, Carousel provide all operational maintenance and support of the Service Delivery Gateway once service transitioning is complete.

Each virtual machine must be configured properly to manage the supported environment. The below are the requirement for the distinct, security hardened gateways:

Service Delivery Gateway 1- (Monitoring Gateway)

Description	A virtual appliance that collects data from the managed environment (Servers, Voice, Switches, Routers, Firewalls, Storage, etc.). The Gateway establishes a secure connection to the ITOM Cloud over the internet via: <ol style="list-style-type: none"> 1. OpenSSH tunnel with 256-bit encryption 2. HTTPS with TLS 1.2
Form Factor	The Gateway is a Virtual Appliance that runs on VMware vSphere and Citrix XenServer platforms.
Operating System	Hardened configuration of Ubuntu Server. Hardening includes the following measures: <ol style="list-style-type: none"> 1. Minimal software is installed 2. All unnecessary services are turned off 3. Applying latest patches and updates 4. All unnecessary users and groups are removed
Access Controls	<ol style="list-style-type: none"> 1. All configuration updates for the Monitoring Gateway are pushed from the ITOM Cloud using a 256-bit encrypted channel created by the Monitoring Gateway. End users do not have access to the Monitoring Gateway. 2. The Gateway password is stored with SHA-512 encryption in a 16-character salt. Single mode login is disabled to prevent unauthorized access or prevent users from entering in single user mode. The Gateway allows only 2 new sessions for every 60 seconds and after 5 wrong passwords, the account locked for 3 minutes.

Infrastructure Size	Virtual Instance Requirements
Up to 25 devices	<ul style="list-style-type: none"> • 2 Virtual CPUs, 2 GB RAM / 40 GB HDD / 1 NIC • Supported hypervisors are VMware ESXi, Citrix XenServer, Microsoft Hyper-V and KVM
Up to 100 devices	<ul style="list-style-type: none"> • 4 Virtual CPUs, 4 GB RAM / 40 GB HDD / 1 NIC • Supported hypervisors are VMware ESXi, Citrix XenServer, Microsoft Hyper-V and KVM
Up to 500 devices	<ul style="list-style-type: none"> • 8 Virtual CPUs, 8 GB RAM / 100 GB HDD / 1 NIC • Supported hypervisors are VMware ESXi, Citrix XenServer, Microsoft Hyper-V and KVM
Greater than 500 devices at single site	<ul style="list-style-type: none"> • Deploy multiple Gateways

Service Delivery Gateway 2- (Support Gateway)

Description	A virtual appliance that is used to support the client's managed environment (Servers, Voice, Switches, Routers, Firewalls, Storage, etc.). The Service Delivery Gateway 2 can only be accessed through secure connection from the ITOM Cloud via RDP.
Form Factor	The Gateway is a Virtual Appliance that runs on VMware vSphere and Citrix XenServer platforms.
Operating System	Microsoft Windows Server 2016 <ol style="list-style-type: none"> 1. Configured with a full tool set for the support of all managed services and devices. 2. Configured with a Just in Time Toolset (JITT) so that services are only active during the time of action needed. This greatly reduces any potential exposure window.
Access Controls	<ol style="list-style-type: none"> 1. Engineers must be granted access to the client environment to gain access. 2. All initial access is funneled through the Carousel ITOM Cloud 3. Secure authentication is provided through API integration with the Carousel Password Vault: (See Password Vault Details below)
Tools (JITT)	Include but are not limited to: RDP, Web Browser (HTTPS), Putty, InformaCast Log Tool, LX Tool, Skype 4 Business, Cisco Agent, Cisco Supervisor, Cisco Attendant Console, RTMT, IP Communicator, configured with a virtual audio driver, CCX Editor, Kiwi Syslog Tool, Translator X, Skype Debugging Tools, Wireshark...

Infrastructure Size	Virtual Instance Requirements
Service Delivery Gateway	<ul style="list-style-type: none"> • 2 Virtual CPUs, 8 GB RAM / 100 GB HDD (Min) / 1 NIC • Supported hypervisors are VMware ESXi, Citrix XenServer, Microsoft Hyper-V and KVM

Connectivity Requirements

The Service Delivery Gateway connects to Carousel's ITOM cloud platform. This connectivity requires that the client enables outbound access from their network. Listed below are the connectivity requirements:

Inbound connectivity: The Carousel SSD Gateway does not impose any inbound connectivity requirements.

Outbound connectivity: The Agent and Gateway 1 need DNS access to resolve *api.opsramp.com*. If the client's organization has firewall policies to limit outbound access to specific IP addresses, then the Agent and Gateway must have access to the specified IP ranges. Gateway 2 is only accessible via the ITOM Cloud, therefore requires no inbound connectivity.

Gateway 1 Outbound Connectivity Requirements		
Description	IP/CIDR	Ports
Data Center 1	63.251.89.0/24	TCP:443/8443
Data Center 2	206.80.7.128/26 140.239.76.0/24	TCP:443/8443
Gateway 2 Outbound Connectivity Requirements		
Description	IP/CIDR	Ports
Data Center 1	63.251.89.0/24	TCP:443/8443
Data Center 2	206.80.7.128/26 140.239.76.0/24	TCP:443/8443

A Day in the Life of a Managed Services Engineer

As an Engineer I will begin by logging into my company provided laptop with my Active Directory (AD) domain credentials. I will start my day by logging into the Carousel ITOM cloud by launching my web browser and go to our HTTPS secured Carousel Industries ITSM portal. If I am on the Carousel domain I will be prompted via Multifactor Authentication (MFA) for my secure token. If I am not on the Carousel domain, I will be prompted for my login information consisting of my email address and AD password. I will then be prompted via MFA for my secure token. I will then access our monitoring platform via HTTPS secure portal. Much like our ITSM portal we will also be leveraging MFA driven authentication. Now, I am securely authenticated into our multi-tenant structured Carousel ITOM cloud. I am prepared to support our clients.

Once an incident or alert is assigned, I can then begin our troubleshooting and remote access process. This begins by accessing the client tenant and based on my role only the assets I am allowed to access will be made available. Once I have identified the asset I need to support, I will launch a secure remote access session (e.g. SSH, RDP, HTTPS). All sessions are recorded and archived for audit purposes. Leveraging a secure API connection back to our enterprise password vault that is encrypted via AES 256 our monitoring platform retrieves the proper credentials for the asset I am supporting. This API validates that I should have access to this asset. Any credentials retrieved from the vault are obfuscated and are not cached. Once my access is validated in the password vault, the asset service account information is then passed to the device and the connection is made with no further interaction from me.

Our gateway is designed to use Just in Time Tools (JITT). JITT is a device hardening technique that keeps minimal services running to only allow the initial RDP connection only from the Carousel ITOM Cloud. Once a connection is established only the tools I specifically require will be enabled. Once I have completed my work and log out, the gateway will return to its hardened steady state.

Best in class security practices are the foundation of the Carousel ITOM Cloud. Every user and system interface is tracked, logged and archived. Every interaction from incident updates, to accessing the client's assets leaves an audit trail that can be retrieved and reviewed.

Remote Access

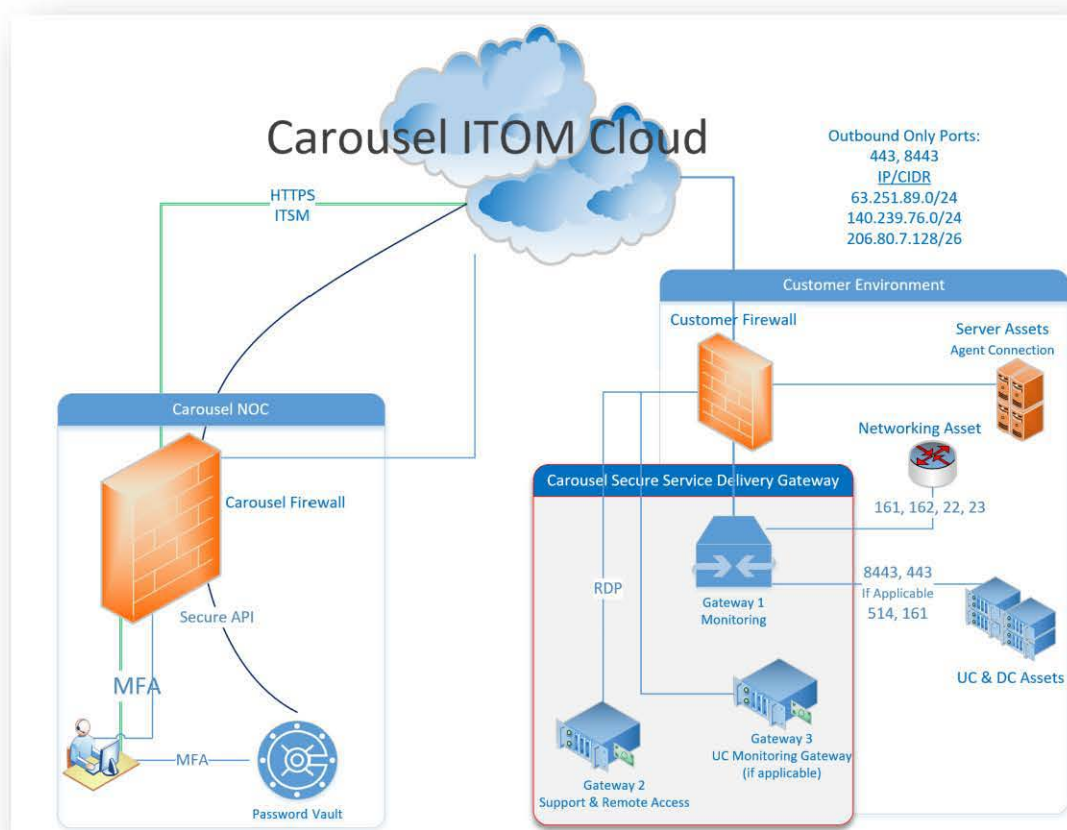
The Service Delivery Gateway gives our engineers a secure, one-click access to the support devices, including those in remote data centers that require connecting to remote access servers first and then hopping to the target devices. Secure Remote Access centralizes the management of all client credentials and access controls, so Carousel's engineers don't have to authenticate themselves at each stage of a remote access. It handles all login and authentication steps automatically, giving us one-click secure access to our client's remote resources.

Engineers assigned to support our client's environment are required to use an individualised 12-character minimum password. Additionally, each login requires a secondary authentication factor so that secure user authentication is assured. All interactions with our client's environments are logged, audited and recorded. This coupled with a single service account with a randomized password of least 15-characters or more, on our client's supported environment. Leveraging machine to machine secure API, the device level service account remains hidden from the engineering and support staff. This ensures that even an authorized engineer will not know the service account information that was used to make the connection.

The Service Delivery Gateway maintains a complete record of 'who', 'what' and 'when' of password access and provides intuitive reports on entire password management scenario in the supported enterprise. Carousel provides Real-time alerts on the occurrence of various password events through integration with Carousel's Security Information and Event Management (SIEM) solutions. Privileged sessions launched from the Service Delivery Gateway can be completely video recorded, archived and played back for forensic audits.

We take our clients trust seriously and execute measures to protect the sharing of service account credentials and resource access. All service accounts information is stored in our enterprise password vault.

Remote Access and Support Diagram



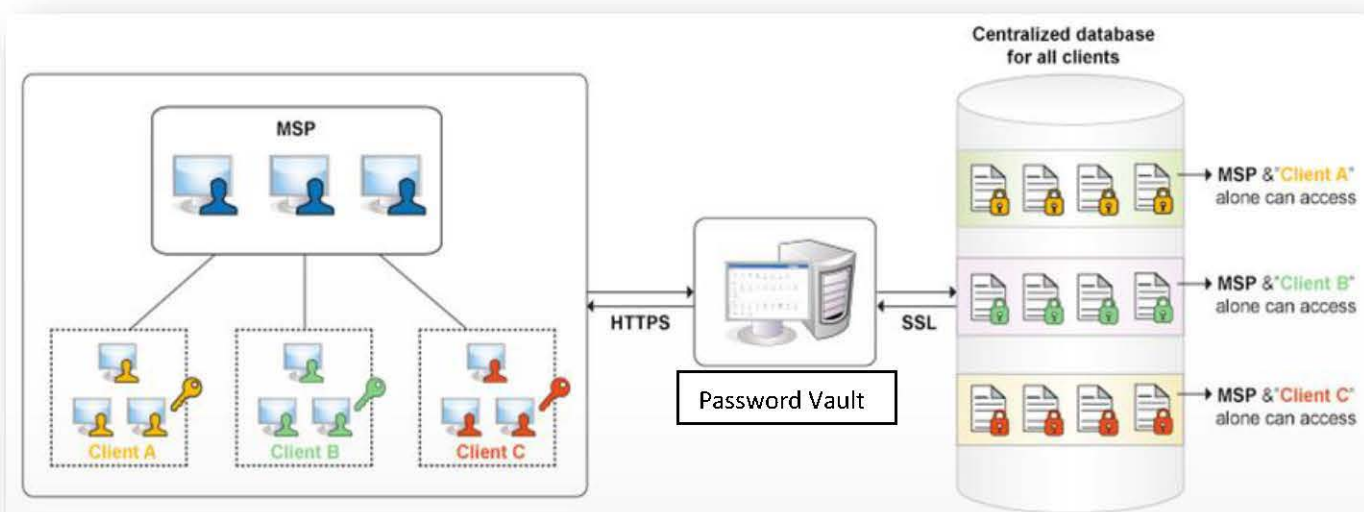
Password Vaulting

Carousel's Service Delivery Gateway provides an enterprise password vault solution to protect IT assets in the supported environment. The Enterprise Password Vault is a platform for secure storing and managing of shared sensitive information such as enterprise-passwords, privileged accounts, shared accounts, documents and digital identities in a centralized repository. This ensures Carousel can offer critical data protection above and beyond our customer's best practice security guidelines for sensitive information.

Secure Features include:

- Confidentiality, Integrity & Availability
 - High Availability Architecture
 - Passwords & sensitive data are encrypted using AES 256-bit encryption.

- Multi-Factor Authentication
 - Enforced MFA for logging in to the Password Vault.
- Automated Password Resets
 - Reset the passwords of remote resources when required or automatically through scheduled tasks.
- Enforced Password Policies
 - Enforce industry standard and custom password policies.
- Comprehensive Audit Trails & Reporting
 - Complete record of 'who', 'what' and 'when' of credential access.
- Real-time Notifications, SIEM Integration
 - Real-time alerts on the occurrence of various password events with integration with Carousel's Security Information and Event Management (SIEM) solutions
- Industry Standard Secure API integration
 - RESTful API and XML-RPC API allow for application to application interaction and database instances.



Data Security and Management

Data Center Overview

The Carousel Secure Service Delivery Gateway is comprised of the various components running on company and partner infrastructure and in Data Centers that are owned and operated by 3rd party 'Best in Class' Data Center providers. Data Center providers are publicly listed U.S. firms.

Locations	Data center 1: Santa Clara, California Data center 2: Rancho Cordova (Sacramento), California Data center 3: Dallas, Texas Data center 4: Chicago, Illinois
Security Certifications	Security certifications that these data centers have include: SOC Certifications, ISO7001, PCI DSS and others.

Data Collection

Carousel collects and stores only data necessary to perform IT operations management and support functions on devices that it manages.

Type of Data	Data Collected	Data Storage and Security
Performance Statistics	System level information necessary to monitor the performance and health of managed devices: <ul style="list-style-type: none"> • CPU and Memory utilization • OS Events • Hardware Events 	Device performance statistics are stored only in the Carousel ITOM Cloud. The Agent and Gateway collect and transmit this data to the Carousel ITOM Cloud

Events and SNMP Traps	Operating System events and traps generated by SNMP agents.	The Monitoring Gateway and Agent processes events and traps locally and send resultant alerts to the ITOM Cloud via a secure channel. Raw event data is not stored in the Cloud.
Device Configuration and Device Metadata	System level information necessary to asset device configuration status: <ul style="list-style-type: none"> DNS Names Make/Model OS and Application Configuration Parameters 	The Monitoring Gateway and Agent sends configuration data to the ITOM Cloud via a secure channel.
Device Credentials	Credentials (username / password) necessary to discover devices, access performance and configuration data, and log into devices to run automation scripts.	Device credentials are stored in the Carousel Enterprise Password Vault, using industry standard FIPS level encryption.
Support Information	Information needed to support Incident, Problem and Change Management <ul style="list-style-type: none"> Contact Information Asset Information 	

Types of Data Carousel Does Not Collect

Carousel does not collect, and has no means to collect, any data processed by applications that Carousel monitors. Examples of such data includes data within database tables, content of application transactions, user credentials of applications, etc.

Data Management

Data Classification	Carousel only collects and stores data required for IT operations management on devices and applications managed by it. Data that Carousel collects is limited to device performance metrics, performance and failure events, and configuration information.
Data Isolation	Carousel implements strict multi-tenancy controls to ensure data access is strictly isolated between customers.
Data Encryption (in-flight)	All data transmitted between the Carousel Agent/Gateway and the Carousel Cloud is encrypted with SSL and TLS/SSH (for gateway).
Data Encryption (at-rest)	Device credentials stored in the Carousel cloud is encrypted using 1024-bit RSA encryption.
Authentication	Carousel Cloud offers SAML and OAuth2 based authentication. Carousel additionally supports third party authentication services such as OneLogin, Okta and ADFS. Carousel Cloud offers two-factor authentication.
User Access Management	Carousel has extensive role-based access controls. Carousel access controls are granular to the managed device, user, and feature.
APIs	Carousel provides REST APIs for integration with Carousel cloud. Carousel REST APIs are backed by OAuth2 based authentication.
Regulatory and Compliance Requirements	Carousel does NOT collect any Personally identifiable information (PII). Carousel is hosted in co-location facilities provided by two U.S based data center providers. Each provider has their own security certifications including SAS and SSAE.

Data Security

Carousel supports an extensive set of security features to ensure that management data collected by Carousel is accessed only by authorized users.

Encryption	All sensitive data is encrypted to FIPS (Federal Information Processing Standards) in Carousel. Customer data (inventory, metrics, alerts, and tickets) is logically partitioned and stored under the client tenant. Customer data is accessible, via Role-based Access Controls (RBAC) only to authorized users of the tenant.
Role Based Access Control (RBAC)	Carousel supports comprehensive Role-based Access Controls. Users' access to devices and actions within Carousel is controlled by fine-grained permissions. Permissions are assigned based on users' roles.

Identity Management	<p>Carousel provides multiple options to manage user identity:</p> <ul style="list-style-type: none"> • Built-in user management system within Carousel • Integration with Microsoft Active Directory • Integration with single sign-on service OneLogin via SAML 2.0.
Authentication and Passwords	<p>Carousel follows standard practices for passwords:</p> <ul style="list-style-type: none"> • NIST based rules of password strengths • CAPTCHA code-based validation • Automated lockout after multiple unsuccessful login attempts • Carousel supports two-factor authentication using, FortiToken, Google Authenticator and Yubico YubiKey.

Data Retention

Definitions	
Active and Inactive Devices	<p>A managed device is considered inactive if it meets all of the following criteria for 90 consecutive days or longer:</p> <ul style="list-style-type: none"> No metrics are collected. No consoles are launched. No jobs, scripts, patches, or anti-virus updates are applied. <p>An active device is one that does not meet the above criteria.</p>
Active and Inactive Clients	<p>A client is considered inactive if they meet one of the following criteria for 90 consecutive days or longer:</p> <ul style="list-style-type: none"> Client has no active devices. Client has been marked as inactive within Vistara. <p>An active client is one that does not meet the above criteria.</p>

Type of data	Criteria	Retention
Devices	Inactive devices	90 days
Clients	Inactive clients	90 days
Tickets	Closed tickets	12 months
	Open tickets	For as long as ticket is open
Metrics	Metrics collected from managed devices	12 months
Alerts	Suppressed and closed alerts	90 days
	Open alerts	For as long as alert is open
Graphs	Graphs with no data	15 days
Reports	Recurring reports	Last 5 generated reports
	One-time reports	90 days
Job, Script, and Patch Activity	Jobs results	90 days
	Custom script results	90 days
Patches	Missing patches, once detected, but not re-detected for 180 consecutive days or longer	90 days
Secure Console Recordings	Rolling history of console recordings for each device.	90 days

Upon contract expiration Carousel inactivates the client "tenant" in the Carousel ITOM Cloud. An inactive tenant's instance inventory, metrics, and alerts data will be available in passive state, however, monitoring, alerting and other management functionality is no longer available.

Based upon an agreement between Carousel and the Client, Carousel will delete all the tenant information from the Carousel ITOM Cloud. Due to a ninety-day data archival retention policy, deleted tenant data will be available in archival repository for ninety days.

The Carousel Commitment

The Carousel Service Delivery Gateway provides secure end-to-end visibility and remote access into your most critical managed systems' health and performance. We support the world's most complex and dynamic environments and can monitor any element or service in your data center or cloud.

Our NIST based world-class practices, manage events from across your network with a laser focus on your most critical managed infrastructure, ensuring the highest levels of system security, integrity and availability for your business.

Exhibit B – Service Transition Details

Carousel's service transition management methodology is based on the Project Management's Institutes' Project Management Body of Knowledge, the most comprehensive and globally recognized standard for project management. It outlines the critical path to planning and managing the service delivery lifecycle and is tailored to meet the Client's service transition requirements as necessary. It includes tools and templates used to manage Scope, Risk, Quality, Communications, Human Resources, Procurement, Time, and Cost. Carousel's service transition activities, based on the information received from the Client, are proposed to be executed in the following phases:



Note: During Service Transition, Carousel will provide best effort reactive support for incidents. Service level metrics will be enforced ninety (90) days after service transition acceptance.

B.1. Planning Phase

Carousel will begin the service transition with a series of internal reviews culminating with a transition kick-off meeting. Carousel's Due diligence conducted during the Planning Phase plays a vital role in understanding, documenting and delivering the proposed managed services, as per its expectations and requirements. Carousel welcomes the opportunity to perform a collaborative due diligence session to assess the client IT landscape.

The objectives of the Planning Phase include:

- Conduct Service Transition kick-off meeting with Client
- Agreement Review
 - Confirm Scope of Services
 - Establish Priorities and Timelines
 - Review Supported Technologies
 - Validate Locations Supported
 - Items Supported
- Response Procedures/runbook
 - Review and Define Escalation and Prioritization Process
 - Collect Escalation Matrix details (Off Hours & Business Hours)
 - Review Vendor Management Requirements (LOA)
 - Review and Define Change Management Process
 - Discuss and Review Out-of-Scope Service Request
- Review the Project Timeline
 - Confirm Communications Plan / Contacts
 - Schedule Weekly Status Meetings
 - Take and publish Meeting Minutes
 - Establish Transition Steering Committee
- Design and formulate a knowledge transfer calendar and plan
- Review Monitoring tool requirements
 - Review Service Delivery Gateway Requirements
 - Review and Plan Service Delivery Gateway Deployment
 - Review Access Credentials
 - Security considerations
- Readiness Assessment

B.2. Execution Phase

Carousel's Service Transition Execution phase is where the plan designed in the prior phase is put into action. The purpose of the Execution phase is to deliver the project expected results (deliverable and other direct outputs). Typically, this is the longest phase of the Service transition lifecycle, where most resources are applied.

The execution team utilizes all the schedules, procedures and templates that were prepared and anticipated during the Planning phase. The Execution Phase is not a blind implementation of what was written in advance but a watchful process where doing things goes along with understanding what is being done to ensure execution corresponds to what was intend and expected.

The focus for the Execution Phase is to enable the supported environment, activate and configure the supported items, and validate connectivity and response. Here is an overview of what is accomplished during this phase:

- Gather the Technical Environment Support Information
 - Network Connectivity Diagrams
 - ISP Information
 - Custom Tasks and Procedures
 - IP Subnets to perform the discovery
 - SNMP read only string for network Devices
 - Windows Administrator credentials for Windows Servers
- Deployment of Services Delivery Gateway
 - Deploy Service Delivery Gateway
 - Configure Service Delivery Gateway
 - Ensure Bi-directional Communication with SDG
 - Perform Auto-Device Discovery
 - Configure the Identified Devices for Services
- Deploy the basic and advanced templates on managed devices and applications
- Validate the data generated by the monitoring system
- Configure Proactive Management Tasks
 - Patch Management
 - Server re-boot schedule
 - Network configuration back-up schedule
 - Application back-up scripts and scheduling
- Conduct Knowledge Transfer sessions
 - Load Client assets into ServiceNow ITSM System
 - Ensure Client Device Level Entitlement are Mapped to Appropriate Assets
 - Load Client Response Procedures into ServiceNow ITSM System
 - Collection of Standard Operating Procedures
 - Knowledge Transfer Sessions on Client's Environment and Architecture
 - Knowledge Transfer Sessions on Standard and Custom Operating Procedures
 - Knowledge Transfer Sessions on Jobs, Maintenance plans.
 - Identifying and documenting the critical items
- Identify risks and formulate a risk mitigation / readiness plan

B.3. Quality Assurance/Testing Phase

After the completion of the Service Transition Execution Phase, services will be started in a pre-steady state environment. During this phase, Carousel will focus on stabilizing the monitored environment by performing a full quality review and operational assurance testing of the managed solution. Further refinement and enhancements are also elements of this phase. The following are the critical activities performed during the phase:

- Identify devices generating higher than average alerts and provide recommendations to reduce alerts
- Building dependency maps for event correlations and noise reduction
- Build custom automation scripts to reduce noise and improve resolution
- Review the Client environment for potential change recommendation and recommend thresholds adjustments
- Review of existing support contract documentation (i.e. Cisco SmartNet,)
- Review and documentation of existing Carrier circuit ID's
- Validation of the monitoring tools and network connectivity to the Carousel Service Delivery Platform
 - All devices configured into monitoring
 - Development of monitoring dependencies
 - Additional Probes and Agents as required

- Review and update response procedures
- Validate ticket workflow
- Identify gaps and additional requirements

B.4. Tuning Phase

This phase is focused on optimizing the managed environment to eliminate noise, false positives and ensure that the monitoring and reporting functions are working as expected. Additionally, Carousel will finalize all delivery process and procedures which include:

- Finalize escalation notification processes
- Initiate 24x7x365 alert processing, validation and escalation
- Execute Standard Operating Procedures (SOPs)
- Test and Review SLAs
- Review Response Procedures/runbook with the Client to identify any changes.

B.5. Steady State Phase

During steady state support, the Carousel service delivery team incorporates a quality assurance and continuous improvement processes as a proactive component of our managed services offering. Our service delivery team compares month-to-month key performance indicators (KPIs) such as “First to Know” trends, SLA attainment, mean time to resolution measurements, “alert to incident” ratios, “alert to device” ratios, and noisy element analysis to drive continual service improvements. And daily, our team reviews a subset of incidents leading to runbook changes, new runbook development, runbook automation, increased event correlation, and improved alert aggregation. The Quality Assurance Review begins during service transitioning and continues throughout the entire contract lifecycle.

- Provide services as per agreed SLAs
- Monitor alerts 24x7x365
- Perform alert triaging and ticketing
- Escalate incidents
- Prepare new SOPs based on alerts
- Execute proactive management tasks
- Report SLAs
- Plan Service Improvement
- Perform monthly reviews
- Portal credentials and review
- Lessons learned review
- Transition closure meeting

Exhibit C – Steady State Entitlements

C.1. Monitoring

C.1.1. Reachability Monitoring

Our Service Delivery Platform measures network connectivity at regular intervals via ICMP polling (PING) to ensure the monitored elements are reachable on the network from an IP address availability perspective.

C.1.2. Incident & Performance Monitoring

Our Service Delivery Platform monitors identified elements utilizing standard SNMP data collection, SNMP trap receiver, syslog monitoring and available APIs to receive specific information, alerts, alarms, faults and performance data.

Incident & Performance Monitoring provides 24x7x365 monitoring of supported devices for those Products listed in Appendix D with our Service Delivery Platform to help raise awareness of specific events that have the potential to cause a significant adverse impact to business operations.

C.2. Reporting & Portals

Carousel provides the client with access to two web-based portals. Our first portal, service management, provides direct access to our Information Technology Service Management (ITSM) system. Our service management portal provides core features such as reporting issues, submitting service requests, general questions, viewing open and closed tickets, and creating/exporting reports. An extranet will also be provided, with access to shared support documentation and static reports.

Our second portal, performance management, provides direct access to our Information Technology Management (ITOM) system. This web-based portal provides access to real time performance dashboards, KPI management tool and on-demand performance reporting. It will allow the measurement and tracking performance against predefined SLAs, streamline service delivery and better support the business with metrics and analytics

C.3. Configuration Management

C.3.1 Network Backup

Our best practice approach for network device configuration backup is a weekly cadence with immediate backup on a device configuration change. Backups will be stored within our cloud-based service delivery platform and we will maintain the last three months of archived configurations.

NOTE: Configuration Management does NOT apply to the Cisco 4000 Series Integrated Services Routers. These are managed by Frontier (ISP), but we will be provided performance monitoring access.

C.4. Event Management

Carousel provides Event Management functionality from our operations located in the United States and India. Event Management is the process that monitors all alarms, alert, and events related to the operation of the IT environment. Our objective is to detect alarms, alerts, and events, analyses them, and determine the correct control action. Our Event Management function provides a strong foundation for service assurance, reporting, and service improvement. Event management responsibilities include:

C.4.1 Service Desk

Carousel will provide 7x24x365 live access to meet the communication needs of Client IT staff via phone, email or web portal. Our service desk is the focal point for reporting and updating status for existing issues, opening new incidences, and initiating a change or service request.

The Service Desk will:

- Answer incoming calls and capture valid information

- Service request/problem description
- Site and contact information
 - Determine Severity by assessing urgency and impact
- Review emails to understand the issue and contact information
 - Service desk may reach out to sender for clarification or additional information before opening a ticket
- Open ticket and assign to Incident Management, Change Management or Service Request queue
- Review portal requests and validate assignment to appropriate queues.

C.4.2 Event Capture, Validation and Recording

Our Service Delivery Platform monitors for a detectable or discernible occurrence that has significance for the management of the IT Infrastructure. We evaluate the event and record the identified conditions in our Information Technology Management System (ITSM).

C.4.3 Event Correlation & Suppression

Our Service Delivery Platform has a powerful event correlation and suppression engine which uses advanced technology for making sense of a large number of events and pinpoint the few events that require attention. This is accomplished by looking for and analysing relationships between events. Our Service Delivery Platform monitors for detectable or discernible occurrence that has significance for the management of the IT Infrastructure. Carousel will evaluate the event and record the identified conditions in our Information Technology Management System (ITSM).

C.5. Incident Management *(Optimize ONLY)*

Incident Management is designed to help restore normal service operation within a reasonable time to help contain the adverse impact on the Client's business operations, service quality and systems availability. When an incident is opened, it is important that the appropriate priority is assigned to reflect the current service impact. As ITIL defines it, incident priority is primarily formed out of its Impact and its Urgency. There are also additional elements, like size, scope, complexity, and resources required for resolution.

The Impact of the incident is the measure of the criticality of the incident to the business. Traditionally, Impact is tied to the number of users or business processes affected. Urgency is a measure of the necessary speed of resolving an incident.

Based on the assessment of Urgency and Impact, the chart below is leveraged to assign the appropriate Priority level.

		Impact		
		High	Mid	Low
Urgency	High	1	2	3
	Mid	2	3	4
	Low	3	4	4

Incident Classification

Priority	Definition
One (P1)	Occurs when there is critical impact to the business operations and urgent action is required to resolve the incident. For example, network is unavailable, a site is partially down and/or impacting a significant part of the business operations and no work-around is available.
Two (P2)	Occurs when performance of a supported service or environment is severely degraded causing a high to medium level of impact. Functionality may be noticeably impaired, but most business operations continue. P2 incidents have a high to medium level of urgency requiring responsiveness, the activation of SOPs, on-call procedures, and invoking vendor support.
Three (P3)	Occurs when operational performance is impaired while most of the business operations remain functional. Limited devices (PC, printer, terminal, extension) are not operational. There is degradation of services although issue is not mission-critical. P3 incidents are responded to using standard operating procedures and operating within the standard workflow and operational structures.
Four (P4)	Occurs when you require information or assistance on Carousel-provided product capabilities, installation, or configuration. There is clearly little or no impact to your business operations. P4 incident are responded to using standard operation procedures as time allows.

C.5.1 Incident Notification

As incidents are prioritized and entered into the Information Technology Service Management (ITSM) platform, the Client is notified via automated email response. The automated email response will contain the incident number, details collected during the event identification process, and affected device, system, service, or location information, and all actions taken. Any time an incident is open, updated, and closed automated email notification is sent to the Client.

In addition, to automated email notifications, Carousel can provide automate SMS notification, if requested by the Client. SMS notification is not a bi-directional SMS texting features rather it's an informational message sent from the ITSM to the Client. Carousel recommends that this function is only enabled for incidents containing the highest level of priority.

Carousel can provide additional telephonic notification for all P1 incidents, if requested by the Client.

C.5.2 Triage & Troubleshooting *(Optimize Only)*

Once the Carousel incident management team receives a service ticket, an engineer will follow step-by-step instructions to achieve predictable, standardized, and desirable results to quickly restore any unplanned interruption. This function covers the Analysis, diagnosis, resolution, and recovery of the incident.

C.5.3 Complex Resolution *(Optimize Only)*

Carousel will work with the Client IT staff or other 3rd parties through resolution when the incident may be a result of multiple technologies contributing to the incident.

C.5.4 Bug Resolution *(Optimize Only)*

When service affecting software anomalies (bugs) have been identified, our service delivery team will drive the resolution process. Carousel will identify the issue, work with the vendor to find a software resolution, begin an emergency service request process, and deploy the appropriate patch, service pack, or upgrade as part of the change management process.

C.5.5 Carrier Management *(Optimize Only)*

For the supported environment, Carousel owns identification, troubleshooting, and resolution of Carrier related issues. Carousel acts as an agent of the Client and drives Carrier escalations for MPLS, Ethernet, broadband, dedicated Internet, SIP trunks, PRI's, or analog circuits in the event of link down, service outage, timing & slips, or high interface errors.

Carousel will:

- Create and maintain the appropriate documentation in Carousel's ITSM system
- Drive escalation with the appropriate Carrier or service provider
- Notify and communicate the issue to Client including carrier ticket number, time of outage and expected time of restoration
- Act as an intermediary between Client and the service provider
- Track and drive activities required to resolve the issue
- Update the Carousel Incident as required
- Validate the resolution of the incident
- Update and close the incident when the issue is resolved
- If available, obtain root cause.

Notwithstanding anything herein to contrary, Carousel resolution SLAs do not apply to Carrier Management Services.

Note: Client is required to sign LOA (Letter of Authorization) for each service provider during the service transition process for Carousel to perform Carrier Management. Limited to circuits connected to devices under Carousel Management.

Note: Any signed LOA (Letter of Authorization) is for incidents only, Carousel will not be responsible or accountable for any procurement, payment, ordering or decommissioning of circuits.

C.5.6 Vendor Management *(Optimize Only)*

For the supported environment, Carousel owns identification, troubleshooting, and resolution of third-party vendor related issues. Carousel drives the third-party vendor escalation process and provides follow-up of a supported vendor related issue. When required, Carousel creates a ticket directly with the third-party vendor on the Clients behalf. We drive the third-party vendor to identify the issue, troubleshoot the defined issues, and ultimately obtain resolution.

Carousel notifies and communicates all third-party vendor issues with the Client including, ongoing status, available work arounds, and expected time of resolution. Carousel works the incident through closure, and if available, obtains the root cause.

When required, Carousel drives the escalation processes to resolve configuration, software, and hardware anomalies, manage hardware replacement, software bug fixing and patch management, and on-site engineering dispatch. Carousel will:

- Create and maintain the appropriate documentation in Carousel's ITSM system

- Drive escalate with the appropriate third-party vendor
- Notify and communicate the issue to Client including ticket number, time of outage and expected time of restoration
- Act as an intermediary between Client and the third-party vendors
- Track and drive activities required to resolve the issue
- For hardware replacement, Carousel drives the replacement process until replacement is shipped, received, installed, configured IP addressing, restore last known configuration and update serial numbers Carousel's ITSM/CMDB
- Update the Carousel Incident as required
- Validate the resolution of the incident
- Update and close the incident when the issue is resolved
- If available, obtain root cause.

Note: Client is required to sign LOA (Letter of Authorization) for each third-party vendor during the service transition process for Vendor Management.

C.5.7 Incident Escalation *(Optimize Only)*

Incident escalation is a process used to highlight or flag certain issues within an Incident, so that the appropriate personnel can respond to these situations and monitor the resolutions. Carousel's escalation management process identifies, tracks, monitors, and manages situations that require increased awareness and swift action.

Carousel's carefully created escalation processes can ensure that unresolved problems don't linger, and issues are promptly addressed. Using Incident Escalation Management can re-prioritize, reassign, and monitor a situation to a satisfactory completion. There are two types of escalations: hierarchical and functional.

Hierarchical escalation is used to ensure attention for notification, action or resolution is moving the technical levels of operation. For example, 1st level support is unable to resolve the issue, so it is escalated to 2nd level support. In case they are also not able to solve the issue, they are escalating it to 3rd level support and so on until the issue is resolved. During the hierarchical escalation the workflow management is evaluating the incident priority against resolution progress.

Functional escalation is used in case that the support team is unable to resolve the issue or stick within the agreed timeline (targeted time for resolution is exceeded). Functional escalation is the process used to assign an incident from one team to another team based on the skills required to resolve the incident. For example, escalating an incident from the unified communications team to the network team when it becomes apparent that the lack of performance is due to network conditions.

C.6. Problem Management *(Optimize Only)*

C.6.1 Root Cause Analysis *(Optimize Only)*

Our service delivery team conducts root cause analysis to determine the underlying cause of an incident, document the findings and take appropriate corrective action. Root cause analyses are performed to understand the cause of critical outages, prevent future incidents from occurring, eliminate chronic incidents, and minimize future impact to problems and outages.

1. Perform problem determination and problem resolution
 2. Perform tracking and management of outage to closure
 3. Perform root cause analysis for individual P1 and P2 incidents
- **NOTE: This can be provided on P3 cases as requested by the client**
4. Identify chronic problems

C.6.2 Chronic Problem Management *(Optimize Only)*

Our service delivery team will drive the identification and resolution of chronic incidents. Chronic issues are defined as the same problem occurring multiple times in a 90-day period. We will attempt to reproduce the problem, identify incident triggers, document the current state, define remediation paths, and work around scenarios and provide detailed root cause analysis.

C.7. Patch & Release Management *(Optimize Only)*

The purpose of Patch & Release Management is to facilitate the physical control of software assets and their release into the production environment.

- (a) **Major Software Release** - Major Release is a major change to the software that introduces new optional features and functionality. Major Releases are typically designated as a change in the digit(s) to the left of the first decimal point (for example, [N], y.z) are out of scope.
- (b) **Minor Software Releases** (aka "dot" release) - A Minor Release is a change to the software that introduces a limited number of optional features and functionality. Minor Releases are typically designated as a change in the digit to the right of the first decimal point (for example, n.[Y].z) and are included **FOR NETWORK DEVICES** as part of release management.
- (c) **Patch Release** - Patch Release is a change to the software to stabilize the code based upon reported bug related issues or to correct/harden a potential security vulnerability. Patch Releases are typically designated as a change in the digit to the right of the second decimal point (for example, n.y.[Z]) and are included as part of release management.

Note: Product correction updates may require system hardware upgrades to comply with current manufacturer's specifications. In these cases, the hardware must be upgraded before the update can be implemented. Hardware upgrades are not included as part of this service.

Note: If Carousel determines the patch is appropriate, it will follow Change Management procedures and policies.

Note: Additional installation, implementation and/or customization services necessary to implement software releases are not included in this service and are defined as projects.

Note: Client must retain entitlement to receive software and/or firmware updates from their manufacturers. Carousel does not provide an alternative to upgrade entitlement or leverage Carousel entitlements on Client's behalf. Carousel does not supply any software or firmware of any kind other than for Carousel owned equipment and systems.

C.7.1 Server Patch Management *(Optimize Only)*

Carousel follows an industry best practice methodology of Scan, Assess, Approve, and Install for updating Microsoft and Linux server patches. We provide weekly assessment, notification, and recommendation of patches. We provide monthly patch implementation or more immediate if service effecting or security related.

Any MAJOR or MINOR releases will be quoted as a project and be considered out of scope.

C.7.2 Network Device Release Management *(Optimize Only)*

Carousel follows a semantic versioning model for network device patches. The model is defined as MAJOR.MINOR.PATCH. We provide quarterly assessment, notification, and recommendation of patches. We provide semi-annual patch and minor implementation or more immediate if service effecting or security related. Carousel will report on MAJOR.MINOR.PATCH, but **will only implement on PATCH & MINOR.**

Any MAJOR releases will be quoted as a project and be considered out of scope.

C.7.3 Application Release Management *(Optimize Only)*

Carousel follows a semantic versioning model for application for select business enablement applications. The model is defined as MAJOR.MINOR.PATCH. We provide quarterly assessment, notification, and recommendation of patches. We provide quarterly patch implementation or more immediate if service effecting or security related. Carousel will report on MAJOR.MINOR.PATCH, but will only implement on PATCH.

Any MAJOR or MINOR releases will be quoted as a project and be considered out of scope.

C.8. IT Asset Change Management *(Optimize Only)*

Carousel's IT asset change management function ensures that a standardized set of procedures is used to promptly handle all requests for service or change. It ensures that all changes are recorded, assessed, approved, prioritized, and deployed in a manner that meets business requirements and protects the stability and reliability of critical IT systems.

The main objective of change management is to control the lifecycle of while minimizing disruption to IT services. Service or change request can be broadly classified as "Standard", "Complex" and "Emergency":

- **Standard** change tasks are well known, defined, documented, and proven. The change management workflow is pre-established, and no approval is necessary.

- **Emergency** change requests need to be executed immediately to resolve imminent Critical/Sev-1/P1 incidents that threaten business continuity. Emergency request requires approval from the eCAB and will follow the workflow defined in the emergency change request.
- **Complex** change request is pervasive, less defined, and the impact of the request is not known. Complex request could change the configuration of an existing feature, enable existing capabilities, or focus resolving a known issue. Complex requests require Change Advisory Board (CAB) approval, and the specification of a maintenance window.

As part of the overall process, Carousel will provide the following where applicable:

- Manage and implement system level configuration changes
- define the changes required
- measure the impact of the proposed change
- develop a back-out plan
- obtain any relevant approvals for change
- schedule the implementation of the change
- implement the change
- post-implementation testing and verifying expected outcomes; and
- in the event of an unsuccessful change, implement the back-out plan in relation to the change.

C.8.1 Standard Change Request *(Optimize Only)*

Our Service Delivery team will manage and implement "system wide" level configuration changes where the implementation process and the risks are known upfront, documented, proven, and the risk is low and well understood, and the change workflow has been pre-established. These changes are managed according to policies that have been established during Service Transitioning. Standard change request approval can be automatically granted.

C.8.2 Emergency Change Request *(Optimize Only)*

Our Service Delivery team will manage and implement emergency change requests when an unexpected error, threat occurs, or events that effect business continuity emerge. Emergency request are evaluated on the basis that the risk of not implementing the request is greater than implementing the request. Emergency request bypass the normal Change Advisory Board (CAB) process and is reviewed by the eCAB requiring a single board members approval. All emergency change requests undergo a post-implementation review process.

C.8.3 Complex Change Request *(Optimize Only)*

Complex Requests must be reviewed by the Change Advisory Board (CAB) who examines the request, assesses the associated risk and impact, and ultimately approves the request for implementation. For complex changes to be implemented, requires a minimum of 51% CAB member approval. Usually a complex request involves a significant change to the service or infrastructure, and it carries some degree of risk. All complex changes require comprehensive planning, documentation, workflow analysis, and governance. If the request is determined to be high-risk, the CAB must decide whether, when and how the request will be implemented or if the complex change request needs to be treated as project. The following list of criteria are used to determine if the complex change request should be treated as a project:

- **On-site** When the service/change request requires onsite Carousel engineers to complete the request.
- **Testing** When the service/change request requires extensive testing by our engineering team, client's team, or a combination of both.
- **Expansion** When the service/change request adds new devices, locations, or features that fundamentally change the nature of the supported environment.
- **Design** When the service/change request changes the fundamentally design, architecture, or the operations of the supported environment.
- **Platform** When the service/change request impacts multiple supported platforms across the supported environment.
- **Coordinate** When the service/change request requires the Carousel team to coordinate multiple resources – vendors, people, locations, or multiple phases of change implementation

Based on the above defined criteria and the nature of the complex change, some request could be managed as a project and billed outside the scope of this contract.

C.9. Health Checks *(Optimize Only)*

C.9.1 Security *(Optimize Only)*

Our Security Health Check entitlement proactively confirms all security components are operating as desired, keeping the configurations as optimized as possible, and provide awareness to new features and functionality in any new code revisions.

Annually, Carousel will conduct an intensive rule base review and clean up, review configuration with current best practices, assess the overall system health, analyze potential threats, and recommend new software features and configurations. The results will be provided, and reviewed with the client.

C.10. Continuous Service Improvement

Carousel's service delivery team incorporates a quality assurance and continuous improvement processes as a proactive component of our managed services offering. Our service delivery team compares month-to-month key performance indicators (KPIs) such as "First to Know" trends, SLA attainment, mean time to resolution measurements, "alert to incident" ratios, "alert to device" ratios, and noisy element analysis to drive continual service improvements. And daily, our team reviews a subset of incidents leading to runbook changes, new runbook development, runbook automation, increased event correlation, and improved alert aggregation. The Quality Assurance Review begins during service transitioning and continues throughout the entire contract lifecycle.

Exhibit D – Service Level Agreement

Carousel requires full access/shared control with the Client of the supported items that are at Operate and/or Optimize level of service. Client needs to inform Carousel of any device additions, deletions, or changes to supported items.

The following table describes the various priority levels and Service Level Objectives (SLO). The start of the process can originate from monitoring system alerts or from user requests entered via the ticketing system, phone or e-mails.

Commitment	Definition	Priority	Objective	Quarterly Measurement
Speed to Answer				
Speed to Answer is measured across all client calls.	Service Desk live answer		<=20 Seconds	90% Aggregate
Incident Response				
Incident Response is measured from receipt of notification via email, call, or alarm.	Notification to Incident	P1	<=15 Minutes	90% Aggregate
	- All Emails considered as P2 by default	P2	<=30 Minutes	
		P3	<=30 Minutes	
		P4	<=30 Minutes	
Incident Assignment (Optimize Only)				
Incident Assignment period is measured from the time the incident has been opened.	Incident to Engineer Assignment	P1	<=30 Minutes	90% Aggregate
		P2	<=1-hour	
		P3	<=4-hour	
		P4	<=8-hour	
Incident Resolution (Optimize Only)				
Incident Resolution period is measured from the time the incident has been opened.	Incident Creation to Incident Resolution	P1	<=4-hour	80% Aggregate
		P2	<=8-hour	
		P3	<=4 Business Days	
		P4	<=10 Business Days	
Problem Management (Optimize Only)				
Problem Management is measured from time of client request for RCA.	Root Cause Analysis (RCA) Inputs	Draft	3 Business Days	80% Aggregate
		Delivery	10 Business Days	
Change Management Response (Optimize Only)				
Change Management Request Response is measured from receipt of the request to the creation of the Service Request (SR).	Emergency Change Critical	P1	<=15 Minutes	90% Aggregate
	Emergency Change Default	P2	<=30 Minutes	
	Complex Change Default	P3	<=30 Minutes	
	Standard Change Default	P4	<=30 Minutes	
Change Management Implementation (Optimize Only)				
Change Management Implementation is measured from the time of the change approval or from the start of the authorized change window.	Emergency Change Critical	P1	<=2-hour	80% Aggregate
	Emergency Change Default	P2	<=Same Bus Day	
	Complex Change Default	P3	<=Next Bus Days	
	Standard Change Default	P4	<=3 Business Days	

Resolution SLO timer is paused when ticket status is changed to “Handed-over to Client and/or Partner,” “On-Hold,” “Under observation,” “Work around” or “Resolved”

Below is a list of conditions that will trigger a pause in the resolution SLO timer:

Resolution SLO timer pause conditions
<ul style="list-style-type: none">• Waiting for remote access/connectivity to client environment• Waiting for the arrival of replacement hardware• Waiting for the arrival of dispatched on-site engineering/resources• Waiting for 3rd Party (Carrier, Courier)• Waiting on client to perform validation, testing,• Scheduled or planned downtime

Resolution SLO timer are stopped when the INCIDENT is experiencing the following conditions:

Exclusions
<ul style="list-style-type: none">• Force Majeure conditions• Lack of power to facilities and inadequate power backup• Lack of Wide Area connectivity without appropriate redundancy• Lack of appropriate manufacturer support coverage on critical elements

Exhibit E - Supported Items

Site Location	Service Bundle	Carousel Item-Number	Manufacturer	Long Description	Quantity
CPD - Clearwater PD	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
CPD - Clearwater PD	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	2
ERB - R911 Host Side B	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
ERB - R911 Host Side B	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	2
LPD - Largo PD	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
LPD - Largo PD	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	2
PPPD - Pinellas Park PD	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
PPPD - Pinellas Park PD	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	2
PSC - R911 Host B	Optimize	MS-OPTM-SECN-FW-T3	FortiNet	Fortigate 60 Series	1
PSC - R911 Host Side A	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
PSC - R911 Host Side A	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	5
PSC - R911 Host Side A	Optimize	MS-OPTM-SECN-APP-T5	FortiNet	Fortinet FortiAnalyzer	1
PSC - R911 Host Side A	Optimize	MS-OPTM-SECN-APP-T5	FortiNet	Fortinet FortiManager	1
PSC - R911 Host Side A	Optimize	MS-OPTM-SECN-FW-T3	FortiNet	Fortigate 60 Series	1
SPPD - St Pete Host A	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
SPPD - St Pete Host A	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 3650 Series Switches	2
SPPD - St Pete Host A	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	3
SPPD - St Pete Host A	Optimize	MS-OPTM-SECN-FW-T3	FortiNet	Fortigate 60 Series	1
SPPD - St. Pete Host B	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
SPPD - St. Pete Host B	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 3650 Series Switches	2
SPPD - St. Pete Host B	Optimize	MS-OPTM-SECN-FW-T3	FortiNet	Fortigate 60 Series	1
TSPD - Tarpon Springs PD	Observe	MS-OBS-NET-RTE-T3	Cisco	Cisco 4000 Series Integrated Services Routers	2
TSPD - Tarpon Springs PD	Optimize	MS-OPTM-NET-SWCH-T2	Cisco	Cisco Catalyst 2960 Series Switches	2






Updated Second Amendment

Final Audit Report

2022-03-07

Created:	2022-03-07
By:	Jo Anne Lewis (legal@carouselindustries.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAATfavBK0R-zRhGN0zuLGkPmEzCPtN6VIK

"Updated Second Amendment" History

-  Document created by Jo Anne Lewis (legal@carouselindustries.com)
2022-03-07 - 6:05:44 PM GMT - IP address: 208.68.224.5
-  Document emailed to Santhosh Daniel (sdaniel@nwnit.com) for signature
2022-03-07 - 6:06:54 PM GMT
-  Email viewed by Santhosh Daniel (sdaniel@nwnit.com)
2022-03-07 - 8:35:35 PM GMT - IP address: 96.233.143.66
-  Document e-signed by Santhosh Daniel (sdaniel@nwnit.com)
Signature Date: 2022-03-07 - 8:35:52 PM GMT - Time Source: server - IP address: 96.233.143.66
-  Agreement completed.
2022-03-07 - 8:35:52 PM GMT