IronOrbit
The Cloud Made Simple.

IronOrbit Cloud Services Support

INFINITY Cloud Support is a crucial add-on service for IronOrbit INFINITY Workspaces, designed to ensure smooth IT operations and maintenance with a guaranteed service level agreement (SLA). Essential Cloud Support is part of our INFINITY Workspaces offerings that guarantee peace of mind by ensuring users can always connect to their hosted desktops from anywhere, at any time. Should any issues arise, IronOrbit's support agents are available 24/7/365 to assist with connectivity. This foundational support covers all aspects necessary for maintaining reliable access to remote desktops, forming the backbone of our customer support structure.

Premium Cloud Support includes:

- Service Availability Assurance (INFINITY Workspaces & IOCentral)
- M365 Administration & Support (Licensing, Configuration, Updates)
- Identity & Credential Management (Entra ID/AD, IO-Provided Credentials)
- Email Administration & Security
- Local Desktop, Laptop & Network Support
- INFINITY Workspace / VDI Image Refresh
- IO Cloud Infrastructure Support
- Protected Storage & Recovery
- Dedicated Customer Success Manager

24/7/365 Helpdesk:

- 100+ technicians and engineers
- Industry-leading service SLAs
- Guaranteed same-day response
- Microsoft Office Suite product support
- Advanced SLAs and Service options available

We Support YOU

24/7/365

Microsoft MCSA x42

Microsoft MCSE x18

Microsoft MCITP x54

Cloud Services

Managed IT Services

Network & Security Services

Data Protection

Professional Services

Software & Licensing:

- Windows 10, 11 Desktop Experience
- Microsoft Server 2019/2022 Licensing
- All Client Applications

(Client specific application licenses are provided by Client, Microsoft OS, Apps & Security/DR licensing provided by IronOrbit)

IO INFINITY ESSENTIAL CLOUD SUPPORT

IO INFINITY ESSENTIAL 24/7/365 USBASED HELPDESK SUPPORT

- **End User Management:**
  - Create/Remove/Change User(s)
  - Reset Password(s)
  - Revise User Permissions
  - Manage Emails and Distribution Groups
- **Basic User Support:**
  - We provide basic 24/7/365 basic user support
  - Ensure users are connected, trouble free, to their IronOrbit workspaces
  - We also ensure access to Microsoft Office applications as part of this service
  - Limited to IronOrbit Desktop Connectivity and Microsoft Office Suite Product Support (Word, Excel, Outlook, and PowerPoint)
- **Advanced 2nd Level Support:**
  - Available on a pay-per-hour basis for out-of-scope support

IO Essential Helpdesk Support is offered as a monthly quota of 15 minutes per user, pooled for the whole account. For example, a customer with 50 users, the monthly allocated support time would be 15 minutes * 50 users = 750 minutes or 12.5 hours per month. Support related to system maintenance is excluded from this pooled time.

IO INFINITY ESSENTIAL INFRASTRUCTURE & DAAS MANAGEMENT

- **Desktop Image Management:**
  - Deployment of the base image to all desktop users after Windows or Microsoft Office updates
  - CPU/GPU/RAM/DISK usage monitoring and management
- **Security Policy Management:**
  - Updates to security settings and policies within cloud domain
  - Antivirus, Firewall, & Antispam
  - 24/7/365 NOC Security Monitoring
  - IDS/IPS
  - Event Correlation
  - Anti-DDoS
  - Data-at-Rest Encryption
  - DNS & Content Filtering

IO Essential Infrastructure & DaaS Management is offered with a monthly quota of 30 minutes per server, pooled for the whole account. For instance, a customer with 6 servers, the monthly allocated support time would be 30 minutes * 6 servers = 180 minutes or 3 hours per month. Support related to system maintenance is excluded from this pooled time.

IO CENTRAL ESSENTIAL ACCESS (UNLIMITED)

- **Desktop Managed Services:**
  - **Monitoring:** Monitor desktop utilization (CPU/GPU/MEM/DISK)
  - **Reporting:** Review desktop performance summary for the past 30 Days
  - **Updating & Patching:** Check your current desktop patch and compliance status
  - **Antivirus and Core System Functions:** Upgrade, scale or switch between the different packages and services that will best suite your needs, all with a few clicks.
- **Server Managed Services:**
  - **Monitoring:** Monitor server utilization (CPU/GPU/MEM/DISK)
  - **Reporting:** Review server performance summary for the past 30 Days
  - **Updating & Patching:** Check your current server patch and compliance status
  - **Antivirus:** Check your antivirus subscription state
- **Full IT Control:**
  - User provisioning
  - Active Directory management
  - Multi-cloud capabilities (MS 365, 2FA, and more)
  - Multi-location management
- **Online Ticket Management:**
  - Open, close and follow up on your tickets in real-time
  - Chat directly with a technician
  - Review status updates and ticket progress, including past tickets and complete support history

IO Central Essential Access is total control at your fingertips from a Single Control Pane. It provides the ability to manage and monitor your environment, as well as support tickets and history.

RESPONSE TIMES

The following table shows the targets of response times for each priority level for Managed Services:

Trouble	Priority	Response Time†
Company Wide Outage, Service Not Available (All users and functions unavailable).	1 (Critical)	Within 1 Business Hour
A large number of users or functions affected. One department or division impacted. Business process can continue but significant impact within the organization.	2 (High)	Within 2 Business Hours
Limited Degradation of Services. There is a limited number of users or functions affected. Business process can continue.	3 (Medium)	Within 4 Business Hours
Small service degradation (business process can continue, one user affected).	4 (Low)	Within 8 Business Hours
General questions, Service changes, Internal productivity affecting only, Requests to install or update business software packages.	5 (Very Low)	Within 24 Business Hours

† - Stated Response Times represent a service goal and not a guarantee. Provider's ability to implement a solution to a reported problem may depend on input or information from Client or from third parties beyond its control, including Client's IT vendors.

IO INFINITY PREMIUM CLOUD SUPPORT

IO INFINITY PREMIUM 24/7/365 US-BASED HELPDESK SUPPORT

- **End User Management:**
  - Create/Remove/Change User(s)
  - Reset Password(s)
  - Revise User Permissions
  - Manage Emails and Distribution Groups
- **Advanced 2nd Level Support:**
  - 24/7/365 Advanced Helpdesk Support includes all hosted applications (no limitations)
- **Advanced User Support:**
  - Includes Basic User Support (Desktop Connectivity and Microsoft Office Suite Product Support)
  - Ensure access to all hosted and 3rd party applications, such as QuickBooks and AutoCAD
  - Helpdesk Support can help customize your workspace, applications and more
- **Vendor Coordination:**
  - If vendor support is required, we coordinate everything from initial contact to final resolution

IO INFINITY Premium Helpdesk Support is offered as a monthly quota of 30 minutes per user, pooled for the whole account. For instance, a customer with 50 users, the monthly allocated support time would be 30 minutes * 50 users = 1,500 minutes or 25 hours per month. Support related to system maintenance is excluded from this pooled time.

IO INFINITY PREMIUM INFRASTRUCTURE & DAAS MANAGEMENT

- **Desktop Image Management:**
  - Deployment of the base image to all desktop users after Windows or Microsoft Office updates
  - CPU/GPU/RAM/DISK usage monitoring and management
- **Security Policy Management:**
  - Updates to security settings and policies within cloud domain
  - Antivirus, Firewall, & Antispam
  - 24/7/365 NOC Security Monitoring
  - IDS/IPS
  - Event Correlation
  - Anti-DDoS
  - Data-at-Rest Encryption
  - DNS & Content Filtering
- **3rd Party Application Support:**
  - User Desktop Software Application Updates
  - Server Software Application Updates
  - Advanced Server Application Support

IO Essential Infrastructure & DaaS Management is offered with a monthly quota of 60 minutes per server, pooled for the whole account. For instance, a customer with 6 servers, the monthly allocated support time would be 60 minutes * 6 servers = 360 minutes or 6 hours per month. Support related to system maintenance is excluded from this pooled time.

IO CENTRAL PREMIUM ACCESS (UNLIMITED)

- **Desktop Managed Services:**
  - **Monitoring 250+ Data Points:** Extended monitoring that covers more than 250 Data Points, in addition to desktop utilization (CPU/GPU/RAM/DISK)
  - **Reporting:** Review desktop performance summary for the past 365 days
  - **Updating & Patching:** Check your current desktop patch and compliance status
  - **Antivirus and Core System Functions:** Upgrade, scale or switch between the different packages and services that will best suite your needs, all with a few clicks.
- **Server Managed Services:**
  - **Monitoring 250+ Data Points**: Extended monitoring that covers more than 250 Data Points, in addition to server utilization (CPU/GPU/RAM/DISK)
  - **Reporting:** Review server performance summary for the past 365 days
  - **Updating & Patching:** Check your current server patch and compliance status
  - **Antivirus:** Check your antivirus subscription state
- **Full IT Control:**
  - User provisioning
  - Active Directory management
  - Multi-cloud capabilities (MS 365, 2FA, and more)
  - Multi-location management
- **Online Ticket Management:**
  - Open, close and follow up on your tickets in real-time

- Chat directly with a technician
- Review status updates and ticket progress, including past tickets and complete support history

IO Central Essential Access is total control at your fingertips from a Single Control Pane. It provides the ability to manage and monitor your environment with robust reporting and visibility, so you focus on the big picture.

RESPONSE TIMES

The following table shows the targets of response times for each priority level for Managed Services:

Trouble	Priority	Response Time†
Company Wide Outage, Service Not Available (All users and functions unavailable).	1 (Critical)	Within 30 Minutes
A large number of users or functions affected. One department or division impacted. Business process can continue but significant impact within the organization.	2 (High)	Within 1 Business Hour
Limited Degradation of Services. There is a limited number of users or functions affected. Business process can continue.	3 (Medium)	Within 2 Business Hours
Small service degradation (business process can continue, one user affected).	4 (Low)	Within 4 Business Hours
General questions, Service changes, Internal productivity affecting only, Requests to install or update business software packages.	5 (Very Low)	Within 8 Business Hours

† - Stated Response Times represent a service goal and not a guarantee. Provider's ability to implement a solution to a reported problem may depend on input or information from Client or from third parties beyond its control, including Client's IT vendors.

IRONORBIT ESSENTIAL SUPPORT

- **End User Management**:
  - Create/Remove/Change User(s)
  - Reset Password(s)
  - Revise User Permissions
  - Manage Emails and Distribution Groups
- **Basic User Support:**
  - Available 24/7/365 via telephone, email, or online ticketing.
  - Ensure users are connected, trouble free, to their IronOrbit workspaces.
  - Ensure access to Microsoft Office applications purchased as part of the Service.
- **Advanced 2nd Level Support:**
  - Available on a pay-per-hour basis for out-of-scope support

IronOrbit Essential Support is performed by US-Based employees, 24/7/265. It is limited to IronOrbit Virtual Desktop Connectivity and Microsoft Office Suite Product Support (Word, Excel, Outlook, and PowerPoint). Offered as a monthly quota of 15 minutes per Virtual Desktop named user, pooled for the entire account. (e.g., A customer with 50 users, the monthly allocated helpdesk support time would be 15 minutes * 50 users = 750 minutes or 12.5 hours per month.) Support related to system maintenance is excluded from this pooled time, and Provider will not charge the pooled time consumed for maintenance purposes.

REPORTS

- **IronOrbit will provide the following reports to Client via emails for each month:**
  - Patch Reports (aging and missing)
  - System Availability/Uptime Report
  - System Utilization Reports
  - Cyber Security Incident Report (number of incident, response time, escalation, resolution results), if any
  - Storage Encryption Report (upon request)
  - Backup Report
  - Asset Management Reports (hardware, software, upcoming EOL)
  - Desktop and Server Capacity
  - Internet Utilization
  - Storage Utilization
  - Number of Service Units (billing)
  - Systems Software Report
  - Customer Support Performance (Summary of issues, outstanding tickets)
- **In addition, annual reports will be provided to Client:**
  - Provider's Resiliency Plan Changes of Client's Cloud Solution (BC/DR plan that has RTO and RPO)
  - Environment/Architecture changes of Client's Cloud Solution
  - Summary of Pentest report limited to IronOrbit corporate
  - Independent audits or assessments (SOC 2 Reports with bridge letters, if needed)
  - Updates or re-assessments to IO risk assessments occur (when available, at least annually)
  - IronOrbit's Audited Annual Financials1
  - IronOrbit's Hiring Polices
  - IronOrbit's Code of Conduct and Ethics
  - IronOrbit's TPRM or Vendor Management Policy
  - IronOrbit's Information Security, Change Management, Risk Management, Incident Response policies
  - SOC Reports from Provider's 3rd parties Vendors for Services provided to Client

Other compliance requirements as identified and reviewed from the FFIEC Cybersecurity Assessment Tool (CAT) Worksheet. A review of the CAT will be conducted between the CPB and IO teams at least annually to align reporting and evidence requirements, subject to the hourly fees set forth herein.

[1]Client agrees to pay Provider for all costs associated with Audited Financials. Client understands that Provider does not require audited financials as part of its normal course of business. If Client waives the requirement for Audited Financials, then there will be no cost to provide Internally Prepared Financial Statements (Profit & Loss / Balance Sheet).

IOCENTRAL SELF-SERVICE PORTAL

- **Full IT Control:**
  - User provisioning
  - Active Directory management
  - Multi-cloud capabilities (e.g., MS365, 2FA, Email Security)

- Multi-location management
- **Online Ticket Management:**
  - Open, close and follow up on Client's tickets in real-time.
  - Chat directly with a certified IronOrbit technician.
  - Review status updates and ticket progress, including past tickets and complete support history.
- **Asset Management:** Manage all cloud assets including desktops and servers from a central location.
- **Scale & Upgrade on Demand:** Upgrade, scale or switch between the different IT packages and services that will best suite Client's needs, all with a few clicks.
- **Monitoring:** Monitor cloud infrastructure utilization (e.g., CPU/MEM/DISK)
- **Reporting:** Review desktop & infrastructure performance

IOCentral Essential Access is total control at Client's fingertips from a Single Control Pane. It provides the ability to manage and monitor Client's environment, as well as support tickets and history.

SMART MANAGED SERVICES FOR INIFINITY WORKSPACES

- **Desktop Managed Services:**
  - **A**vailability Monitoring: Monitor desktop availability and readiness.
  - Performance Monitoring: Monitor desktop utilization (CPU/MEM/DISK)
  - Security Patching & Updates: Automated OS security patching for important & critical security vulnerabilities
  - 3rd Party Patching: Automated 3rd party application security patching for important & critical security vulnerabilities.
    - Limited to IronOrbit's standard 3rd party application set.
  - **Endpoint Protection Monitoring:** Check Client's EDR/MDR/XDR/AV subscription state
- **Server Managed Services:**
  - **A**vailability Monitoring: Monitor server availability and readiness.
  - Performance Monitoring: Monitor server utilization (CPU/MEM/DISK)
  - Security Patching & Updates: Automated OS security patching for important & critical security vulnerabilities
  - 3rd **Party Patching:** Automated 3rd party application security patching for important & critical security vulnerabilities.
    - Limited to IronOrbit's standard 3rd party application set.
  - **Endpoint Protection Monitoring:** Check Client's EDR/MDR/XDR/AV subscription state

IronOrbit Smart Managed Services For Infinity Workspaces is offered with a monthly quota of 30 minutes per server, pooled for the entire account. (e.g., A customer with 6 servers, the monthly allocated support time would be 30 minutes * 6 servers = 180 minutes or 3 hours per month.) Support related to infrastructure system maintenance is excluded from this pooled time.

IRONORBIT SECURITY CONTROLS

- **SOCII TYPE II Certified Service & Availability Baseline Controls for IronOrbit Cloud Solution and Maintenance and Support:**
  - N+1 or Greater Design for High Availability
  - Next Generation Firewall Protection
  - Threat Prevention Detects and Prevents Advanced Threats with Zero-Day Update Services
  - Advanced URL Filtering
  - Intrusion Detection and Prevention (IDS/IPS)
  - Anti-DDoS Configurations
  - Geo-blocking Baseline
  - DNS & Content Filtering
  - 24/7/365 NOC & Security Monitoring

IRONORBIT PROTECTED STORAGE

- Usage: Based on high speed, solid-state storage, protected storage is designed to deliver high performance for Cloud Services including Client's Network and all associated workloads. All virtual machines and data, including servers and desktops, reside on this platform.
- Encryption: All IronOrbit Protected Storage is secured by non-deprecated data-at-rest encryption (DARE).
- Backup: Utilizes advanced backup technology, ensuring data backups are encrypted, air-gapped and retained for 60 days.
- Immutable Off-Premises Backups: Backups are transferred to an off-premises cloud location in an immutable fashion, utilizing one-way writes to ensure data cannot be modified or deleted. This method serves as an additional layer of protection against cyber threats, reinforcing data security and integrity.
- Full Restoration: One full system restoration is allowed per month at no charge.
- File Level Restoration: Unlimited self-service restorations are available if compatible and configured within the Client Network. Up to three professional file-level restorations are allowed per month at no charge.
- Additional Restoration: Requests beyond the provided limits are charged in accordance with the fee schedule above.
- Storage Limits: Based on the storage tier selected.
- Usage Notification: Automated email notifications are in place to alert Client when their then current storage tier

utilization reaches 75%, enabling proactive management of storage resources.
- o Automatic Upgrade: When storage tier utilization exceeds the maximum allocated storage, the system automatically initiates an upgrade to the next tier to ensure uninterrupted service and data accessibility.
- o Downgrade: Client can manually adjust their storage tiers downward if their total allocation is reduced below their then current tier.

SERVICE LEVEL AGREEMENT FOR IRONORBIT CLOUD SERVICES

99.999% Cloud Solution Uptime Guarantee:

Provider guarantees that the Cloud Solution (Provider Server(s)/Desktop(s)) will be available not less than 99.999% of the time in a given month. This guarantee does not take into account any scheduled maintenance or service changes requested by Client. The Cloud Solution Uptime Guarantee is limited to the hosted virtual servers and desktops. If the Client fails to have access less than 99.999% to their Cloud Solution at any time during the month, due to an unscheduled service disruption, and the Client requests a service credit, as defined below.

99.999% Data Center Internet Connection Uptime Guarantee:

Provider guarantees that its Data Center Internet Connection will be available not less than 99.999% of the time in a given month. Provider's Data Center Internet Connection is defined as the portion of the data center network extending from the outbound network interface of Client's Cloud Solution to the outbound port of the data center border router. This includes core infrastructure such as managed switches, routers, firewalls and cabling. The foregoing guarantee does not cover any failure of service arising from any failure or malfunction of equipment or services outside of Provider's data center including but not limited to internet service providers (ISPs) between Provider's data center and Client's local network. If the Client fails to have access to the Cloud Solution due to an outage of the Data Center Internet Connection at any time during the month, the Client shall receive a service credit as defined below.

Dedicated Support Phone Number

Provider will assign a dedicated phone number to Client to call into for support and incident communications.

SERVICES SLA

- Definitions:

Priority: Urgency & Impact classification

Problem Description: General criteria for classification

Acknowledgement: The time within which the problem is reported to the IronOrbit to the initial communication from IronOrbit is received by Client. Notification – Status updates and communication between parties.

Problem Management: The following table shows the targets of response times for each priority level for Managed Services:

Priority	Acknowledgement	Notifications
1	15 minutes	Every hour until resolved
2	15 minutes	Every hour until resolved
3	2 hours	As necessary until resolved
4	4 hours	As necessary until resolved
5	8 hours	As necessary until resolved

For a P1 – P2: One or more violations of "Acknowledgement" or "Notifications" in a 30-day period will result in a $500 credit back to Client. For a P3 – P5: Two or more violations of "Acknowledgement" or "Notifications" in a 30-day period will result in a $250 credit back to Client.

Priority	Problem Description
1 - Critical	• Outage lasting > 15 minutes Company Wide Outage • Outage of All DRP 1 Classified Servers defined by Client • Service Not Available
2 - High	• Outage lasting > 30 minutes 75 or more Users Affected • Outage of 5 or more DRP 1 or DRP 2 Classified Servers defined by Client • Outage of 10 or more DRP3 through DRP 6 Classified Servers defined by Client Violations of RPO and/or RTO of DRP 1 or DRP 2
3 – Medium	• Limited Degradation of Services. • There is a limited number of users or functions affected. Business process can continue. Violations of RPO and/or RTO of DRP 3 or DRP 4.
4 – Low	• Small service degradation. • Business process can continue, one user affected.
5 – Very Low	• General Questions, Service Changes. • Internal productivity not impacted. Service requests to install or update business software packages. Service Requests including password changes.

- **Service Credit:**
  When a "service credit" is available, as determined by Provider, and is requested by a Client, it is defined as the prorated amount, calculated as follows:

  For a Priority 1 incident, the monthly fees of IronOrbit services (servers, desktops & storage – excluding Client Applications, 3rd party colocation, Third Party Provider connectivity, and Client's 3rd party add-ons such as Microsoft 365, etc.) for the billing period during the unavailability/interruption, multiplied by the number of downtime hours, divided by forty-eight (monthly Fees x downtime hours /48).

  For a Priority 2 incidents, the monthly fees of IronOrbit services (servers, desktops & storage – excluding Client Applications, 3rd party colocation, Third Party Provider connectivity, and Client's 3rd party add-ons such as Microsoft 365, etc.) for the billing period during the unavailability/interruption, multiplied by the number of downtime hours, divided by two-hundred (monthly Fees x downtime hours /200), cumulatively not to exceed 25% of monthly Fees.

  For a Priority 3 incident, the monthly fees of IronOrbit impacted services (servers, desktops & storage – excluding Client Applications, 3rd party colocation, Third Party Provider connectivity, and Client's 3rd party add-ons such as Microsoft 365, etc.) for the billing period during the unavailability/interruption, multiplied by the number of downtime hours, divided by seven hundred-twenty (monthly Fees x downtime hours /720).

  Notwithstanding anything in this Service Level Agreement or any related agreement between the Client and Provider to the contrary: No service credit is available if Client does not request a service credit from Provider, in writing, within thirty (30) calendar days of the restoration of any access to service by Client and no other notice provision may extend this notice period; the service credit request will be reviewed and a determination made within 30 days of the Client's request; the account must be brought to current within 15 calendar days with no past due balances that are not disputed by parties; the service credit will be applied to future invoices or issued as a refund; and the maximum total service credit for the monthly billing period shall not exceed 100% of Service Fee for the billing period during the unavailability. No service credit is available for downtime caused by switching to or from Hawaii Datacenter to or from a DR site (provided no RPO and RTO violation) if Client declares a "disaster" when the Services are functionally normally, or down time caused solely by force majeure events.

- **Disaster Recovery SLA:**

  In the unlikely event of a complete cloud node failure, Provider will restore a copy of any impacted virtual servers, utilizing the most recent backup or replica to an alternate production cloud node. Specific system Disaster Recovery Priority ("DRP"), will be defined by Client. Disaster Recovery does not guarantee the availability of GPU backed workspaces on a recovery cloud node. A successful fail over of services to the Disaster Recovery site will downgrade the severity of the event to a P3 or lower.

Disaster Recovery Priority	Max RPO	Max RTO
DRP 1	30 Min	2 Hours
DRP 2	30 Min	4 Hours
DRP 3	2 Hours	8 Hours
DRP 4	4 Hours	24 Hours
DRP 5	8 Hours	24 Hours
DRP 6	24 Hours	24 Hours

- **Disaster Recovery Testing:**

  Provider will provide assistance and support as requested by Client for Client's DR testing, which occurs at least twice per year, subject to costs as mutually agreed by the parties based on the scope of the testing.

Definitions:

- **Recovery Time Objective (RTO):**
  The maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs. A "Disaster" means any event, whether natural, technological, human-caused, 3rd party caused, or acts of God, that results in a significant disruption of Provider's ability to deliver Services in accordance with the SLA. A disaster may be declared by Client. Provider may declare a "disaster" when Client is not responsive to Provider's inquiry for more than 2 hours when an unplanned event has caused a significant disruption to the Services that cannot be resolved with Provider. The declaration of a disaster will trigger the initiation of the disaster recovery process.

- **Recovery Point Objective (RPO):**
  The age of files that must be recovered for normal operations to resume if a system goes down as a result of a failure. A "Disaster" means any event, whether natural, technological, human-caused, 3rd party caused, or acts of God, that results in a significant disruption of Provider's ability to deliver Services in accordance with the SLA. A disaster may be declared by Client. Provider may declare a "disaster" when Client is not responsive to Provider's inquiry for more than 2 hours when an unplanned event has caused a significant disruption to the services that cannot be resolved with Provider. The declaration of a disaster will trigger the initiation of the disaster recovery process.

- **Patch Management SLA:**
  The following table shows the targets of response times for each priority level for patch release. If client exceeds 150 servers or 750 desktops, the Patch Cadence shall be reviewed and revised as mutually agreed upon.

CVE Severities	Patch Cadence	Missed Patches (exceeding release date SLA)
Critical	90% of patches across managed systems completed within 15 calendar days of Client approval for production.	$1,500 per SLA violation per day
High	90% of patches across managed systems completed within 22 calendar days of Client approval for production.	$1,000 per SLA violation per day
Moderate	90% of patches across managed systems completed within 30 calendar days of Client approval for production.	$500 per SLA violation per day
Low	90% of patches across managed systems completed within 90 calendar days of Client approval for production.	$250 per SLA violation per day