MANAGED SERVICE SCHEDULE

The Managed Service Schedule sets forth the Services offered by US Signal and contains specific terms and conditions for those Services. Capitalized terms not elsewhere defined in this Managed Service Schedule shall have the meaning ascribed to them in the Agreement. The additional terms and conditions set forth in this Managed Service Schedule shall apply to any Managed Services purchased by Customer.

SECTION 1 REMOTE MONITORING & MANAGEMENT ("RMM")

1.1 Description

US Signal's RMM is a server operating system and endpoint monitoring and alerting service designed to assist Customer with the ongoing management of its systems including patch management, process automation, and remediation dependent on the chosen service tier. Both physical and virtualized servers ("**Server(s)**") as well as supported network endpoints ("**Endpoints**") are monitored via the installation of software based agents into Customer's environment. Alarms are generated based on configured policies and reported directly to US Signal's Technical Operations Center ("**TOC**"). US Signal's TOC will respond to alarms when configured alert conditions or thresholds are met. Customer shall have access to US Signal's provided interface in order to view all Servers and Endpoints currently being monitored.

1.2 Approved Server List

Customer may request RMM Service by submitting to US Signal an OFS and a completed Preliminary Server List ("**PSL**"). The PSL shall identify specific server and endpoint information necessary for US Signal's Managed Services Technicians ("**MST**") to evaluate and provision the RMM Service. The MST will qualify each network device requested and determine, at its sole discretion, those acceptable for RMM Service. US Signal shall issue a revised approved server list that reflects the acceptable devices ("**Approved Server List** or **ASL**").

1.3 RMM Definitions

a. **"Automated Remediation"** is a service that may be configured to perform certain automated tasks based on policies defined and created between Customer and US Signal during the onboarding process. The Automated Remediation may be used to perform supported OS and third party application level automated tasks on Customer's behalf when pre-defined input parameters or global variables are met.
b. **"Customer Interface"** shall be the software interface that permits certain settings or features to be viewed and/or changed by Customer through the use of a read-only management portal provided by US Signal. Authorized Customer users will be supplied with a unique user name and password by US Signal.
c. **"Patch Management"** is a service that provides for manual or scheduled installation of supported OS and third party application level software patches based on policies defined and created between Customer and US Signal during the onboarding process. For the avoidance of doubt, Patch Management shall not include zero-day exploit workarounds.
d. **"Remediation"** is a service that includes the investigation of sustained alarms for the determination of a root cause for failure, as well as, options for resolution. Remediation stops at the OS level and resolution of the identified problem may result in additional fees and charges. For the avoidance of doubt, Remediation does not include any of the following:
    1. help desk tasks for Customer's end users;
    2. hardware/software/OS upgrades or installation/re-installation of the same;
    3. restoration of OSs (even from Customer provided backups) due to hardware or software failure or corruption or as a result of patching (even if performed by US Signal as part of the RMM Service), viruses, malware, or customer negligence;
    4. manual virus/malware removal; or
    5. zero-day exploit workarounds.

1.4 Rates

Monthly recurring charges ("**MRC**" or "**MRCs**") are applied per Server and/or Endpoint according to the chosen service tier and any optional services within each tier. Additional charges may apply in arrears if Customer: 1) via use of the Customer Interface makes any self-directed adjustments to the settings or features of the Services; or 2) additional Remediation fees are approved by Customer prior to US Signal conducting the work.

1.5 Service Term

The Service Term, as defined in the Agreement, begins on the date of US Signal's written notice to Customer that the Service has been successfully uploaded and is operational and continues on a month-to-month basis until such time as either party provides thirty (30) days written notice of cancellation to the other party. Customer is responsible for all charges up until the effective date of cancellation.

1.6 Service Tier Options

a. **Standard Tier**. The Standard Tier includes the following:
   1. Customer Interface access
   2. Performance reporting access
   3. 24/7/365 advanced performance monitoring of configured alarms and alerts including, but not limited to:
      i. CPU
      ii. disk space
      iii. memory
      iv. patch status
      v. connectivity
      vi. OS/application services
   4. Automated Remediation - this is an optional service, available for additional MRC per Server or Endpoint
   5. Server OS and third party Patch Management
   6. Alert management whereby Customer is notified via automated emails for incidents, problems, and/or resolution, Customer is responsible for updating US Signal of any email notification address changes by emailing MST via managedservices@ussignal.com.

b. **Premier Tier**. The Premier Tier includes the following:
   1. Customer Interface access
   2. Performance reporting access
   3. 24/7/365 advanced performance monitoring of configured alarms and alerts including, but not limited to:
      i. CPU
      ii. disk space
      iii. memory
      iv. patch status
      v. connectivity
      vi. OS/application services
   4. Automated preventative maintenance including, but not limited to:
      i. check disk
      ii. defragment
      iii. delete temporary files
      iv. firmware updates (where possible)
      v. sync time with domain controller
   5. Automated Remediation
   6. Server OS and third party Patch Management
   7. Alert management whereby US Signal's TOC receives alerts, performs alert triage and contacts Customer regarding incidents and Automated Remediation attempts if applicable (Remediation stops at the OS level and does not extend into application support)

1.7 Onboarding

a. Customer is responsible for providing all physical and communications access, privileges, environmental conditions, properly functioning hardware and software, qualified personnel, project details, material information, decisions and directions that are reasonably necessary for US Signal's performance of the onboarding.

b. US Signal is not responsible for any onboarding delays caused by Customer and may invoice Customer for any time US Signal was not able to perform the onboarding, as scheduled, due to Customer's delay or performance failure. US Signal's rate is one hundred twenty five ($125.00) dollars per hour ("**Onboarding Fee**").

c. Prior to US Signal's commencement of the onboarding, Customer shall provide written notice of any safety and/or security requirements, including but not limited to network, cloud or premise rules and procedures.

d. Either party may cancel the Service during the onboarding process by providing the other party written notice of such cancellation. The Onboarding Fee shall apply to any cancellation.

e. Upon completion of the onboarding, US Signal shall reconcile the PSL with all Servers and Endpoints onboarded and provide the final ASL to Customer.

1.8 Service Changes

Customer may request a change to the ASL by written notice to **managedservices@ussignal.com**. A change request email should include the Server or Endpoint name and IP Address. Requests to add a Server or Endpoint to the Standard Tier should also identify whether the optional Automated Remediation should be included. New monthly recurring charges shall apply accordingly. All non-service affecting changes shall be performed between 8:00 am – 5:00pm Monday through Friday, ET ("**Business Hours**"). Such Business Hours shall exclude any designated US Signal holidays.

1.9 Technical Standards of Performance

The service metrics for Managed Services can be found at https://ussignal.com/sla-agreements (the "**Service Metrics**"). In the event US Signal fails to meet the Service Metrics, Customer shall be entitled to a credit determined according to the following:

US Signal shall provide a service credit to Customer for each qualifying exception to the Response Time Objective. Credit will be equal to five (5%) percent of Customer's MRC for the affected Server or Endpoint. Service credits shall not equal more than fifty (50%) percent of Customer's total MRC cumulatively for any given month. The credit shall be Customer's sole and exclusive remedy for any failure to meet a Service Metric.

SECTION 2 ENTERPRISE BACKUP-AS-A-SERVICE ("EBAAS")

2.1 Description and Rates

Enterprise Backup-as-a-Service ("**EBaaS**") is a backup solution, specifically tailored for enterprise environments supporting: 1) server operating systems such as Microsoft Windows and Linux; 2) server applications such as Microsoft Exchange and Structured Query Language ("**SQL**"); 3) workstation operating systems such as Mac and Microsoft Windows; and 4) image level protection of virtual machines.

There are three (3) deployment options available:

- Agent-Based Deployment – agent based backup solution that can protect and restore: 1) file and application level data; and 2) server and workstation operating systems. Customer shall elect one (1) or a combination of the three (3) supported configuration options as follows: 1) local appliance for local backup and restore; 2) software agents for remote device backup; and/or 3) cloud backup target. The minimum SIT for Agent-Based Deployment is one (1) year. Within thirty (30) days of the expiration of the SIT for termed orders, Customer shall provide written notice to US Signal of its intent to either: i) renew the Services for a new, minimum of one (1) year SIT; or ii) terminate the Services at the end of the SIT.
- Image-Based Deployment – agentless backup solution that is available to virtual machines running within the multi-tenant IaaS (Infrastructure-as-a-Service). Restorations are available for the entire image level as documented in the EBaaS Design Document. Imaged-Based Deployment may be purchased either on a month-to-month basis whereby recurring rates may be subject to change upon thirty (30) days' written notice, or on a one year SIT whereby Customer's rates are discounted for the term. Within thirty (30) days of the expiration of the SIT for termed orders, Customer shall provide written notice to US Signal of its intent to either: i) renew the Services for a new, minimum of one (1) year SIT; or ii) terminate the Services at the end of the SIT.
- Blended Deployment – combination of the Agent-Based Deployment and Image-Based Deployment solutions. The minimum SIT for Blended Deployment is one (1) year. Within thirty (30) days of the expiration of the SIT for termed orders, Customer shall provide written notice to US Signal of its intent to either: i) renew the Services for a new, minimum of one (1) year SIT; or ii) terminate the Services at the end of the SIT.

US Signal shall: 1) operate and manage two (2) geographically diverse data center backup and replication storage targets; and 2) manage the provisioning of EBaaS including the installation of client software, creation of backup jobs, retention schedules and remote monitoring. Upon commencement of the SIT for EBaaS, US Signal shall: 1) manage the backup jobs; 2) provide proactive response for backup and infrastructure alerts; and 3) process restores as requested by Customer, subject to the Rates set forth below.

All associated MRCs and NRCs for EBaaS are ICB which may comprise any of the following:

a. **EBaaS Agent Data MRC:** Customer's aggregate data calculated by the total amount of data in a single full backup of all data (in GBs) comprising Customer's EBaaS protected systems ("**Front-End Data**") as reported monthly by the backup software, multiplied by the rate per GB, as identified in the applicable OFS.
b. **EBaaS Image Data MRC:** Customer's aggregate data calculated by the actual storage (GB) consumed each month multiplied by the rate per GB on the OFS ("**Back-End Data**").
c. **EBaaS Appliance MRC:** CPA, as described in Section 2.5 herein (if any), as identified in the applicable OFS.
d. **EBaaS Management MRC:** Based on the number of protected systems at the rate identified on the OFS.
e. **EBaaS Setup NRC:** Installation charge based on the number of protected devices.
f. **EBaaS Support NRC:** Applies to restoration requests as defined herein.

In the event Customer experiences an event that requires restoration efforts ("**EBaaS Restoration Event**"), Customer shall declare such event by opening a trouble ticket with US Signal's TOC at 888.663.1700 or toc@ussignal.com. US Signal shall invoice Customer an EBaaS Support NRC for the EBaaS Restoration Event according to the following table:

EBaaS Restoration Event	EBaaS Support NRC (per quarter hour)
First 30 Minutes	$0.00
> 30 Minutes	$25.00

Billing for an EBaaS Restoration Event shall be based on actual technician time as recorded in US Signal's third party software. US Signal shall invoice Customer in increments of fifteen (15) minutes, or fraction thereof, rounded up to the nearest whole increment.

2.2 FastPath (Optional)

FastPath provides Customer a private connection between Customer's' EBaaS and its applicable US Signal Cloud Service. FastPath shall include a Fixed Port with a Cloud Based Managed Security appliance. Customer shall provide US Signal one (1) of Customer's IP addresses for the provisioning of FastPath. All associated MRCs for FastPath are on an individual case basis ("**ICB**").

2.3 EBaaS Design Document

Customer is solely responsible for working with US Signal to establish the initial EBaaS Design Document within thirty (30) days of engagement by US Signal personnel and maintaining such EBaaS Design Document by providing US Signal updates when applicable. The "**EBaaS Design Document**" shall include such items as authorized contacts, information about the protected systems and all the notable components and processes to restore Customer's protected systems. US Signal shall retain one (1) current version of the EBaaS Design Document in order for US Signal to perform EBaaS.

2.4 Responsibilities of Customer

Customer is solely responsible for: (a) power and environmental condition of the CPA in Customer's possession, if any; (b) providing US Signal ten (10) business days' written notice of adding any new protected systems to its existing EBaaS; (c) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (d) its compliance with all laws in connection with the Services under the Agreement; (e) loss of stored data resulting from an act by Customer; (f) the integrity of its data; (g) any host-based anti-virus, malware or spyware unless purchased through a Service; (h) the on and/or off-Boarding of Customer's data onto the Services; and (i) maintaining an interoperable software version compatible with US Signal's current software version. Upgrading or patching software versions without confirmation of interoperability shall void all US Signal responsibilities in relation to this product including Outage Credits.

2.5 Customer Premise Appliance

a. In the event Customer elects a Customer Premise Appliance ("**CPA**"), US Signal shall provide Customer the applicable CPA as described in the corresponding OFS or MS Request. Customer shall create a local or domain access VM in its environment to serve as a jump box for US Signal to access the CPA. Such device shall have; 1) Windows XP (at minimum) or later version; 2) 2.0 GB of RAM; 3) the same network as the CPA; and 4) accessibility via the Internet. Such CPA is considered US Signal's equipment. Customer shall provide adequate space and power within six (6) feet of the equipment placement location. Customer agrees not to open, alter, misuse, tamper with or remove the CPA. Customer will not remove any markings or labels or serial numbers from the CPA. Customer will safeguard the CPA from loss or damage of any kind, and will not permit anyone other than a representative authorized by US Signal to perform any work on the CPA. If the CPA is damaged, destroyed, lost or stolen while in Customer's possession, Customer shall be liable

for the cost of repair or replacement of such CPA. Prior to installation of the CPA, Customer shall notify US Signal of any special requirements regarding the placement of the CPA. Any request, post installation, to relocate the CPA will result in additional non-recurring charges. Within sixty (60) days of termination of the Service's SIT, US Signal shall retrieve the CPA at its own cost.

b. Any maintenance or changes in addition to what is outlined in the OFS or MS Request will be coordinated with the Customer and may result in additional non-recurring charges. US Signal agrees to maintain its CPA in accordance with the terms described in the OFS or MS Request. If an event occurs whereby Customer desires additional support resulting in manufacturer support charges Customer shall be responsible for such charges.

2.6 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

2.7 EBaaS Outage Credits

In the event US Signal fails to meet the applicable metric identified in the technical standards of performance in Section 2.6 above ("**EBaaS Outage**"), Customer shall be entitled to a credit determined according to the following tables:

Availability Credit:

Length of EBaaS Outage (hours)	EBaaS Availability Credit
< 4 Hours	0% of EBaaS Data MRC
4 – 6 Hours	10% of EBaaS Data MRC
6 – 8 Hours	25% of EBaaS Data MRC
8 – 10 Hours	40% of EBaaS Data MRC
> 10 Hours	50% of EBaaS Data MRC

Such MRC shall be based upon the previous month's EBaaS Data MRC. In no event will EBaaS outage credits for US Signal's failure to meet the availability metric for any one (1) month exceed one hundred percent (100%) of the current month's charges for the applicable EBaaS Data MRC.

Response Time:

Length of Response	EBaaS Credit
SLA + 1 Hour	10% of EBaaS Support NRC
SLA + 2 Hours	20% of EBaaS Support NRC
SLA + 3 Hours	30% of EBaaS Support NRC
SLA + 4 Hours	40% of EBaaS Support NRC
SLA + 5 Hours	50% of EBaaS Support NRC
SLA + 6 Hours	60% of EBaaS Support NRC
SLA + 7 Hours	70% of EBaaS Support NRC
SLA + 8 Hours	80% of EBaaS Support NRC
SLA + 9 Hours	90% of EBaaS Support NRC
SLA + 10 Hours	100% of EBaaS Support NRC

In no event will credits for EBaaS Restoral for any one (1) month exceed one hundred percent (100%) of the NRC for the applicable EBaaS Support NRC.

2.8 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services

team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 3 MANAGED BACKUP FOR BAAS

3.1 Description and Rates

Managed Backup for BaaS utilizes US Signal's chosen software. US Signal shall: 1) operate and manage two (2) geographically diverse data center storage targets for Customer backups; 2) install the underlying agent software; 3) remediate any third party backup agent software issues; 4) create and modify any backup schedules and retention plans ("**Managed Backup Adjustments**") as directed by Customer, provided that such Managed Backup Adjustments are requested during Business Hours as identified in Section 1.8 herein; 5) monitor the backups for success or failure; 6) if within a twenty four (24) hour period Customer's Managed Backup experiences consecutive single endpoint backup failures, then US Signal shall notify Customer; and 7) restore any of Customer's files, folders, images or Microsoft 365 data to its source only. For the avoidance of doubt, restoration shall not include the creation of any new virtual machines, installation of OSs or the restoration of files and/or images to endpoints that are not visible and online within the third party software's management portal. Customer shall select one (1) of the two (2) data center targets from the available US Signal data centers. Customer's data shall be hosted on object based storage with erasure coding. At US Signal's sole discretion, US Signal may test its restoration of any backups for validity of the backup functionality. Managed Backup shall only be available in conjunction with BaaS. There are two ways to purchase Managed Backup for BaaS:

a. Managed Backup for BaaS may be purchased on a month-to-month term whereby recurring charges are based upon monthly storage consumption. US Signal may change monthly recurring rates for Managed Backup upon thirty (30) days' written notice. Customer may terminate Managed Backup at any time upon five (5) business day's prior written notice. Customer shall be responsible for all recurring charges up until the date of termination. In the event Customer's Consumed Data equals zero (0) for more than ninety (90) consecutive calendar days, then US Signal may terminate the applicable Managed Backup upon ten (10) days written notice; or

b. Managed Backup for BaaS may be purchased on a term ("**Managed Backup Minimum**") whereby Customer's charges are discounted by committing to a minimum data consumption threshold invoiced as an MRC each month. Any data consumed beyond the Managed Backup Minimum threshold is priced according to the per GB rate on the service's OFS. Cancellation of BaaS Minimum service prior to the expiration of its SIT is subject to the Early Termination charges as described in the Agreement.

   Customer's actual storage (GB) consumed each month ("**Consumed Data**") shall be monitored using third party software. Billing periods shall commence on the first (1st) of the month and end on the last day of the month. Consumed Data shall be calculated on the amount of Customer's data present in the BaaS environment on the last day of the billing period. Such recurring charges shall be billed in arrears according to the following formula:

   Price per GB X actual GB Consumed Data by Customer during the previous month = BaaS Usage Charge MRC

All associated MRCs and NRCs for Managed Backup are ICB which may comprise any of the following including the purchase options listed above:

1. **Backup Management Fee MRC:** The maximum number of supported and managed endpoints X the management rate, as identified in the applicable OFS.
2. **Managed Backup Setup NRC:** Installation charge based on the number of supported and managed endpoints as identified in the quote. During the Service Term, if Customer adds endpoints to the Managed BaaS then this NRC shall apply. For the avoidance of doubt, if Customer terminates an endpoint, then requests such endpoint is added back to the Service, then this Managed Backup Setup NRC shall apply to the applicable endpoint.
3. **Managed Backup Support NRC:** Applies to Managed Backup restoration requests as defined herein.
4. **Backup Management Fee – M365 Objects:** Based maximum number of managed Microsoft 365 Objects X the management rate, as identified in the applicable OFS. Objects consist of users, public folders, Teams and SharePoint Sites.

In the event Customer experiences an event that requires restoration efforts ("**Managed Backup Restoration Event**"), Customer shall declare such event by opening a trouble ticket with US Signal's TOC at 888.663.1700 or toc@ussignal.com. US Signal shall invoice Customer a Managed Backup Support NRC for the Managed Backup Restoration Event according to the following table:

Managed Backup Restoration Event	Managed Backup Support NRC (per quarter hour)
First 30 Minutes	$0.00
> 30 Minutes	$25.00

Billing for a Managed Backup Restoration Event shall be based on actual technician time as recorded in US Signal third party software. US Signal shall invoice Customer in increments of fifteen (15) minutes, or fraction thereof, rounded up to the nearest whole increment.

3.2 FastPath (Optional)

FastPath provides Customer a private connection between Customer's' Managed Backup storage location and its applicable US Signal Cloud Service. FastPath shall include a Fixed Port with a Cloud Based Managed Security appliance. Customer shall provide US Signal one (1) of Customer's IP addresses for the provisioning of FastPath. All associated MRCs for FastPath are on an individual case basis ("**ICB**").

3.3 Advanced Backup (Optional)

Advanced Backup provides additional backup features such as expanded backup support for Microsoft SQL Clusters, Microsoft Exchange Clusters, Maria DB, MySQL, Oracle DB, and SAP HANA. Advanced Backup also provides continuous data protection, data protection map and compliance reporting, and off-host data processing.

Advanced Backup offers the follow types of workloads:

a. Advanced Backup – Server: Workload for backups of physical servers.
b. Advanced Backup – VM: Workload for backups of virtual servers.
c. Advanced Backup – Host: Workload for backups of host servers.
d. Advanced Backup – Workstation: Workload for backups of workstations.
e. Advanced Backup – M365: Workload for backups of a Microsoft 365 seat.
f. Advanced Backup – Google Workspace: Workload for backups of a Google Workspace seat.

Advanced Backup is charged at a per agent rate identified on the OFS. The rate is determined by the type of workload.

3.4 Responsibilities of Customer

Customer is solely responsible for: (a) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (b) its compliance with all laws in connection with the Services under the Agreement; (c) loss of stored data resulting from an act by Customer; (d) the integrity of its data; (e) any host-based anti-virus, malware or spyware unless purchased through a Service; and (f) the on and/or off-Boarding of Customer's data onto the Services; (g) access to each endpoint, as necessary, for the installation and remediation of the backup agent software; (h) providing US Signal ten (10) business days written notice of any change or addition to the endpoints; (i) providing US Signal's TOC adequate information in order to troubleshoot service related issues; (j) notifying US Signal of any backup agent software issues; and (k) notifying US Signal of restoration events.

3.5 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

3.6 Response Credits

In the event US Signal fails to meet the technical standards of performance in Section 3.5 above, Customer shall be entitled to a response time credit determined according to the following table:

Response Time:

Length of Response	Backup Management Fee ("BMF") MRC Credit
SLA + 1 Hour	10% of BMF MRC
SLA + 2 Hours	20% of BMF MRC

SLA + 3 Hours	30% of BMF MRC
SLA + 4 Hours	40% of BMF MRC
SLA + 5 Hours	50% of BMF MRC

In no event will response time credits for a response time for any one (1) month exceed fifty percent (50%) of the Backup Management Fee MRC.

3.7 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 4 RECOVERY-AS-A-SERVICE ("RAAS")

4.1 Description and Rates

Recovery-as-a-Service ("**RaaS**") is an enhancement to US Signal's BaaS and Managed Backup services, whereby in the event of a disaster, US Signal shall manage the recovery of Customer's backups into a US Signal hosted compute environment. For the avoidance of doubt, Customer must utilize US Signal's BaaS to be eligible for RaaS. Customer shall elect either: 1) an on-demand; or 2) reserved compute environment. An on-demand compute environment means that US Signal shall not pre-provision a compute environment; therefore, all necessary components will be provisioned at the time of disaster declaration ("**On-Demand Compute Environment**"). Such On-Demand Compute Environment shall only be available in conjunction with Multi-Tenant Cloud Resource Pools and Multi-Tenant Cloud Compliant Resource Pools. A reserved compute environment means that US Signal shall provide Customer a pre-provisioned environment and such environment shall remain in an active state and available for backup restores in the event of a disaster ("**Reserved Compute Environment**"). Such Reserved Compute Environment shall only be available in conjunction with Multi-Tenant Cloud Resource Pools, Multi-Tenant Cloud Compliant Resource Pools or Single-Tenant Cloud Service. There are two ways to purchase RaaS:

a. RaaS may be purchased on a month-to-month term whereby Customer's charges are based upon the actual number of virtual machines documented in Customer's RaaS Playbook. Customer may terminate RaaS at any time upon five (5) business days prior written notice. Customer shall be responsible for all recurring charges up until the date of termination; or,

b. RaaS may be purchased on a term ("**RaaS Minimum**") whereby Customer's charges are discounted by committing to a specific term invoiced as an MRC each month. Cancellation of RaaS Minimum service prior to the expiration of its SIT is subject to the Early Termination charges as described in the Agreement.

Recurring charges are based upon the actual number of virtual machines documented in Customer's RaaS Playbook. Billing shall commence on the first (1st) of the month and end on the last day of the month. Any changes to the number of virtual machines as identified in the RaaS Playbook shall be: 1) prorated according to the actual number of days such machine(s) are added and/or removed from the RaaS Playbook; and 2) reflected in the next month's billing cycle according to the rates identified in the OFS.

4.2 RaaS Playbook

Customer is solely responsible for working with US Signal to establish a disaster recovery playbook within thirty (30) days of engagement by US Signal personnel and maintaining such RaaS Playbook. The "**RaaS Playbook**" shall include all the necessary components and processes to restore Customer's environment. US Signal shall retain one (1) current version of the RaaS Playbook in order for US Signal to perform RaaS.

4.3 RaaS Disaster Event and Testing

In the event Customer experiences a disaster that requires RaaS ("**RaaS Disaster Event**") or desires to test the RaaS ("**RaaS Test Event(s)**"), Customer shall declare such event by opening a trouble ticket with US Signal's TOC at 888.663.1700 (collectively "**RaaS Event**"). US Signal shall invoice Customer for the RaaS Event according to the following table, including virtual environment fees:

RaaS Event	NRC (per quarter hour)
Disaster Event	$62.50
Test Event	$25.00
Recovery Environment	**NRC (for the duration of any RaaS Event)**
Compute	$5.00 per Ghz
Memory	$5.00 per GB
Storage	$0.15 per GB

Customer shall be eligible for up to two (2) free RaaS Test Events that last up to forty eight (48) consecutive hours during any three hundred and sixty five (365) consecutive day period commencing on the first (1st) day of the SIT. Any RaaS Test Event that: 1) last longer than forty eight (48) hours; or 2) exceeds the two (2) free RaaS Test Events shall be billed according to the RaaS Event NRC as identified above. Billing for a RaaS Event shall commence upon Customer's declaration of such event to US Signal's TOC and end upon Customer's confirmation to US Signal's TOC that RaaS support is no longer needed by Customer. US Signal shall invoice Customer in increments of fifteen (15) minutes or fraction thereof rounded up to the nearest whole increment.

4.4 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for RaaS technical standards of performance. For Reserved Compute Environment services, additional technical standards of performance shall be found in the applicable RaaS Playbook.

4.5 Outage Credits

In the event US Signal fails to meet the technical standards of performance for RaaS as identified in Section 4.4, then Customer shall be entitled to a credit equal to 100% of the RaaS MRC for that month.

An event shall be deemed to have commenced upon notification by Customer to US Signal's TOC of a RaaS Disaster Event. Each RaaS Disaster Event shall be deemed to end upon Customer's confirmation to US Signal's TOC that RaaS support is no longer needed by Customer. Periods of Planned Maintenance and Repair will not be excluded when calculating RaaS Outage Credits. In no event will Outage credits for RaaS for any one (1) month exceed one hundred percent (100%) of the current month's charges for the applicable RaaS.

4.6 Responsibilities of Customer

Customer is solely responsible for: (a) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (b) its compliance with all laws in connection with the Services under the Agreement; (c) loss of stored data resulting from an act by Customer; (d) the integrity of its data; (e) any host-based anti-virus, malware or spyware unless purchased through a Service; and (f) the on and/or off-Boarding of Customer's data onto the Services.

SECTION 5 DISASTER RECOVERY AS A SERVICE ("DRAAS")

5.1 Description

Disaster Recovery-as-a-Service ("**DRaaS**") is a managed service whereby US Signal shall manage the protection and recovery of Customer's production server environment by utilizing its third party vendor's virtual replication technology. US Signal shall manage the installation of all applicable applications to support the replication operation in both Customer's production and replication sites. Customer may elect to purchase DRaaS on either a month-to-month or single to multi-year term as follows:

a. Month-to-month term - US Signal may change monthly recurring rates for DRaaS upon thirty (30) days' prior written notice. Customer may terminate DRaaS at any time upon five (5) business day's prior written notice.

b. Single or Multi-year term ("**Termed DRaaS**") - Customer commits to a term specified on the Ordering Document. Rates shall remain unchanged during the SIT. Cancellation of Termed DRaaS prior to the expiration of its SIT is subject to the Early Termination charges as described in the Agreement.

5.2 Rates

DRaaS consists of both recurring and non-recurring charges described as follows:

a. Recurring charges include: 1) the average number of virtual machines replicated per calendar month as reported by the replication software ("**VM Replication Fee**"); and 2) the replication site storage ordered on the Ordering Document and further documented in the DRaaS Playbook during the SIT ("**DRaaS Storage**").

i. VM Replication Fee:

$$\frac{\text{Sum total of servers replicated per day within the applicable calendar month X rate per VM}}{\text{Number of days in the applicable calendar month}} = \text{VM Replication Fee}$$

ii. DRaaS Storage Fee: rate on Ordering Document based on initial storage allocation. Fees are adjusted in subsequent months based on GB used over the initial allocation determined by the original rate per GB.

b. Non-recurring or event-based charges apply when Customer experiences a disaster that requires DRaaS ("**DRaaS Disaster Event**") or desires to test DRaaS ("**DRaaS Test Event(s)**"), (collectively "**DRaaS Event**"). In the event of a DRaaS Event, US Signal shall invoice Customer on a usage basis for: 1) the Compute and Memory, as described in the Cloud Service Schedule, used per day according to the rates on the Ordering Document; plus 2) the DRaaS Event support rates according to the following table:

DRaaS Event	NRC (per quarter hour)
Disaster Event	$62.50
Test Event	$25.00

Customer shall be eligible for up to two (2) free DRaaS Test Events that last up to forty eight (48) consecutive hours during any three hundred and sixty five (365) consecutive day period commencing on the first (1st) day of the SIT. Any DRaaS Test Event that: 1) last longer than forty eight (48) hours; or 2) exceeds the two (2) free DRaaS Test Events shall be billed according to the DRaaS Event NRC as identified above plus the Compute and Memory charges. Billing for a DRaaS Event shall cover the interval of time from DRaaS Declaration to DRaaS Conclusion as further described in Section 5.6. US Signal shall invoice Customer in increments of fifteen (15) minutes or fraction thereof rounded up to the nearest whole increment.

5.3 Layer 2 Extension (Optional)

Layer 2 Extension provides Customer a private Layer 2 VPN connection between Customer's equipment at its Ground site and its applicable US Signal Cloud Service. Layer 2 Extension includes a VMware NSX Edge instance to allow the same subnet to exist in both the Ground site and US Signal Cloud. Layer 2 Extension may be purchased on a term or month-to-month basis and all associated MRCs are on an individual case basis ("**ICB**").

5.4 Configuration Requirements

The following are additional service requirements for DRaaS:

a. Customer shall elect one (1) of the following US Signal DRaaS production/replication designs:
   1. Customer owned and operated environment ("**Ground**") to a US Signal Cloud Service described in the Cloud Service Schedule ("**Cloud**");
   2. Cloud to Cloud;
   3. Cloud to Ground; or
   4. If Customer chooses a second target environment in addition to its design choice above, ("Multi-Cloud Replication"), Customer's second target design must also be identified on the OFS.

b. Customer shall designate a DRaaS tier of service for protected VMs as further described in Section 5.5, herein.

c. In the event Customer elects a design that includes a Ground component, Customer shall be responsible for the stability, quality and condition of Customer supplied equipment required to support DRaaS.

d. In the event Customer elects a design that includes a Cloud component, Customer shall also purchase hosting components approved by US Signal for DRaaS as described under the Cloud Service Schedule.

e. In the event Customer elects a Ground to Cloud configuration or in the event remote access is required to recover Services, Customer shall purchase a US Signal CBAS or CBAS+ along with a DIA Port as described under the Cloud Service Schedule for proper connectivity.

f. Customer shall elect up to five (5) consecutive calendar days' cumulative data retention for replicated data.

g. No individual VM shall exceed 32 vCPUs.

5.5 DRaaS Service Tiers

DRaaS is offered with two service tier options: Premium and Standard. The service tier designation shall be documented on the Ordering Document and in detail in the completed DRaaS Playbook. Protected virtual machines shall receive the level of service as summarized in the following table and further described below:

	DRaaS Tiers	
	Premium	**Standard**
Annual Testing	Included	Included
Playbook Creation	Included	Included
Event Restoration Priority	Primary	Secondary
Storage Performance	Standard	Best Effort
Resource Capacity Objective (RCapO)	100%	Best Effort
RTO SLA	As Tested	Best Effort

- Annual Testing: as further described in Section 5.2 – DRaaS Test Event
- Event Restoration Priority: Premium virtual machines shall get priority restoration above Standard virtual machines
- Storage Performance: Premium workloads are ensured the storage performance as ordered and defined by the Platinum, Silver and Gold storage in Section 1.1.a of the Cloud Service Schedule. For Standard workloads, the storage performance is best effort
- RCapO: Premium workloads are ensured the full compute, memory and storage capacity requirements as documented in the DRaaS Playbook, Standard workloads receive resources based on availability
- SLA: Premium workloads receive a tested and documented RTO SLA in the DRaaS Playbook, the SLA does not apply to Standard workloads as the RTOs may vary based on the failure type and Restoration Priority

5.6 DRaaS Event Operation

The declaration of a DRaaS Event may be dependent on the design of the solution ("**DRaaS Declaration**"):

a. For DRaaS with a Ground source location, Customer shall declare a DRaaS Event by calling the TOC at 888.663.1700 or by emailing toc@ussignal.com.

b. For DRaaS with a Cloud source location, Customer may declare a DRaaS Event by calling the TOC at 888.663.1700 or by emailing toc@ussignal.com. In the case of an entire US Signal datacenter failure, US Signal shall independently declare a DRaaS Disaster Event for Premium tier servers and begin the failover process without Customer declaration.

Regardless of the DRaaS design, a DRaaS Event shall end upon Customer's notification to US Signal that US Signal support is no longer required ("DRaaS Conclusion").

5.7 Responsibilities of Customer

Customer is solely responsible for working with US Signal to establish a disaster recovery playbook within thirty (30) days of engagement by US Signal personnel and maintaining such DRaaS Playbook. The "**DRaaS Playbook**" shall include all the necessary components and processes to restore Customer's environment to the replications site in the event of a disaster or test scenario. US Signal shall retain one (1) current version of the DRaaS Playbook in order for US Signal to perform DRaaS. Customer is also solely responsible for: (a) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (b) its compliance with all laws in connection with the Services under the Agreement; (c) loss of stored data resulting from an act by Customer; (d) the integrity of its data; (e) any host-based anti-virus, malware or spyware unless purchased through a Service; (f) the on and/or off-Boarding of Customer's data onto the Services; and (g) maintaining an interoperable software version compatible with US Signal's current software version. Upgrading or patching software versions without confirmation of interoperability shall void all US Signal responsibilities in relation to this product, including Outage Credits.

5.8 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for DRaaS technical standards of performance.

5.9 Outage Credits

In the event US Signal fails to meet the technical standards of performance identified in Section 5.8 above, then Customer shall be entitled to a restoral credit equal to 100% of the DRaaS MRC.

A DRaaS Event shall be deemed to have commenced upon notification by Customer to US Signal's TOC of an event requiring DRaaS. Each DRaaS Event shall be deemed to end upon Customer's confirmation to US Signal's TOC that DRaaS support is no longer needed by Customer. Periods of Planned Maintenance and Repair will not be excluded when calculating DRaaS Outage Credits. In no event will performance credits for DRaaS for any one (1) month exceed one hundred percent (100%) of the current month's charges for the applicable DRaaS.

5.10 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 6 ENTERPRISE REPLICATION ("EREPLICATION")

6.1 Description

Enterprise Replication ("**EReplication**") is a data protection solution whereby US Signal manages its cloud-hosted target systems for the offsite replication of Customer data. EReplication supports the native replication of EMC Avamar and Data Domain integrated systems or EMC Data Domain independent systems. US Signal shall: 1) operate and manage two (2) geographically diverse data center replication targets; and 2) manage the provisioning of EReplication. EReplication shall include the configuration of Customer's applicable equipment. Upon commencement of the EReplication SIT, US Signal shall: 1) provide proactive response for replication and infrastructure alerts; and 2) assist with restorations as requested by Customer, subject to the Rates set forth in Section 6.3 below.

6.2 Term

The minimum SIT for EReplication is one (1) year. Within thirty (30) days of the expiration of the SIT, Customer shall provide written notice to US Signal of its intent to either: i) renew the Services for a new, minimum of one (1) year SIT; or ii) terminate the Services at the end of the SIT.

6.3 Rates

All associated charges for EReplication are on an individual case basis ("ICB").

a. **EReplication Data MRC:** Customer's actual storage (GB) consumed each month multiplied by the rate per GB on the OFS.
b. **Additional MTree MRC:** Total MTrees replicated per node minus one (1) MTree multiplied by the MTree rate on the OFS.
c. **EReplication Setup NRC:** Installation charge based on the number of replicating source nodes.
d. **EReplication Support NRC:** Applies to restoration requests as defined herein.

Customer's EReplication Data Charge MRC shall: 1) apply to the applicable Avamar and/or Data Domain systems as selected by Customer; 2) be monitored by US Signal's third party software; and 3) billed in arrears. The Additional MTree Charge MRC shall only apply to replication of Data Domain systems.

In the event Customer experiences an event that requires restoration efforts ("**EReplication Restoration Event**") Customer shall declare such event by opening a trouble ticket with US Signal's TOC at 888.663.1700 or toc@ussignal.com. US Signal shall invoice Customer an EReplication Support Charge NRC for the EReplication Restoration Event according to the following table:

EReplication Restoration Event	EReplication Support NRC (per quarter hour)
First 30 Minutes	$0.00
> 30 Minutes	$25.00

Billing for an EReplication Restoration Event shall be based on actual technician time as recorded in US Signal third party software. US Signal shall invoice Customer in increments of fifteen (15) minutes or fraction thereof rounded up to the nearest whole increment.

6.4 Responsibilities of Customer

Customer is solely responsible for: (a) power and environmental conditions of the CPA in Customer's possession; (b) providing US Signal at least ten (10) business days' written notice of adding any new systems to its existing EReplication service; (c) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (d) its compliance with all laws in connection with the Services under the Agreement; (e) loss of stored data resulting from an act by Customer; (f) the integrity of its data; (g) any host-based anti-virus, malware or spyware unless purchased through a Service; (h) the on and/or off-boarding of Customer's data onto the Services; and i) maintaining an interoperable software version compatible with US Signal's current software version. Upgrading or patching software versions without confirmation of interoperability shall void all US Signal responsibilities in relation to this product including Outage Credits.

6.5 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

6.6 EReplication Credits

In the event US Signal fails to meet the technical standards of performance above in Section 6.5 ("**EReplication Outage**"), Customer shall be entitled to a credit determined according to the following tables:

Availability Credit:

Length of EReplication Outage	EReplication Credit
< 4 hours	0% of EReplication Data MRC
4 – 6 hours	10% of EReplication Data MRC
6 – 8 hours	25% of EReplication Data MRC
8 – 10 hours	40% of EReplication Data MRC
> 10 hours	50% of EReplication Data MRC

Such MRC shall be based upon the previous month's respective EReplication Data MRC. In no event will EReplication Outage Credits for any one (1) month exceed one hundred percent (100%) of the current month's charges for the applicable EReplication Data.

Response Time:

Length of Response	EReplication Credit
SLA + 1 Hour	10% of EReplication Support NRC
SLA + 2 Hours	20% of EReplication Support NRC
SLA + 3 Hours	30% of EReplication Support NRC
SLA + 4 Hours	40% of EReplication Support NRC
SLA + 5 Hours	50% of EReplication Support NRC
SLA + 6 Hours	60% of EReplication Support NRC
SLA + 7 Hours	70% of EReplication Support NRC
SLA + 8 Hours	80% of EReplication Support NRC
SLA + 9 Hours	90% of EReplication Support NRC
SLA + 10 Hours	100% of EReplication Support NRC

In no event will credits for EReplication response for any one (1) month exceed one hundred percent (100%) of the applicable EReplication Support NRC.

6.7 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 7 WEBSITE AND APPLICATION SECURITY ("WaAS")

7.1 Description

Website and Application Security is a US Signal managed service providing security for websites and applications including Distributed Denial of Service Protection ("**DDoS Protection**"). US Signal and Customer will participate in a discovery call to gather technical requirements prior to provisioning the services. US Signal shall configure the initial service based on specific Customer requirements and provide configuration support for any changes upon request. Configuration changes and general support requests can be made by contacting the TOC. Website and application traffic is automatically routed to a global Anycast network of datacenters. Malicious requests are filtered using third party software and human engineering interaction ("**Partner Service**"). The filtered traffic is allowed to pass to the website origin server and/or the application origin server.

7.2 Website and Application Security Tier Options

Service is available in two feature tiers and can also include optional enhancement features:

a. **Standard Tier**. The Standard Tier includes the following:

1. Multilayer DDoS Mitigation - Volumetric protection with global Anycast network to absorb up to 30Tbps of traffic
2. Authoritative DNS with reverse proxy
3. Content Delivery Network (CDN) – Globally distributed CDN
4. Firewall
    i. IP Reputation Database with preconfigured security levels
    ii. IP Firewall Rule Sets
5. Web Application Firewall - Application protection that learns from threat intelligence gathered from worldwide internet domains. Includes up to 25 custom rulesets in addition to prebuilt rulesets
6. SSL Management - The application and management of SSL for subscribed websites including up to one customer provided SSL certificate

7. Advanced Analytics - Monitoring and reporting of threats, analytics and audit logs
8. Available DNSSEC – DNS authentication to prevent DNS spoofing

b. **Premium Tier**. The Premium Tier includes the Standard Tier features in addition to the following:

1. Rate Limiting - Custom protection that limits requests for specific API endpoints and webpages
2. Spectrum - Extends IP firewall and SSL encryption to TCP and UDP ports
3. WAF – Allows for the creation of an unlimited number of custom rulesets
4. Network prioritization – Web assets are placed on dedicated IP ranges, providing prioritized routing and protection
5. Access to raw logs
6. Upload multiple SSL certificates

c. **Optional Features**. The following can be added to Standard Tier or Premium Tier service:

1. Cloud Load Balancer - Automatically adjusts to failures while load balancing traffic across up to five (5) servers
2. Access Identity Management – Provides secure access to applications without a VPN by leveraging multiple existing identity providers and authenticating at the perimeter
3. Javascript Workers – Build serverless applications that exist on the network edge
4. Rate Limiting – Configure rules that restrict the number of requests made on specific web pages

d. The following optional features can only be added to Premium Tier service:

1. Argo Tunnel and Smart Routing – Optimizes edge network routing and uses a software daemon on the origin server to create a persistent, encrypted tunnel between origin and nearest edge server allowing origin servers to serve all traffic directly through edge servers
2. Bot Management – Combines behavioral analysis and machine learning to block malicious bot requests

7.3 Term

Customer may request WaAS Services via an OFS. The minimum SIT for WaAS Service is one (1) year. Flat rated Optional Features shall run coterminous with the WaAS Service's term. Upon expiration of the SIT, the WaAS Service and any Optional Features shall be automatically renewed for an additional one (1) year term, at the then current rates, unless either party provides the other party with written notice of its intent not to renew at least thirty (30) days prior to the expiration of the SIT.

7.4 Rates

Monthly recurring charges ("MRCs") apply for Internet domain names where the Service is requested. MRC rate is determined by the WaAS Tier Package, egress traffic estimates, and the number of domains included as documented on the OFS. A Non-recurring charge ("NRC") applies for installation of the Service at the rate identified on the OFS. The rates for any Optional Features are determined on an ICB and are subject to a monthly recurring charge, billed in advance.

7.5 Service Upgrades

Customer may upgrade its existing Standard Tier to the Premier Tier by executing an OFS whereby the original Service is not considered terminated. Upgrading from an existing Standard Tier to the Premier Tier is not considered coterminous and will require a new minimum one (1) year SIT. Upgraded tiers cannot be downgraded during the SIT. Any Optional Features ordered with a Standard Tier will be cancelled when upgrading to the Premium Tier. To continue using an Optional Feature when upgrading to the Premium Tier, Customer may need to purchase any Optional Feature(s) that are not already included in the Premium Tier. Optional Features can be added via an executed OFS and shall be considered coterminous to the applicable tier's SIT if they are added in conjunction with the new SIT. Optional Features that are added after the current SIT has begun are not considered coterminous with the original SIT and will require a new minimum one (1) year SIT. Optional Features will be billed at a monthly flat rate identified on the OFS.

7.6 Responsibilities of Customer

Customer is responsible for notifying US Signal's TOC once it has determined that a web-based cyber-attack, such as a DDoS attack, is being experienced. US Signal may make recommendations to Customer to improve the effectiveness of the service or to deal with specific issues, however, the actions taken with respect to any recommendations are the responsibility of Customer. Customer is responsible for providing proper disclosures or notices to meet any compliance obligations. Website and Application Security uses cookies and may require specific notifications to be used on Customer's website to meet GDPR and other compliance standards.

7.7 US Signal TOC Response and Website Updates

Upon Customer's request or notification of a cyber-attack, US Signal's TOC will evaluate the potential configuration changes or cyber-attack and may make configuration changes depending on both the type and severity of the attack. Additionally, in providing the Service, US Signal may update website(s) for Customer's benefit, based on the applicable settings, in order to, among other things: a) intercept requests determined to be threats and present them with a challenge page; b) add cookies to a domain to track visitors, such as those who have successfully passed the CAPTCHA on a challenge page; c) add scripts to a website(s) to, for example, improve page load performance, add services, enable apps, or perform additional performance tracking; d) add or remove response headers based on edge-side code; e) detect email addresses and replace them with a script in order to keep them from being harvested: and/or f) make other changes to increase the performance or security of a website(s). US Signal will describe to Customer how each such update works and, if necessary, work with Customer on a mechanism to disable an update.

7.8 US Signal Support Escalations

Depending on the type of request or the severity of a cyber-attack, US Signal's TOC may choose to escalate to the US Signal Security Operations Center (SOC). Customer requests that are escalated to the SOC, including cyber-attacks, will be evaluated and the SOC will take one or more of the following actions:

1. Make configuration changes.
2. Provide a quote for analyst work to fulfill request or mitigate a cyber-attack.
3. Recommend specific tooling that can be added to the service, such as Bot Management, to, for example, stop a specific cyber-attack.
4. Make recommendations for actions Customer may take to help resolve issues or mitigate an attack.

7.9 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

7.10 Website and Application Security Outage Credits

In the event US Signal fails to meet the technical standards of performance above in Section 7.9 ("**Website and Application Security Outage**"), Customer shall be entitled to a credit determined according to the following tables:

Availability Credit:

Outage Length	Credit
< 1 hour	25% of WaAS MRC
1-3 hours	50% of WaAS MRC
3-5 hours	75% of WaAS MRC
5+ hours	100% of WaAS MRC

In no event will credits for Website and Application Security for any one (1) month exceed one hundred percent (100%) of the MRC for Website and Application Security.

Response Time:

Response Length	Credit
SLA + 1 hour	10% of WaAS MRC
SLA + 2 hour	15% of WaAS MRC
SLA + 3 hour	20% of WaAS MRC
4+ hours	25% of WaAS MRC

In no event will credits for a WaAS Service for any one (1) month exceed one hundred percent (100%) of the MRC for the applicable WaAS Service.

7.11 Use of Service Data by Partner Service

Customer agrees and acknowledges that in the ordinary operation of WaAS, the Service collects and transmits data related to the diagnostic use of WaAS functionality ("Service Data") from Customer's network environment and/or the Internet, including third party domains, to Partner Service's servers, and that Partner Service uses such Service Data for all reasonable and necessary purposes required to provide the Service. Service Data does not include Customer's stored data. Customer acknowledges its responsibility to ensure that its use of the Service is permitted under the laws of its jurisdiction. Customer

also grants to US Signal the perpetual, irrevocable right to use, reproduce, modify, and otherwise utilize the operational metrics, both during and after the SIT, for the purpose of improving and enhancing the Service, monitoring the performance of the Service, and performing internal research and development for the provisioning of Partner Service's products and services. Customer shall be responsible for informing owners or operators of third-party domains of Partner Service's receipt of, and rights to, such information and for obtaining any necessary consents. These grants are essential to the provision of the Service. Partner Service may retain Customer-specific aggregations solely for internal research and development, audit, and anti-fraud purposes.

SECTION 8 MANAGED CLOUD BACKUP FOR VEEAM

8.1 Description

Managed Cloud Backup for Veeam ("**MCBFV**") utilizes Veeam software. US Signal shall: 1) operate and manage a data center storage target for Customer backups; 2) create and modify any backup schedules and retention plans ("**Managed Cloud Backup for Veeam Adjustments**") as directed by Customer, provided that such Managed Backup Adjustments are requested during Business Hours as identified in Section 1.8 herein; 3) monitor the backups for success or failure; 4) if within a twenty four (24) hour period Customer's MCBFV experiences consecutive single endpoint backup failures, then US Signal shall notify Customer; and 5) restore any of Customer's files, folders or images to its source only. For the avoidance of doubt, restoration shall not include the creation of any new virtual machines, installation of OSs or the restoration of files and/or images to endpoints that are not visible and online within the third party software's management portal. At US Signal's sole discretion, US Signal may test its restoration of any backups for validity of the backup functionality. There are two ways to purchase ("MCBFV"):

a. MCBFV may be purchased on a month-to-month term whereby Customer's charges for the service are based upon Customer's actual storage (GB) consumed each month. Usage rates are priced according to the GB rate on the service's OFS. Customer may terminate CBFV on month-to-month term upon five (5) business days' prior written notice. Customer is responsible for all charges up until the date of termination. In the event Customer's Consumed Data equals zero (0) for more than ninety (90) consecutive calendar days, then US Signal may terminate the applicable CBFV upon ten (10) days written notice; or,

b. MCBFV may be purchased on a term ("**MCBFV Minimum**") whereby Customer's charges are discounted by committing to a minimum data consumption threshold invoiced as an MRC each month. Any data consumed beyond the MCBFV Minimum threshold is priced according to the per GB rate on the service's OFS. Cancellation of MCBFV Minimum service prior to the expiration of its SIT is subject to the Early Termination charges as described in the Agreement.

8.2 Rates

Recurring charges are based upon Customer's actual storage (GB) consumed each month ("**Consumed Data**") which shall be monitored using third party software. Billing periods shall commence on the first (1st) of the month and end on the last day of the month. Consumed Data shall be calculated on the amount of Customer's data present in the Veeam environment on the last business day of the billing period. Such recurring charges shall be billed in arrears according to the following formula:

Price per GB X actual GB Consumed Data by Customer during the previous month = Storage Usage Charge MRC

All associated MRCs and NRCs for Managed Cloud Backup for Veeam are ICB which may comprise any of the following including the purchase options listed above:

1. **MCBFV Management Fee MRC:** The maximum number of supported and managed endpoints X the management rate, as identified in the applicable OFS.
2. **Production Site Setup NRC:** Installation charge based on the number of managed endpoints as identified in the quote and estimated support required to configure Veeam infrastructure.
3. **MCBFV Agent Setup NRC:** Setup fee for additional managed endpoints requiring Veeam agent software installation.
4. **MCBFV Support NRC:** Applies to MCBFV restoration requests as defined herein.

In the event Customer experiences an event that requires restoration efforts ("**MCBFV Restoration Event**"), Customer shall declare such event by opening a trouble ticket with US Signal's TOC at 888.663.1700 or toc@ussignal.com. US Signal shall invoice Customer a Managed Cloud Backup for Veeam Support NRC for the MCBFV Restoration Event according to the following table:

MCBFV Restoration Event	MCBFV NRC (per quarter hour)
First 30 Minutes	$0.00

> 30 Minutes	$25.00

Billing for a MCBFV Restoration Event shall be based on actual technician time as recorded in US Signal third party software. US Signal shall invoice Customer in increments of fifteen (15) minutes, or fraction thereof, rounded up to the nearest whole increment.

8.3 FastPath (Optional)

FastPath provides Customer a private connection between Customer's' Managed Cloud Backup for Veeam storage location and its applicable US Signal Cloud Service. FastPath shall include a Fixed Port with a Cloud Based Managed Security appliance. Customer shall provide US Signal one (1) of Customer's IP addresses for the provisioning of FastPath. All associated MRCs for FastPath are on an individual case basis ("**ICB**").

8.4 Responsibilities of Customer

Customer is solely responsible for: (a) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (b) its compliance with all laws in connection with the Services under the Agreement; (c) loss of stored data resulting from an act by Customer; (d) the integrity of its data; (e) any host-based anti-virus, malware or spyware unless purchased through a Service; and (f) the on and/or off-Boarding of Customer's data onto the Services; (g) access to each endpoint, as necessary, for the installation and remediation of the backup agent software; (h) providing US Signal ten (10) business days written notice of any change or addition to the endpoints; (i) providing US Signal's TOC adequate information in order to troubleshoot service related issues; (j) notifying US Signal of any backup agent software issues; and (k) notifying US Signal of restoration events.

8.5 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

8.6 Response Credits

In the event US Signal fails to meet the technical standards of performance in Section 8.5 above, Customer shall be entitled to a response time credit determined according to the following table:

Response Time:

Length of Response	MCBFV Management Fee MRC Credit
SLA + 1 Hour	10% of MCBFV Management Fee MRC
SLA + 2 Hours	20% of MCBFV Management Fee MRC
SLA + 3 Hours	30% of MCBFV Management Fee MRC
SLA + 4 Hours	40% of MCBFV Management Fee MRC
SLA + 5 Hours	50% of MCBFV Management Fee MRC

In no event will response time credits for a response time for any one (1) month exceed fifty percent (50%) of the MCBFV Management Fee MRC.

8.7 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 9 MANAGED CLOUD REPLICATION FOR VEEAM

9.1 Description

Managed Cloud Replication for Veeam ("**MCRFV**") utilizes Veeam software. US Signal shall: 1) operate and manage a US Signal Resource Pool for replicated Customer virtual machines; 2) create and modify any replication schedules and retention plans ("**Managed Cloud Replication for Veeam Adjustments**") as directed by Customer, provided that such Managed Cloud Replication for Veeam Adjustments are requested during Business Hours as identified in Section 1.8 herein; 3) monitor replication for success or failure; 4) if within a twenty four (24) hour period Customer's MCRFV experiences consecutive single endpoint replication failures, then US Signal shall notify Customer; and 5) restore any of Customer's replicated virtual machines in their US Signal Resource Pool or back to source. For the avoidance of doubt, restoration shall not include the creation of any new virtual machines, installation of OSs or the restoration of files and/or images to endpoints that are not visible and online within the third party software's management portal. At US Signal's sole discretion, US Signal may test its restoration of any virtual machines for validity of the replication functionality. There are two ways to purchase ("MCRFV"):

a. MCRFV may be purchased on a month-to-month term whereby Customer's charges for the Service are based upon Customer's actual storage (GB) consumed each month. Usage rates are priced according to the GB rate on the Service's OFS. Customer may terminate MCRFV on month-to-month term upon five (5) business days' prior written notice. Customer is responsible for all charges up until the date of termination. In the event Customer's Consumed Data, as defined below, equals zero (0) for more than ninety (90) consecutive calendar days, then US Signal may terminate the applicable MCRFV service upon ten (10) days written notice; or,

b. MCRFV may be purchased on a term ("**CRFV Minimum**") whereby Customer's charges are discounted by committing to a minimum data consumption threshold invoiced as an MRC each month. Any data consumed beyond the MCRFV Minimum threshold is priced according to the per GB rate on the Service's OFS. Cancellation of Termed MCRFV service prior to the expiration of its SIT is subject to the Early Termination charges as described in the Agreement.

9.2 Rates

MCRFV consists of both recurring and non-recurring charges described as follows:

a. Recurring charges:

   i. **MCRFV Management Fee**: Number of supported and managed endpoints X the management rate, as identified in the applicable OFS.

   ii. **Gold Storage - Usage:** Usage and/or overage charges for MCRFV Minimum are based upon Customer's average storage (GB) consumed each month ("**Consumed Data**") which shall be monitored using third party software. The billing period shall commence on the first (1st) of the month and end on the last day of the month. Consumed Data shall be calculated on the average amount of Customer's data present per day in the CRFV environment during the billing period. Such recurring charges shall be billed in arrears according to the following formula:

   Price per GB X Average GB Consumed Data Daily by Customer during the previous month = Gold Storage - Usage

b. Non-recurring or event-based charges also apply when Customer experiences a failover event ("**MCRFV Failover Event**") or desires to test MCRFV ("**MCRFV Test Event(s)**"), (collectively "**MCRFV Event**"). In the occurrence of an MCRFV Event, US Signal shall invoice Customer on a usage basis for: 1) the average GHz Compute and GB Memory of powered-on VMs over the month; plus 2) the MCRFV Event support rates according to the following table:

MCRFV Event	NRC (per quarter hour)
Failover Event	$62.50
Test Event	$25.00

Customer shall be eligible for up to two (2) free MCRFV Test Events that last up to forty eight (48) consecutive hours during any three hundred and sixty five (365) consecutive day period commencing on the first (1st) day of the SIT. Any MCRFV Test Event that: 1) last longer than forty eight (48) hours; or 2) exceeds the two (2) free MCRFV Test Events shall be billed according to the MCRFV Event NRC as identified above plus the Compute and Memory charges. Billing for a MCRFV Event shall cover the interval of time from MCRFV Declaration to MCRFV Conclusion as further described in Section 9.5., herein. US Signal shall invoice Customer in increments of fifteen (15) minutes or a fraction thereof rounded up to the nearest whole increment. In order to obtain a credit for the charges related to one of the two (2) free qualifying CRFV Test Events, Customer shall make a written request to orders@ussignal.com within thirty (30) days of the conclusion of the event.

9.3 Layer 2 Extension (Optional)

Layer 2 Extension provides Customer a private Layer 2 VPN connection between Customer's equipment at its Ground site and its applicable US Signal Cloud Service. Layer 2 Extension includes a VMware NSX Edge instance to allow the same subnet to exist in both the Ground site and US Signal Cloud. Layer 2 Extension may be purchased on a term or month-to-month basis and all associated MRCs are on an individual case basis ("**ICB**").

9.4 Configuration Requirements

The Following are additional service requirements for MCRFV;

a. Customer shall utilize the Ground to Cloud, as defined in Section 5.3 of the Managed Service Schedule replication design.
b. Customer shall own and manage equipment at Ground site.
c. Equipment shall replicate to a US Signal Resource Pool.
d. Customer shall purchase a US Signal CBAS or CBAS+ along with a DIA Port as described in Sections 2.1 and 2.3 in the Cloud Service Schedule for proper connectivity.
e. No individual VM shall exceed 32 vCPUs.

9.5 MCRFV Event Operation

A MCRFV Event begins when Customer powers on replicated workloads in the cloud ("**MCRFV Declaration**") and ends when workloads in the cloud are powered off ("**MCRFV Conclusion**").

9.6 Responsibilities of Customer

Customer is solely responsible for working with US Signal to establish a disaster recovery MCRFV playbook within thirty (30) days of engagement by US Signal personnel and maintaining such MCRFV playbook. The "**MCRFV Playbook**" shall include all the necessary components and processes to restore Customer's environment to the replication site in the event of a MCRFV Event. US Signal shall retain one (1) current version of the MCRFV Playbook in order for US Signal to perform MCRFV. Customer is also solely responsible for: (a) the security, including the encryption of data to National Institute of Standards of Technology in the United States (NIST) Data at Rest Special Publication 800-111 and Data in Motion Special Publication 800-52 standards; (b) its compliance with all laws in connection with the Services under the Agreement; (c) loss of stored data resulting from an act by Customer; (d) the integrity of its data; (e) any host-based anti-virus, malware or spyware unless purchased through a Service; (f) the on and/or off-boarding of Customer's data onto the Services; and (g) maintaining an interoperable software version compatible with US Signal's current software version. Upgrading or patching software versions without confirmation of interoperability shall void all US Signal responsibilities in relation to this Service, including Outage Credits.

9.7 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

9.8 Outage Credits

In the event US Signal fails to meet the service metrics as defined in Technical Standards of Performance above ("**MCRFV Outage**"), Customer shall be entitled to credits determined according to the following:

Length of MCRFV Outage	**MCRFV Credit**
< 4 hours	0% of the MCRFV MRC
4 - <12 hours	25% of the MCRFV MRC
12- <24hours	50% of the MCRFV MRC
24 - <48 hours	75% of the MCRFV MRC
>48 hours	100% of the MCRFV MRC

In the event US Signal fails to meet the RTO as defined in the MCRFV Playbook, then Customer shall be entitled to a restoral credit equal to 100% of the MCRFV MRC.

A MCRFV Event shall be deemed to have commenced upon notification by Customer to US Signal's TOC of an event requiring MCRFV. Each MCRFV Event shall be deemed to end upon Customer's confirmation to US Signal's TOC that MCRFV support is no longer needed by Customer.

The MRC credits shall be based upon the previous month's MCRFV MRC. Periods of Planned Maintenance and Repair will not be excluded when calculating MCRFV Outage Credits. In no event will any combined performance credits for MCRFV for any one (1) month exceed one hundred percent (100%) of the current month's charges for the applicable MCRFV.

9.9 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 10 INTENTIONALLY LEFT BLANK

SECTION 11 COHESITY DATA MANAGEMENT ("CDM")

11.1 Description

Cohesity Data Management ("**CDM**") utilizes Cohesity software to provide Cohesity Backup protection and management of Customer data.

11.2 Cohesity Backup Description and Rates

Cohesity Backup is a backup solution supporting: 1) server operating systems such as Microsoft Windows and Linux; 2) server applications such as Microsoft Exchange and Structured Query Language ("SQL"); 3) workstation operating systems such as Mac and Microsoft Windows; and 4) image level protection of virtual machines. A Cohesity Hybrid Extender proxy VM must be deployed on the Customer's network to provide secure communication between US Signal and Customer networks. Backup data older than 30 days will be archived in Object Storage at a standard rate of $.02 per GB, unless otherwise noted on the OFS. Cohesity Backup may be purchased either on a month-to-month basis whereby recurring rates may be subject to change upon thirty (30) days' written notice, or on a one year SIT whereby Customer's rates are discounted for the term. Within thirty (30) days of the expiration of the SIT for termed orders, Customer shall provide written notice to US Signal of its intent to either: i) renew the Services for a new, minimum of one (1) year SIT; or ii) terminate the Services at the end of the SIT.

US Signal shall: 1) operate and manage two (2) geographically diverse data center backup and replication storage targets; and 2) manage the provisioning of Cohesity Backup including the creation of backup jobs, retention schedules and monitoring. Upon commencement of the SIT for Cohesity Backup, US Signal shall: 1) manage the backup jobs; 2) provide proactive response for backup and infrastructure alerts; and 3) process restores as requested by Customer, subject to the Rates set forth below.

All associated MRCs and NRCs for Cohesity Backup are ICB which may comprise of the following:

a. **Backup Storage Fee MRC:** Customer's aggregate data calculated by the actual storage (GB) consumed on the last business day of each month multiplied by the rate per GB on the OFS ("**Back-End Data**"). This will appear on the invoice as a combination of Backup Storage and Replication Storage, totaling the Backup Storage Fee amount.

b. **Replication Storage Fee MRC:** Customer's aggregate data calculated by the actual storage (GB) consumed on the last business day of each month multiplied by the rate per GB on the OFS ("**Back-End Data**").

c. **Backup Management Fee MRC**: Peak number of VMs protected concurrently per day within the applicable calendar month multiplied by the rate per VM on the OFS.

d. **Setup NRC:** Installation charge based on the number of protected devices.

e. **Support NRC:** Applies to restoration requests as defined herein.

f. **Hybrid Extender MRC:** Charge based on number of Hybrid Extenders operating in the Customer environments multiplied by the per Hyper Extender rate on the OFS.

In the event Customer experiences an event that requires restoration efforts ("**Cohesity Backup Restoration Event**"), Customer shall declare such event by opening a trouble ticket with US Signal's TOC at 888.663.1700 or toc@ussignal.com. US Signal shall invoice Customer a Support NRC for the Cohesity Backup Restoration Event according to the following table:

Cohesity Backup Restoration Event	Support NRC (per quarter hour)
First 30 Minutes	$0.00
> 30 Minutes	$25.00

Billing for a Cohesity Backup Restoration Event shall be based on actual technician time as recorded in US Signal's third party software. US Signal shall invoice Customer in increments of fifteen (15) minutes, or fraction thereof, rounded up to the nearest whole increment.

11.2.1 FastPath (Optional)

FastPath provides Customer a private connection between Customer's' Cohesity Backup and its applicable US Signal Cloud Service. FastPath shall include a Fixed Port with a Cloud Based Managed Security appliance. Customer shall provide US Signal one (1) of Customer's IP addresses for the provisioning of FastPath. All associated MRCs for FastPath are on an individual case basis ("**ICB**").

11.2.2 Cohesity Backup Design Document

Customer is solely responsible for working with US Signal to establish the initial Cohesity Backup Design Document within thirty (30) days of engagement by US Signal personnel and maintaining such Cohesity Backup Design Document by providing US Signal updates when applicable. The ("**Cohesity Backup Design Document**") shall include such items as authorized contacts, information about the protected systems and all the notable components and processes to restore Customer's protected systems. US Signal shall retain one (1) current version of the Cohesity Backup Design Document in order for US Signal to perform Cohesity Backup.

11.2.3 Responsibilities of Customer

Customer is solely responsible for: (a) providing US Signal ten (10) business days' written notice of adding any new protected systems to its existing Cohesity Backup; (b) its compliance with all laws in connection with the Services under the Agreement; (c) loss of stored data resulting from an act by Customer; (d) the integrity of its data; (e) any host-based anti-virus, malware or spyware unless purchased through a Service; (f) the on and/or off-Boarding of Customer's data onto the Services.

11.2.4 Cohesity Backup Outage Credits

In the event US Signal fails to meet the applicable metric identified in the technical standards of performance ("**Cohesity Backup Outage**"), Customer shall be entitled to a credit determined according to the following tables:

Availability Credit:

Length of Cohesity Backup Outage (hours)	Cohesity Backup Availability Credit
< 4 Hours	0% of Cohesity Backup Data MRC
4 – 6 Hours	10% of Cohesity Backup Data MRC
6 – 8 Hours	25% of Cohesity Backup Data MRC

8 – 10 Hours	40% of Cohesity Backup Data MRC
> 10 Hours	50% of Cohesity Backup Data MRC

Such MRC shall be based upon the previous month's Cohesity Backup Data MRC. In no event will Cohesity Backup outage credits for US Signal's failure to meet the availability metric for any one (1) month exceed one hundred percent (100%) of the current month's charges for the applicable Cohesity Backup Data.

Response Time:

Length of Response	Cohesity Backup Credit
SLA + 1 Hour	10% of Cohesity Backup Support NRC
SLA + 2 Hours	20% of Cohesity Backup Support NRC
SLA + 3 Hours	30% of Cohesity Backup Support NRC
SLA + 4 Hours	40% of Cohesity Backup Support NRC
SLA + 5 Hours	50% of Cohesity Backup Support NRC
SLA + 6 Hours	60% of Cohesity Backup Support NRC
SLA + 7 Hours	70% of Cohesity Backup Support NRC
SLA + 8 Hours	80% of Cohesity Backup Support NRC
SLA + 9 Hours	90% of Cohesity Backup Support NRC
SLA + 10 Hours	100% of Cohesity Backup Support NRC

In no event will credits for Cohesity Backup Restoral for any one (1) month exceed one hundred percent (100%) of the NRC for the applicable Cohesity Backup Support NRC.

11.3 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

11.4 Retrieval Period

Customer shall have up to thirty (30) consecutive calendar days immediately following its request for termination of an Ordering Document to arrange access to the Services for the purpose of removing its data ("**Removal Interval**"). US Signal shall destroy any Customer data that remains after the Removal Interval. Upon Customer's request, US Signal may, at its sole discretion, assist in Customer's retrieval of its data, which shall be described under a separate addendum or agreement as referenced herein. The terms and conditions of this Agreement shall survive any expiration or termination of any applicable Ordering Document, or the Agreement, until such time as Customer's data is either: 1) removed from US Signal's cloud infrastructure by Customer; 2) transferred to a third party cloud infrastructure through engagement with US Signal's Professional Services team, documented via separately executed SOW; or 3) destroyed by US Signal. For the avoidance of doubt, the terms and conditions in this Agreement shall apply until Customer's data is no longer in US Signal's possession.

SECTION 12 INTENTIONALLY LEFT BLANK

SECTION 13 ENDPOINT DETECTION AND RESPONSE

13.1 Description

US Signal will provide the third party platform to Customer for endpoint detection, remotely guide the deployment process, configure alerts, and optionally monitor and manage alerts for Customer. The platform ("**Platform**") consists of the software agents deployed on Customer endpoints and the access and features of the third party service portal. The license required to provide Services will be obtained and managed by US Signal. Endpoint Detection and Response ("**EDR**") is an endpoint security solution that deploys software-based tools to gather data from endpoints and utilizes that data to analyze suspicious system activities. US Signal also provides a managed version of this product called Managed Detection and Response ("**MDR**"). EDR and MDR are available on a single or multi-year term identified on the OFS at the service tier options listed below. Rates per endpoint shall remain unchanged during the SIT. Cancellation of EDR and MDR prior to the expiration of the SIT is subject to the Early Termination charges as described in the Agreement.

13.2 Service Tiers

EDR is comprised of three service tiers:

1. **Standard EDR:** Contains a basic set of EDR features. US Signal will provide the Platform and remotely guide deployment of the Service. Following deployment, the responsibility of monitoring and reviewing alerts will be passed on to Customer.
2. **Premium EDR:** Contains an advanced set of EDR features. US Signal will provide the Platform and remotely guide deployment of the Service. Following deployment, the responsibility of monitoring and reviewing alerts will be passed on to Customer.
3. **Premium MDR:** Contains an advanced set of EDR features. US Signal will provide the Platform and remotely guide deployment of Service. Following deployment, the responsibility of monitoring and reviewing alerts will be managed by US Signal.

13.3 Scope of Service

Standard and Premium EDR

US Signal Responsibilities:

1. During the SIT, US Signal will provide Customer with the EDR Licenses set forth on the OFS and in accordance with the terms of the Agreement.
2. Provide technical support for the Platform between 8:00 am – 5:00pm Monday through Friday, ET, excluding Federal US holidays ("**Business Hours**").
3. Provide Customer access and orientation to Third-Party Portal.
4. Provide Senior Project Manager for implementation.
5. Assist Customer with Platform Configuration.
6. Assist Customer with Platform alert configuration and logging settings.
7. Assist Customer with exclusions and deployment support during implementation.

Customer Responsibilities:

1. Make adequate resources or staffing available for Service implementation.
2. Only deploy EDR Software Agent on systems with compatible operating systems defined as:
    a. Microsoft supported versions of Windows and Windows Server
    b. Apple supported versions of Mac OS X
    c. Current version of Linux
3. Deploying EDR Software Agent to the endpoints to be included within the Service.
4. Manage the frequency and level of review for alerts, notifications, and events created within the Service and configuring the desired response and actions.
5. Mitigation or remediation activities associated with an alert or event identified by the EDR Platform.
6. If Customer requires more than 14-day log retention, Customer must work with US Signal to establish log forwarding to Customer's logging server.

Premium MDR

US Signal Responsibilities:

1. During the SIT, US Signal will provide Customer with the EDR Licenses set forth on the OFS and in accordance with the terms of the Agreement.
2. Provide 24x7x365 monitoring of alerts generated within the EDR console for all registered and operational software agents deployed by Customer.
3. Initiate incident triage on critical and high priority alerts within one (1) hour from the initial alert in the EDR Platform.
4. Triage and analyze telemetry data for potentially malicious behavior and files.
5. For non-remediated threats, notify Customer contact via established telephone numbers.
6. For auto-remediated threats, provide email notification to Customer of threat containment and relevant incident details.
7. Make recommendations to Customer regarding any potential action to be performed on endpoints in response to an identified threat.

8. Update the Endpoint Software Agents deployed into the environment based on a schedule and strategy communicated to Customer.
9. Provide technical support for the Platform during Business Hours.
10. During the SIT, US Signal will provide Customer with the EDR Licenses set forth on the OFS and in accordance with the terms of the Agreement.
11. Provide Customer access and orientation to Third-Party Portal.
12. Provide Senior Project Manager for Implementation.
13. Configure Platform for alerting and deploy protection policies.
14. Hold a quarterly account review with Customer to review Service.

Customer Responsibilities:

1. Assign a project lead to serve as the primary point of contact for the MDR implementation.
2. Commit adequate personnel and resources to successfully implement the MDR solution.
3. Deploying EDR Software Agent to the endpoints to be included within the Service.
4. Provide an email alias to receive proactive notifications for threats requiring Customer attention.
5. Provide an escalation and emergency contact list for the US Signal SOC team to call for urgent incidents.
6. Provide adequate staffing and reasonable assistance to US Signal to support diagnostic testing, troubleshooting and incident response.
7. Only deploy EDR Software Agent on systems with compatible operating systems defined as:
    a. Microsoft supported versions of Windows and Windows Server
    b. Apple supported versions of Mac OS X
    c. Current version of Linux
8. Contact US Signal if Customer believes an incident is in progress or has occurred.
9. If Customer requires more than 14 day log retention, Customer must work with US Signal to establish log forwarding to Customer's logging server.
10. Review and evaluate the reports and notifications provided by US Signal and take necessary action for remediation.
11. Perform US Signal or third party recommended changes to improve the operation or performance of MDR or to resolve identified incidents.
12. Properly decommissioning an endpoint agent or notifying the US Signal SOC team for assistance with decommissioning the endpoint agent.

13.4 Rates

Rates are determined based on the number of endpoints deployed, multiplied by the service tier rate per endpoint as identified in the OFS. Endpoint charges will be billed in arrears in the form of a Monthly Recurring Charge ("**MRC**"). Billing will begin as soon as the first endpoint is deployed. Customer will be billed for the highest number of endpoints deployed at any given time within the month. A Non-Recurring Charge ("**NRC**") applies for the initial setup and guided deployment of the Service at the rate identified on the OFS.

13.5 Service Changes

Customer may change the number of endpoints being protected within the Platform at any time during the SIT; all endpoints will be coterminous with the initial SIT. During the SIT, Customer may not remove greater than fifty (50%) percent of the endpoints identified on the original OFS. Customers who have purchased Standard EDR may upgrade to Premium EDR Service via an executed OFS or an email request sent directly through the TOC (a) email: toc@ussignal.com; or (b) by calling 888-663-1700. Customers may also upgrade from Standard EDR or Premium EDR to Premium MDR via an executed OFS. Upgrading Services will result in new MRCs but will not extend the SIT. All Service upgrades shall be performed during Business Hours.

13.6 Deployment and Configuration Requirements

US Signal will provide guidance during the deployment process to ensure proper deployment is achieved. However, Customer is responsible for correctly configuring its systems in accordance with any instructions provided by US Signal and is ultimately accountable for the execution of the software agent deployment. If additional assistance is required beyond the remote deployment guidance offered by US Signal, US Signal may require a Statement of Work ("**SOW**") to perform such Services.

13.7 Acknowledgements

Customer acknowledges and agrees: (a) if US Signal loses the underlying software license to provide the Services, the Service(s) shall terminate without further liability or obligation by either party; (b) the Services provided work best when the endpoint has access to the Internet, if the endpoint does not have Internet access Service may be degraded; (c) it may not utilize Service on systems located outside of the United States; (d) there is no guarantee, despite best efforts, that Service will ensure that the US Signal SOC team is able to catch and contain all threats in Customer environment; (e) the Service will take action on all appropriate threats based on the guidelines established between Customer and US Signal for the Service; (f) it grants the US Signal SOC permission to take the recommended response action in Customer's production environment, based on the guidelines established between Customer and US Signal for the Service; and (g) the Platform and MDR Service is subject third party provider maintenance windows currently set as Sunday between 2:00 a.m. and 11:00 a.m. Eastern Time.

13.8 Data Privacy

Most of the information collected through the Services is not personally identifiable information ("**PII**") and relates to the computing processes of devices protected against malware infection by the third party provider, or device standard identifiers. Such information includes device or network usage, endpoint login data, types and versions of operating systems and browsers, computer name, file execution information, and information about installed software applications. Some of the data collected may be considered PII depending on the jurisdiction's laws where it is collected, such as IP addresses and endpoint browsing history. In some cases, PII is collected to the extent it is included within usernames, filenames, file paths, and machine names. At Customer direction, US Signal may also collect or retrieve files as part of its Services such as additional data to analyze certain malware threats or network information to enable connected device discovery and mapping. Files, file names, file paths and machine names, for example, may contain PII if such PII is included in such files. Data retention by US Signal or third party provider is minimized to the time required to provide Services.

13.9 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

13.10 Outage Credits

In the event US Signal fails to meet the technical standards of performance identified in Section 13.9 above, then Customer shall be entitled to a credit according to the following table:

Length of Outage	Credit as a Percentage of One Month of Service
<1 Hour	0%
1-12 Hours	10%
12-24 Hours	20%
24-48 Hours	30%
48 Hours or greater	50%

In no event will credits for the Service for any one (1) month exceed one hundred percent (100%) of the MRC for EDR or MDR.

SECTION 14 MANAGED EXTENDED DETECTION AND RESPONSE ("MXDR")

14.1 Description

US Signal will utilize a third party platform for incident detection, remotely guide the deployment process, configure alerts, and monitor and manage alerts for Customer. Managed Extended Detection and Response ("**MXDR**") is a network security solution that utilizes software-based tools to gather data from endpoints and correlates that data to analyze suspicious network activities. The license required to provide Services will be obtained and managed by US Signal. MXDR is available on a twelve (12) month term as identified on the OFS. Rates per endpoint shall remain unchanged during the SIT. Cancellation of MXDR prior to the expiration of the SIT is subject to the Early Termination charges as described in the Agreement.

14.2 Scope of Service

US Signal Responsibilities:

1. During the SIT, US Signal will provide Customer with the MXDR Licenses set forth on the OFS and in accordance with the terms of the Agreement.
2. Provide 24x7x365 monitoring of alerts generated within the MXDR console for all enrolled endpoints.

3. Perform incident investigation limited to data collected by and reported within the MXDR console.
4. Initiate incident triage on critical and high priority alerts within one (1) hour from the initial alert in the MXDR console.
5. Triage and analyze telemetry data for potentially malicious behavior.
6. For detected threats requiring remediation, notify Customer contact via established telephone numbers.
7. For detected threats not requiring remediation, provide email notification to Customer of relevant incident details.
8. Make recommendations to Customer regarding any potential action to be performed on endpoints in response to an identified threat.
9. Provide technical support for the MXDR Service during Business Hours.
10. During the SIT, US Signal will provide Customer with the MXDR Licenses set forth on the OFS and in accordance with the terms of the Agreement.
11. Provide a project manager for implementation.
12. Configure the MXDR console for alerting and deploy protection policies.
13. MXDR Service will retain one (1) year of log data.
14. Hold a monthly account review meeting with Customer to review the Service.

Customer Responsibilities:

1. Assign a project lead to serve as the primary point of contact for the MXDR implementation.
2. Commit adequate personnel and resources to successfully implement the MXDR Service.
3. Deploy the MXDR Software Agent to endpoints.
4. Customer must deploy MXDR Software Agent to at least 80% of endpoints in Customer's environment to ensure adequate monitoring and detection capability for the Service.
5. Configure the endpoints to send logs for collection.
6. Work with US Signal SOC to deploy log collectors as needed to support additional log sources. Additional log source types can be found at https://docs.rapid7.com/insightidr/insightidr-event-sources.
7. Provide an email alias to receive proactive notifications for threats requiring Customer attention.
8. Provide an escalation and emergency contact list for the US Signal SOC team to call for urgent incidents.
9. Provide adequate staffing and reasonable assistance to US Signal to support diagnostic testing, troubleshooting, and incident response.
10. Deploy MXDR Software Agent on systems with compatible operating systems.
11. Timely update any MXDR software installed in the environment as instructed by US Signal.
12. Immediately contact US Signal if Customer believes an incident is in progress or has occurred.
13. If Customer requires more than one (1) year log retention, Customer must work with US Signal to establish log forwarding to Customer's logging server.
14. Review and evaluate the reports and notifications provided by US Signal and take necessary action for remediation.
15. Perform recommended changes as specified by US Signal to improve the operation or performance of the MXDR Service or to resolve identified incidents.
16. If Customer decommissions an endpoint, they will work with the US Signal SOC to decommission the MXDR software agent.
17. Customer will deploy MXDR software agent on any new customer endpoints deployed after the initial implementation.

14.3 Rates

Endpoint charges will bill in arrears as a Monthly Recurring Charge ("**MRC**") at the rates identified on the OFS. A minimum commitment of endpoints is required per month and is established by the Extended Detection and Response - Endpoint Fee quantity identified on the OFS ("Minimum Commitment"). The billing shall commence in the month after the first endpoint is deployed. The Customer shall be billed for the Minimum Commitment if the number of endpoints deployed is below the established quantity on the OFS. If the quantity of endpoints exceeds the Minimum Commitment during the month, the MRC is calculated using the highest number of endpoints monitored at any point in time within the month. A Non-Recurring Charge ("**NRC**") applies for the initial setup and guided Service deployment at the rate identified on the OFS. All associated MRCs and NRCs for MXDR are comprised of the following:

a. **Extended Detection and Response – Endpoint Fee:** A per endpoint MRC for monitored endpoints.
b. **MXDR Setup:** Installation NRC based on the number of endpoints and complexity of the Customer environment.

14.4 Renewals

The Service's Initial Term (SIT) shall automatically renew for a twelve (12) month term at the rate equal to standard rate at the time of renewal unless Customer or US Signal provides the other party with written notice of its intention not to renew at least thirty (30) days before the expiration of the SIT or the existing Service Term.

14.5 Service Changes

Customer may change the number of endpoints being monitored within the MXDR Service at any time during the SIT. If the number of endpoints exceeds the Minimum Commitment by twenty-five percent (25%) or more in any given month during the SIT, the Customer must increase the Minimum Commitment and extend the term by executing a new OFS.

14.6 Deployment and Configuration Requirements

US Signal will remotely guide the deployment process to help ensure proper Service installation. However, Customer is responsible for correctly configuring its systems according to instructions provided by US Signal and is ultimately accountable for the execution of the software deployment and log configuration. If additional assistance is required beyond the remote deployment guidance offered by US Signal, US Signal may require a Statement of Work ("SOW") to perform such Services.

14.7 Acknowledgements

Customer acknowledges and agrees: (a) if US Signal loses the underlying software license to provide the Services, the Service(s) shall terminate without further liability or obligation by either party; (b) the Services provided work best when the endpoint has access to the Internet, if the endpoint does not have Internet access, Service may be degraded; (c) it may not utilize the Service on systems located outside of the United States; (d) there is no guarantee, despite best efforts, that the Service will ensure that the US Signal SOC team is able to catch and contain all threats in the Customer environment; (e) the Service will provide notification to Customer of any active threats identified within the MXDR console; and (f) the MXDR Service is subject third party provider maintenance windows.

14.8 Data Privacy

The information collected through the Services relates to the computing processes of devices protected against security threats by the third-party provider, or device standard identifiers. Such information includes device or network usage, endpoint login data, types and versions of operating systems and browsers, computer name, file execution information, and information about installed software applications. Some of the data collected may be considered personally identifiable information ("PII"), such as IP addresses and endpoint browsing history, depending on the jurisdiction's laws where it is collected. In some cases, PII is collected to the extent it is included within usernames, filenames, file paths, and machine names. At Customer direction, US Signal may also collect or retrieve files as part of its Services such as additional data to analyze certain threats or network information to enable connected device discovery and mapping. Files, file names, file paths and machine names, for example, may contain PII if such PII is included in such files. Data retention by US Signal or a third-party provider is minimized to the time required to provide Services.

14.9 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

14.10 Outage Credits

In the event US Signal fails to meet the technical standards of performance identified in Section 14.8 above, the Customer shall be entitled to a credit according to the following table:

Length of Outage	Credit as a Percentage of One Month of Service
<1 Hour	0%
1-12 Hours	10%
12-24 Hours	20%
24-48 Hours	30%
48 Hours or greater	50%

Outage credits will not exceed 100% of the MRC for the Service in any given month.

14.11 Vulnerability Management as a Service (Optional)

Vulnerability Management as a Service ("VMaaS") is an optional add-on service to MXDR, utilizing scanning tools that evaluate Customer's network and a wide range of connected devices to identify potential threats malicious actors may exploit. US Signal will configure and manage the service for Customers and provide monthly account review meetings for recommended remediation or mitigation of threats discovered.

14.11.1 Rates

VMaaS charges will bill in arrears as a Monthly Recurring Charge ("MRC") at the rates identified on the OFS. A minimum commitment of assets is required per month and is established by the Vulnerability Management Licensed Asset - Fee quantity identified on the OFS ("Minimum Commitment"). The billing shall commence in the month after the first MXDR endpoint is deployed. The Customer shall be billed for the Minimum Commitment if the number of assets scanned is below the established quantity. If the quantity of assets exceeds the Minimum Commitment, the MRC is calculated using the highest number of assets monitored at any point in time within the month. A Non-Recurring Charge ("NRC") applies for the initial setup and guided Service deployment at the rate identified on the OFS. All associated MRCs and NRCs for VMaaS are comprised of the following:

a. **Vulnerability Management Licensed Asset - Fee:** An MRC per scanned asset.
b. **VMaaS Setup:** Installation NRC based on the Customer environment and complexity.

14.11.2 Renewals

The Service's Initial Term (SIT) shall automatically renew for a twelve (12) month term at the rate equal to standard rate at time of renewal unless Customer or US Signal provides the other party with written notice of its intention not to renew at least thirty (30) days before the expiration of the SIT or the existing Service Term.

14.11.3 Service Changes

Customer may change the number of assets being monitored within the VMaaS Service at any time during the SIT. If the number of assets exceeds the Minimum Commitment by twenty-five percent (25%) or more in any given month during the SIT, the Customer must increase the Minimum Commitment and extend the term by executing a new OFS.

SECTION 15 SECURE ACCESS SERVICE EDGE ("SASE")

US Signal's Secure Access Service Edge ("SASE") is a suite of services utilizing Cato Networks Inc. hardware and software as a service to provide cloud-based connectivity and security.

15.1 SD-WAN

Software Defined Area Network ("SD-WAN"). Software Defined Wide Area Network solution is a fully managed service providing a network management overlay for secure and private connectivity between customer environments. This Service utilizes Cato Networks Inc. ("Cato") hardware and software-as-a-service ("SaaS") management portal for centralized configuration and delivery of SD-WAN.

15.1.1 SD-WAN Rates

SD-WAN consists of both Monthly Recurring Charges ("MRC") and non-recurring charges ("NRC") at the rates identified on the OFS and described as follows:

a. **SD-WAN Site:** MRC based on the level of bandwidth purchased.
b. **SD-WAN Mobile Users:** MRC charged per user with SD-WAN client access.
c. **SD-WAN Socket:** MRC charged per hardware or software appliance.
d. **SD-WAN IP Addresses:** MRC for purchase of additional IP Addresses.
e. **SD-WAN Third Party IPsec:** MRC charged per third party IPsec connection with bandwidth limits of 5Mbps or less. Third party IPsec connections requiring more than 5Mbps will be billed as an additional SD-WAN Site.
f. **Setup:** NRC for setup of SD-WAN hardware, software and services.
g. **SD-WAN Socket Replacement Charge:** NRC for replacement of hardware damaged by customer.
h. **SD-WAN Dual Mount Rack Kits:** NRC for SD-WAN Socket dual mount rack kits.
i. **Capacity Pool Bandwidth:** MRC based on the level of bandwidth purchased.
j. **Digital Experience Monitoring – User**: MRC based on the number of users licensed for Digital Experience Monitoring.

Configuration Changes: Initial configuration setup is included in the Setup NRC. Customer may request changes to configuration after the initial setup but is limited to receiving one (1) free hour per month of US Signal labor time to make such changes. If US Signal labor time exceeds one (1) hour for the month, hourly service rates shall apply. To request a configuration change, Customer may open a ticket with US Signal's Technical Operations Center ("TOC") by calling 888.663.1700 or by emailing toc@ussignal.com.

15.1.2 Term

The term of this Agreement shall be the Service's Initial Term (SIT) set forth in the OFS, but in no event shall be less than twelve (12) months. The SIT for all SASE Services shall automatically renew for successive one-year periods thereafter (each the "Service's Renewal Term") unless Customer or US Signal provide the other party with written notice of its intention not to renew at least thirty (30) days before the expiration of the SIT or the Service's Renewal Term, individually and collectively referred to as the "Service Term". Should any OFS be submitted by Customer for additional SASE Services and/or SASE hardware (an "Additional Order") as defined within this Section 15 during any Service Term, the SIT of such Additional Order shall be pro-rated to concur with the existing Service Term so that the termination of all initial and renewal SASE Service Terms shall coincide to take effect on the same date.

15.1.3 Cato Terms

Customer's continued use of Cato proprietary software as a service ("SaaS"), hardware, software and/or services that are delivered to Customer shall be subject to Customer's compliance with Cato's Master Service Agreement found at https://www.catonetworks.com/msa/.

15.1.4 US Signal Responsibilities

US Signal will be responsible for the configuration, management, and monitoring of hardware and services. This includes the socket hardware ("Socket") and SaaS.

In Region - US Signal installs the Socket at Customer's service location that is located within fifty (50) miles of a US Signal point of presence. In the event such Socket is placed within a US Signal Colocation location, Customer agrees to: 1) verify its cabinet contains two (2) rack units of space; 2) supply its own power to the Socket; and 3) provide US Signal escorted access to the Socket to the extent reasonably determined by US Signal for the performance of its obligations required under the Agreement.

15.1.5 Customer Responsibilities

Customer is solely responsible for (a) power and environmental condition of the Socket in Customer's possession; and (b) its compliance with all laws in connection with the Services under the Agreement. For out of region locations, more than fifty (50) miles from a US Signal point of presence, Customer shall self-install preprogrammed Socket. Customer shall coordinate the testing and turn-up of the Socket with US Signal's Network Operations Center within five (5) days of its receipt of the Socket. Customer agrees not to open, alter, misuse, tamper with or remove the Socket. Customer will not remove any markings or labels or serial numbers from the Socket. Customer will safeguard the Socket from loss or damage of any kind and will not permit anyone other than a representative authorized by US Signal to perform any work on the Socket. If the Socket is damaged, destroyed, lost or stolen while in Customer's possession, Customer shall be liable. Prior to installation of the Socket, Customer shall notify US Signal of any special requirements regarding the placement of the Socket.

In the event of failure of a Socket component, US Signal will diagnose the problem and attempt to resolve the problem with the Customer over the phone. If after troubleshooting, US Signal determines that the failure is caused by defective Socket, US Signal will initiate Socket exchange. The replacement Socket component will ship within one (1) business day of US Signal's determination that an exchange is appropriate. Failed Sockets must be returned within ten (10) calendar days from receiving the replacement Socket. In the event that the defective Socket is the result of Customer's misuse of the hardware, all inbound and outbound hardware component shipping charges for Socket component hereunder will be paid by Customer, in addition to an amount of three hundred ($300) per Socket.

15.1.6 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

15.1.7 SD-WAN Outage Credits

In the event US Signal fails to meet the service metrics as defined in Technical Standards of Performance above, Customer shall be entitled to a credit determined according to the table below. Availability is determined based upon the following formula:

A = (T – M – D) / (T – M) x 100%
A = Availability
T = Total Monthly Minutes
M = Maintenance Time
D = Downtime

Availability	SD-WAN Credit
>=97.9% but < 99.999%	5% of SD-WAN MRC
>=96.9% but < 97.9%	7% of SD-WAN MRC
< 96.9%	9% of SD-WAN MRC

To receive credits, Customer must make a written request within forty-five (45) days of the end of the month for which the interruption occurred. In no event will credits during any one (1) calendar month exceed 100% of the MRC for the Service. Any credit shall be Customer's sole and exclusive remedy for any failure by US Signal to meet a service metric. Outage credits do not apply to outages: (i) caused by the negligence or willful misconduct of Customer; (ii) an outage due to Customer's network failure; (iii) due to failure of power (excluding any industry standard back-up power sources that US Signal is required to have in place); (iv) during any period in which US Signal is not given access to Customer's premise if necessary to resolve an outage; (v) during any period of unscheduled emergency maintenance or repair, scheduled maintenance, alteration or implementation; and (vi) during any Force Majeure Event as defined herein. US Signal may withhold issuance of any credits due Customer under this Agreement until any amounts past due by Customer have been paid in full.

15.2 SSE

Secure Service Edge ("SSE") are fully managed services providing cloud-based security for SASE customers.

IPS
Intrusion Prevention System ("IPS"). Intrusion Prevention System inspects inbound and out bound traffic to prevent communication with compromised or malicious resources and prevent exploits.

NGAM
Next-Generation Anti Malware ("NGAM"). Next-Generation Anti Malware provides cloud-based inspection to protect users from malware.

CASB
Cloud Access Security Broker ("CASB"). Cloud Access Security Broker provides visibility into cloud-based SaaS usage. The Service also allows defined policies to control access to SaaS resources.

DLP
Data Loss Prevention ("DLP"). Data Loss Prevention allows enterprises to protect sensitive data against unintentional loss or a data breach.

RBI
Remote Browser Isolation ("RBI"). Remote Browser Isolation provides secure browsing through a virtualization service that executes in-browser code remotely and streams web pages to user devices, protecting them from threats such as ransomware and phishing.

Threat Prevention
Threat Prevention is a collection of different security services which includes NGAM, IPS, DNS security, threat intelligence, inline artificial intelligence/machine learning and anti-phishing services.

XDR Pro
Extended Detection and Response provides aggregation of, and explanation for, network and security events, along with recommended actions to be taken in the event of network and security events.

15.2.1 SSE Rates

SSE is purchased based on the amount of site bandwidth licensed and/or a per user basis. This consists of Monthly Recurring Charges ("MRC") at the rates identified on the OFS and described as follows:

a. **Intrusion Prevention System – Site**: MRC based on licensed IPS bandwidth.
b. **Next-Generation Anti Malware – Site:** MRC based on licensed NGAM bandwidth.
c. **Cloud Access Security Broker – Site:** MRC based on licensed CASB bandwidth.
d. **Data Loss Prevention – Site:** MRC based on licensed DLP bandwidth.
e. **Remote Browser Isolation – Site:** MRC based on licensed RBI bandwidth.
f. **Intrusion Prevention System – User:** MRC based on licensed IPS users.
g. **Next-Generation Anti Malware – User:** MRC based on licensed NGAM users.
h. **Cloud Access Security Broker – User:** MRC based on licensed CASB users.
i. **Data Loss Prevention – User:** MRC based on licensed DLP users.
j. **Remote Browser Isolation – User:** MRC based on licensed RBI users.
k. **Setup:** NRC for setup of SSE software and services.
l. **Threat Prevention – Site:** MRC based on licensed Threat Prevention bandwidth.
m. **Threat Prevention – User:** MRC based on licensed Threat Prevention users.
n. **XDR Pro – User**: MRC based on licensed XDR Pro users.

Configuration Changes: Initial configuration setup is included in the Setup NRC. Customer may request changes to configuration after the initial setup but is limited to receiving one (1) free hour per month of US Signal labor time to make such changes. If US Signal labor time exceeds one (1) hour for the month, hourly service rates shall apply. To request a configuration change, Customer may open a ticket with US Signal's Technical Operations Center ("TOC") by calling 888.663.1700 or by emailing toc@ussignal.com.

15.2.2 Terms

The term of this Agreement shall be the Service's Initial Term (SIT) set forth in the OFS, but in no event shall be less than twelve (12) months. The SIT for all SASE Services shall automatically renew for successive one-year periods thereafter (each the "Service's Renewal Term") unless Customer or US Signal provide the other party with written notice of its intention not to renew at least thirty (30) days before the expiration of the SIT or the Service's Renewal Term, individually and collectively referred to as the "Service Term". Should any OFS be submitted by Customer for additional SASE Services and/or SASE hardware (an "Additional Order") as defined within this Section 15 during any Service Term, the SIT of such Additional Order shall be pro-rated to concur with the existing Service Term so that the termination of all initial and renewal SASE Service Terms shall coincide to take effect on the same date.

15.2.3 Cato Terms

Customer's continued use of Cato proprietary software as a service ("SaaS"), hardware, software and/or services that are delivered to Customer shall be subject to Customer's compliance with Cato's Master Service Agreement found at https://www.catonetworks.com/msa/.

15.2.4 US Signal Responsibilities

US Signal is responsible for (a) providing Customer with the Licenses set forth on the OFS and in accordance with the terms of the Agreement; (b) setup and configuration of services; (c) escalating applicable support requests to Cato Networks Inc.

15.2.5 Customer Responsibilities

Customer will be responsible for (a) providing a project lead to serve as primary point of contact for SSE implementation; (b) providing information for setup and configuration including but not limited to network traffic, services, and data, to allow or deny; (c) notifying of technology and rule changes.

15.2.6 Technical Standards of Performance

Refer to https://ussignal.com/sla-agreements for the technical standards of performance.

15.2.7 SSE Outage Credits

In the event US Signal fails to meet the service metrics as defined in Technical Standards of Performance above, Customer shall be entitled to a credit determined according to the table below. Availability is determined based upon the following formula:

A = (T – M – D) / (T – M) x 100%
A = Availability
T = Total Monthly Minutes
M = Maintenance Time
D = Downtime

Availability	SSE Credit
>=97.9% but < 99.999%	5% of SSE MRC
>=96.9% but < 97.9%	7% of SSE MRC
< 96.9%	9% of SSE MRC

To receive credits, Customer must make a written request within forty-five (45) days of the end of the month for which the interruption occurred. In no event will credits during any one (1) calendar month exceed 100% of the MRC for the Service. Any credit shall be Customer's sole and exclusive remedy for any failure by US Signal to meet a service metric. Outage credits do not apply to outages: (i) caused by the negligence or willful misconduct of Customer; (ii) an outage due to Customer's network failure; (iii) due to failure of power (excluding any industry standard back-up power sources that US Signal is required to have in place); (iv) during any period in which US Signal is not given access to Customer's premise if necessary to resolve an outage; (v) during any period of unscheduled emergency maintenance or repair, scheduled maintenance, alteration or implementation; and (vi) during any Force Majeure Event as defined herein. US Signal may withhold issuance of any credits due Customer under this Agreement until any amounts past due by Customer have been paid in full.

15.3 Co-Management (Optional)

SASE, and the SD-WAN and SSE features, is managed through the Cato Management Application ("CMA"). Customer will have the optional ability to manage network, access and security configuration items within the CMA. Customer accepts the risk that altering initial network and site configurations can impact performance and availability of the platform. As a result, Customer will not be entitled to Outage Credits arising out of or related to configuration changes made by Customer. Customer also acknowledges that changes made to initial security configurations could expose the Customer's network, endpoints, and users to risk of exploitation, malware and availability. As a result, Customer accepts responsibility for security related incidents arising out of or related to configuration changes made by the Customer.

15.3.1 Scope of Service

US Signal Responsibilities:

a. During Implementation:
   i. Work with the Customer to set scope and timeline of implementation and onboarding.
   ii. Document configuration information provided by Customer.
   iii. Configure initial settings of the Customer's Cato account including network, access, and security configuration items.
   iv. Assist with the configuring of security policies throughout implementation to improve the Customer's security posture.
   v. Assist Customer with the installation of equipment where possible.
   vi. Work with the Customer to activate Cato sockets and test connectivity.

b. For Support and Incident Response:
   i. Assist in the investigation and diagnosis of incidents.
   ii. Work with the platform vendor to troubleshoot platform related issues.

c. For management and configuration changes through the use of the CMA:
   i. US Signal will provide Tier 1 and Tier 2 support for any configuration changes and consult with the Customer on how configuration changes can be made on the CMA.

ii. US Signal will manage and update network configuration settings for sites within US Signal managed data center networks, and cloud interconnect sites that connect to US Signal MPLS Services. US Signal is not responsible for updating network configuration settings for sites relating to a Customer's colocation cabinet within a US Signal data center.
iii. US Signal will be responsible for acquiring new or upgrading existing licensing, equipment, or any other SASE Services on behalf of the Customer.

Customer Responsibilities:

a. During Onboarding and Implementation:
   i. Work with US Signal to set scope and timeline of the onboarding project.
   ii. Provide necessary configuration information to US Signal to configure sites, network settings, routing, security policies, access authentication and policies.
   iii. Review and approve baseline configuration of security policies.
   iv. Install equipment with the assistance of a US Signal field technician (where available).
   v. Deploy and configure the mobile user client on Customer's endpoints.
   vi. Activate and test sites with the assistance of US Signal technician.

b. For Ongoing Support and Incident Response:
   i. Customer will be responsible for any impact on performance and availability of the SASE platform as a result of network configuration changes.
      1. Customer will not be entitled to any SD-WAN Outage Credits if it is determined the outage was caused by a configuration change made by the Customer.
      2. US Signal will charge Customer for billable hours if a US Signal TOC technician is engaged to assist with resolving any performance issues or outages that are a result of a network configuration change made by the Customer.
   ii. Customer will be responsible for any security incidents that are caused as a result of configuration changes made by the Customer.
      1. Customer will not be entitled to any SSE Outage Credits if it is determined the outage was caused by a configuration change made by the Customer.
      2. Customer is responsible for resolving any security incident as a result of a change they have made.
      3. US Signal will charge Customer for billable hours if a US Signal TOC technician is engaged to assist with resolving any security incident that is a result of a security configuration change made by the Customer.

c. For monitoring, management and configuration changes through the use of the CMA:
   i. Customer is responsible for monitoring of the platform and responding to events generated by the platform.
   ii. Customer will have the ability to modify network settings for all sites excluding the sites that are hosted on a US Signal managed data center network or a cloud interconnect site that connects to a US Signal MPLS Service.
   iii. Customer will have the ability to modify access settings including the creation, removal and modification of remote users, remote user license assignments, authentication services, and access control settings.
   iv. Customer will have the ability to create and modify security settings including firewall configurations, as well as advanced security features including IPS, NGAM, DLP, CASB, and RBI.
   v. Customer will receive notification of network and security events as identified by Cato XDR and will have the ability to respond to these events.
   vi. Customer will be responsible for tracking any changes made on the CMA through the use of the audit trail or their own change control mechanism.
   vii. Customer will be responsible for creating, removing and managing administrator accounts. Customer will also be responsible for the authentication methods of administrator accounts including two-factor authentication.

SECTION 16 ADDITIONAL TERMS AND CONDITIONS

US Signal utilizes third-party service providers for various licensing, subscriptions, and other service elements that are vital components of the products and services offered within this schedule. In the event a third-party service provider to US Signal materially increases the costs of its products or services ("Third Party Cost Increase"), US Signal reserves the right to increase the price on impacted products and services upon notice to Customer.