Effective January 1st, 2026. This Service Attachment for Cyber Security Solutions and Backup and Disaster Recovery Services supersedes and replaces all prior versions.

Services Attachment for Cyber Security Solutions, Backup and Disaster Recovery Services

This Service Attachment is between Cronos, the 'Provider' (sometimes referred to as "we," "us," or "our"), and the 'Client' found on the applicable Order (sometimes referred to as "you," or "your,") and, together with the Order, Master Services Agreement, and other relevant Service Attachments or Descriptions, forms the Agreement between the parties the terms to which the parties agree to be bound.

The parties further agree as follows:

Provider will deliver only the Services itemised in the Services section of the Order, and/or subsequent Purchase Orders. The following is a list of available solutions and services. Additional Services may be added only by entering into a new Order including those Services.

DATA BACKUP AND RECOVERY SERVICE

To the extent ordered by Client, Provider will perform the following services related to backup and disaster recovery:

1. Local Backups

1.2 Description:

1. Provider, through its Third-Party Service Providers, will utilise backup software, backups will be performed on a nightly basis or at agreed intervals. The provider selects best of breed providers for these services and will clearly indicate the recommended provider based on the Client requirements.

1.3 Hardware and Software

2. Provider utilises Third-Party Service Providers who own the hardware and software agents (backup software) used to perform the backups.

1.4 Provider responsibility:

3. To work with the Third-Party Service Provider, to ensure the process is implemented as agreed, whether that includes backup, disaster recovery, malware scanning, AI scanning or any other element of the backup and disaster recovery scope agreed.

1.5 Client responsibility:

4. Notify the Provider of any failures
5. If requested, perform simple on-site tasks (e.g., powering down and rebooting hardware).

2. Remote Back Up

2.1 Description

1. Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at Provider's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution.

2.2 Hardware and software:

2. There is no additional hardware required.
3. All data is backed up via a third-party client-side desktop/server software application (the "Application")

2.3 Provider responsibility:

4. Notify the Client of any failures, either via the portal or email notifications.
5. Work with third-party to resolve backup failures Client responsibility:
6. If requested, perform simple on-site tasks (e.g., powering down and rebooting hardware).

3. Cloud Backup

3.1 Description:

1. Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, stored on a third-party owned storage server at the Third-Party Services Provider's data center facility.

3.2 Hardware and Software:

2 The Third Party Service Provider owns the hardware and includes third-party software agents used to perform the backups.

3.3 Provider Responsibility

3 Monitor the status of all scheduled backup jobs.
4 Notify Client of failures and corrective actions via the portal or email notifications.
5 Perform additional remote responsibilities to manage Provider Owned Storage.
6 Contact Client should user intervention be required, such as power cycling servers.

3.4 Client responsibility

7 If requested, perform simple on-site tasks (e.g., powering down and rebooting hardware).
8 Maintain all Protected Workloads in a state of operational readiness and ensure that the Third Party Service Providers Agent remains installed and operational on each Protected Workload at all times.

4. Disaster Recovery

Client may select Disaster Recovery services, in addition to back up, this will be provided by the same Third Party Service Provider and can see the data recovered to the clients choice of their own server or a cloud created server, should the clients servers not be considered suitable for recovery.

4.1 Description:

This service enables the Client's Protected Workloads to be failed over to virtual machines running in the Third Party Service Providers Cloud Infrastructure in the event of a hardware failure, ransomware attack, natural disaster, or other disruptive incident, with the aim of restoring business operations within the agreed Recovery Time Objective.

The Disaster Recover As A Service (DRaaS) operates on a continuous replication model. The Agent, installed on each Protected Workload, routinely captures incremental backup images of the system disk, data volumes, and configuration state at intervals defined by the agreed backup policy. These images are encrypted in transit and at rest, and are transmitted to the Third Party Service Providers Cloud Infrastructure where they are stored as recovery points.

In the event that a Protected Workload becomes unavailable, the Client may initiate a Failover from the Management Console. During Failover, Third Party Service Providers instantiates a cloud-based virtual machine (a "Recovery Server") using the most recent clean recovery point. The Recovery Server is made accessible to the Client via a secure site-to-site VPN tunnel or point-to-point connection, allowing end users to resume working with minimal interruption.

Once the primary environment has been restored or rebuilt, the Client will coordinate a Failback to return operations to the Client's primary infrastructure. Only changed data blocks are transferred during Failback, reducing downtime associated with the migration. This process is fully supported by the Third Party Service Provider.

The service supports automated Failover using pre-configured Runbooks, which define the order and conditions under which Protected Workloads are recovered. This orchestration capability reduces manual intervention and shortens recovery time for environments with interdependent systems.

4.2 Hardware and Software:

1. The Third Party Service Provider owns the hardware and provides software agents used to perform the backups and disaster recovery.

4.3 Provider Responsibility

2. Support the Client with the service set-up and onboarding of the DRaaS
3. Provide first-line technical support in relation to the DRaaS service during the Company's standard support hours as defined in the main Agreement.
4. Provide the Client with access to reporting on backup status and storage usage.
5. Provide the Client with a post-incident report within five (5) business days of the conclusion of the Failover event.

4.4 Client responsibility

6. Maintain all Protected Workloads in a state of operational readiness and ensure that the Agent remains installed and operational on each Protected Workload at all times.

5. Cyber Security Solutions

Client may select cyber security services, including, but not limited to, Endpoint Management, Email Security, Patch Management, Data Loss Prevention, Anti Malware and Anti Ransomware solutions. These will be provided by a recommended Third Party Service Provider. These services are delivered as a unified, integrated offering through a single management console and a single software agent deployed on each Managed Endpoint. In the event of any conflict between this Schedule and the main body of the Agreement, this Schedule shall prevail in respect of the services described herein.

5.1 Description:

Remote Monitoring and Management (RMM)

The RMM service provides the Client with continuous, real-time visibility into the health, availability, and security posture of all Managed Endpoints and the Client's Microsoft 365 environment. The Agent collects endpoint telemetry including CPU, memory, disk, network performance, service status, and security posture data, and transmits this to the Management Console. The platform uses this data to proactively identify and resolve issues before they affect end users.

Email Security

The Email Security service protects the Client's inbound and outbound email traffic from a comprehensive range of threats, before malicious content reaches end-user inboxes. The service is powered by Perception Point technology, integrated natively within the Third Party Service Providers platform, and operates at the gateway layer, scanning 100% of email traffic in real time.

Patch Management

The Patch Management service automates the discovery, testing, and deployment of Patches across all Managed Endpoints. The Agent continuously scans each endpoint for missing operating system updates and third-party application patches, generating a prioritised list of vulnerabilities based on severity.

Anti-Malware and Anti-Ransomware Protection

The Anti-Malware Protection service provides continuous, real-time protection on every Managed Endpoint against malware, ransomware, spyware, trojans, rootkits, and other malicious code. The service operates through the Agent and uses a combination of approaches to achieve broad and deep protection:

Endpoint Management – Managed Detection and Response (MDR)

The MDR service extends the endpoint security capabilities by adding continuous human-led monitoring, threat hunting, and active response, delivered by the Third Party Service Providers 24/7 Security Operations Centre. The MDR service is designed for clients who require around-the-clock security oversight beyond the automated controls already in place.

The Agent collects rich endpoint telemetry, including process activity, network connections, file system changes, registry modifications, and authentication events and forwards this to the Third Party Service Providers SOC. The SOC team ingests this telemetry alongside broader threat intelligence feeds and analyses it continuously using EDR tooling, XDR correlation, and human expertise. The service is structured around the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).

- Continuous monitoring: The SOC monitors all endpoint telemetry from Managed Endpoints on a 24/7 basis, filtering noise and prioritising genuine threats.
- Threat hunting: SOC analysts proactively hunt for indicators of compromise and attacker behaviours that automated detection may not immediately surface, using MITRE ATT&CK framework techniques as a reference.
- Triage and investigation: When a potential threat is identified, SOC analysts investigate the full attack chain, from initial entry through lateral movement and privilege escalation, to determine scope and severity.
- Incident response: On confirmation of a threat, the SOC takes agreed response actions, which may include isolating affected endpoints, terminating malicious processes, blocking attacker infrastructure, and initiating point-in-time recovery from clean backup states. Critical response actions (such as server isolation) are subject to human-in-the-loop approval by the Company or an authorised Client contact, as agreed at onboarding.
- Reporting: The SOC provides post-incident reports, audit trails, and ongoing summary reporting to demonstrate service value and support compliance requirements.

Data Loss Prevention (DLP)

The DLP service prevents the unauthorised transfer of sensitive data from Managed Endpoints via peripheral devices (such as USB drives, external hard drives, and smartphones) and network communication channels (including email, web uploads, cloud storage applications, and instant messaging). The service operates through the Agent and is centrally managed via the Management Console.

5.2 Hardware and Software:

1. The Third Party Service Provider owns the hardware and provides software agents used to run the services.

5.3 Provider Responsibility

2. Support the Client with the service set-up.
3. Provide first-line technical support in relation to the services during the Company's standard support hours as defined in the main Agreement.
4. Provide the Client with periodic service reports covering endpoint health, patch compliance, threat detections, email security events, and DLP incidents.

4.4 Client responsibility

5. Maintain all Protected Workloads in a state of operational readiness and ensure that the Agent remains installed and operational on each Protected Workload at all times.

IF CLIENT CHOOSES A NON-PROVIDER-SUPPLIED BACKUP OR CYBER SOLUTION, THE PROVIDER CANNOT GUARANTEE ANY OUTCOMES. CLIENT SHALL BE SOLELY RESPONSIBLE FOR ANY RESULTING OUTCOMES FOR NOT USING THE PROVIDER-SUPPLIED BACKUP OR CYBER SOLUTION, PROVIDER MAY CHANGE THE THIRD PARTY SERVICE PROVIDER AT ANY TIME BUT MUST THE CLIENT MUST BE INFORMED.

6. Support Services

In connection with the Services that are within the scope of this Service Attachment, we will provide to your designated administrator(s), technical contacts or users: management of the Services by individuals trained in the Services you have selected.

7. Setup

We recommend a fully managed installation of services, to ensure they are correctly set up and fully functioning. In this instance, Provider will install the services, for backup and DR, this would include, scheduling all backup routines, program appropriate alerts, and ensure a successful initial backup and testing the DR mapping and service. For all cyber security services, Provider similarly will install the endpoint agent, set up the applicable policies, and ensure a successful deployment.

In the event of a Client choosing to self deploy, the Provider will only be able to support with services correctly activated. The portal will show which services are correctly activated.

CLIENT OPERATING ENVIRONMENT

Unless otherwise agreed in writing by the parties, Client must ensure the availability of Client's network, IP WAN connection, and all component systems to be backed up by the Provider backup Service.

In addition, unless otherwise agreed in writing by the parties, Client also must define appropriate backup sets and schedules for those systems to be backed up before Provider may commence delivery of Services under this Attachment. Provider cannot and does not guarantee to successfully back up all open files.

Unless otherwise specifically agreed by the parties, Provider is not obligated to perform any data forensic or restoration operations under this Attachment.

SERVICE FEES AND SUPPORTED DEVICES

8. Setup Fee

Prior to the delivery of the Services, Provider will charge a Setup Fee in order to connect to Client's environment and to deploy any software required in order to deliver the Services under this Service Attachment. Provider will identify the Setup Fee in an initial invoice, and Client shall pay the Setup Fee, as set forth in the MSA. Provider shall have no obligation to continue with the delivery of any Services under this Service Attachment until it receives payment.

9. Service Fee

If total number of client installations and optional plugins covered within the scope of

this Service Attachment determined by Provider in any month is greater than the number of units determined at the beginning of the preceding month, Provider (1) will include in its next invoice charges for all additional Units placed in service during the preceding month, and (2) will increase the number of Units invoiced in future months, unless and until Provider determines that the number of Units has decreased.

Client shall pay Service Fees specified in the Order. Any devices via the Services must be limited to equipment accessed only by Client's employees, consultants, contractors, or agents who are authorised to use the Services. Client shall not allow any third parties to access any devices connecting to Services within the scope of this Service Attachment.

The fees to be charged will be based on actual number of Units added to the scope of this Service Attachment, as directed by Client, and on the actual volume of any offsite data-storage capacity required to back up Client Data rounded to the nearest gigabyte, subject to a required monthly minimum of the greater of (1) 50 GB, or (2) the data volume identified in the first month's invoice for Services. In addition, under no circumstances during the Term may the total number of Units decrease to less than the number of Units indicated in the Order. Provider's invoices will be based on at least that number, notwithstanding any actual decreases in those numbers. Client shall pay all such charges as set forth in the MSA. The Fees for the Service are stated in the Order.

PROVIDER OBLIGATIONS AND WARRANTY

In addition to delivery of the Services, Provider accepts the following obligations under this Service Attachment:

10. Data Security and Privacy

In addition to its other confidentiality obligations under this Service Attachment, Provider shall not have access to the Client data being managed by the Third Party Service Provider. The Third Party Service Providers Terms are available alongside this document in the Providers portal or website.

As between Provider and Client, all Client Data is owned exclusively by Client. Client Data constitutes Confidential Information subject to the terms of the MSA, and shall be returned to Client upon request, provided that Client is current in all payments, termination fees, and third-party service fees. Provider may access Client's User accounts, including Client Data, solely to respond to service or technical problems or otherwise at Client's request.

11. Maintenance Windows

Routine server and application maintenance and upgrades will occur during scheduled maintenance windows, and some applications, systems or devices may be unavailable or non-responsive during such times.

12. Warranty

Provider warrants that the Services will be performed materially in accordance with the service documentation previously provided for the Services in a professional and workmanlike manner.

HOWEVER, PROVIDER DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE. THERE ARE RISKS

INHERENT IN INTERNET CONNECTIVITY THAT COULD RESULT IN THE LOSS OF YOUR PRIVACY, CONFIDENTIAL INFORMATION, AND PROPERTY. WE HAVE NO OBLIGATION TO PROVIDE SECURITY OTHER THAN AS STATED IN THIS SERVICE ATTACHMENT. WHILE THE SERVICES ARE DESIGNED TO IMPROVE THE PROBABILITY OF THE PROTECTION AND RECOVERY OF INFORMATION COMPARED TO THE CLIENT'S CURRENT METHODS EMPLOYED, PROVIDER MAKES NO CLAIMS OR WARRANTIES THAT DATA BACK-UPS AND DATA / SERVER / DESKTOP RECOVERIES USING THE SERVICES WILL BE ERROR FREE OR THAT ALL RECOVERIES CAN BE PERFORMED WITHIN A CERTAIN TIME FRAME.

IN ADDITION, CLIENT ACKNOWLEDGES THAT THIS AGREEMENT CONVEYS NO WARRANTIES, EXPRESS OR IMPLIED, BY ANY THIRD-PARTY VENDORS OF SOFTWARE PRODUCTS MADE AVAILABLE TO CLIENT BY PROVIDER AND THAT THOSE VENDORS DISCLAIM ANY AND ALL LIABILITY, WHETHER DIRECT, INDIRECT OR CONSEQUENTIAL, ARISING FROM THE SERVICES.

ADDITIONAL CLIENT OBLIGATIONS

13. Hardware Equipment

Client equipment must be maintained under manufacturer's warranty or maintenance contract or is in working order. Provider is not responsible for client equipment that is not maintained under manufacturer's warranty or maintenance contract or that is otherwise out of order. All fees, warranties, and liabilities against Provider assumes equipment is under manufacturer's warranty or maintenance contracts or is in working order.

Provider in its reasonable opinion and supported by manufacturer information, may designate certain equipment as obsolete or defective, and therefore exclude it from coverage under this Agreement.

14. Minor On-Site Tasks

Provider may occasionally ask you to perform simple on-site tasks (e.g., powering down and rebooting a computer). Client agrees to cooperate with all reasonable requests.

15. Software Media

Client shall obtain and supply all necessary software media with installation keys (if any) upon request.

Except for any software provided by Provider in connection with the Services, you are solely responsible for obtaining all required software licenses, including all client access licenses, if any, for the software products installed on your computers.

TERM AND TERMINATION

16. Term

This Service Attachment is effective on the date specified on the Order (the "Service Start Date") or if not specified then the first live date for the relevant service. Unless properly terminated by either party, this Attachment will remain in effect through the end

of the term specified on the Order (the "Initial Term").

16.1 Renewal

"RENEWAL" MEANS THE EXTENSION OF ANY INITIAL TERM SPECIFIED ON AN ORDER FOR AN ADDITIONAL TWELVE (12) MONTH PERIOD FOLLOWING THE EXPIRATION OF THE INITIAL TERM, OR IN THE CASE OF A SUBSEQUENT RENEWAL, A RENEWAL TERM. TO ENSURE CONTINUITY, THIS SERVICE ATTACHMENT WILL RENEW AUTOMATICALLY UPON THE EXPIRATION OF THE INITIAL TERM OR A RENEWAL TERM UNLESS ONE PARTY PROVIDES WRITTEN NOTICE TO THE OTHER PARTY OF ITS INTENT TO TERMINATE NO MORE THAN SIXTY (60) DAYS PRIOR TO AND NO LESS THAN THIRTY (30) DAYS PRIOR TO THE EXIPIRATION OF THE INITIAL TERM OR THE THEN-CURRENT RENEWAL TERM. ALL RENEWALS WILL BE SUBJECT TO PROVIDER'S THEN-CURRENT TERMS AND CONDITIONS.

16.2 Early Termination by Client With Cause

Client may terminate this Agreement for cause following sixty (60) days' advance, written notice delivered to Provider upon the occurrence of any of the following:

- Provider fails to fulfill in any material respect its obligations under the Agreement and fail to cure such failure within thirty (30) days following Provider's receipt of Client's written notice.
- Provider terminates or suspends its business operations (unless succeeded by a permitted assignee under the Agreement).

16.3 Early Termination by Client Without Cause

If Client has satisfied all of its obligations under this Service Attachment, then no sooner than ninety (90) days following the Service Start Date, Client may terminate this Service Attachment without cause during the Initial Term upon sixty (60) days' advance, written notice, provided that Client pays Provider a termination fee equal to fifty percent (50%) of the recurring, Monthly Service Fees remaining to be paid from the effective termination date through the end of the Initial Term, based on the prices identified on the Order then in effect.

16.4 Termination by Provider

Provider may elect to terminate this Service Attachment upon thirty (30) days' advance, written notice, with or without cause. Provider has the right to terminate this Service Attachment immediately for illegal Client conduct. Provider may suspend the Services upon ten (10) days' notice if Client violates a third-party's end user license agreement regarding provided software. Provider may suspend the Services upon fifteen (15) days' notice if Client's action or inaction hinders Provider from providing the contracted Services.

16.5 Effect of Termination

As long as Client is current with payment of: (i) the Fees under this Attachment, (ii) the Fees under any Project Services Attachment or Statement of Work for Off-Boarding,

and/or (iii) the Termination Fee prior to transitioning the Services away from Provider's control, then if either party terminates this Service Attachment, Provider will assist Client in the orderly termination of services, including timely transfer of the Services to another designated provider. Client shall pay Provider at our then-prevailing rates for any such assistance. Termination of this Service Attachment for any reason by either party immediately nullifies all access to our services.
Provider will immediately uninstall any affected software from Client's devices, and Client hereby consents to such uninstall procedures.

Upon request by Client, Provider may provide Client a copy of Client Data in exchange for a data-copy fee invoiced at Provider's then-prevailing rates, not including the cost of any media used to store the data. After thirty (30) days following termination of this Agreement by either party for any reason, Provider shall have no obligation to maintain or provide any Client Data and shall thereafter, unless legally prohibited, delete all Client Data on its systems or otherwise in its possession or under its control.

Provider may audit Client regarding any third-party services. Provider may increase any Fees for Off-boarding that are passed to the Provider for those third-party services Client used or purchased while using the Service.