Unitrends DRaaS Service Schedule

This DRaaS Service Schedule is subject to all terms and conditions of the Unitrends Cloud Services Terms and Conditions set forth at https://www.unitrends.com/legal-notices/service-schedule-unitrends-cloud-services/, as the same may be updated from time to time, and is incorporated by reference therein. All defined terms used herein shall have the meaning accorded to such terms in the Service Schedule for Unitrends Cloud.

DRAAS SUMMARY

Customers with an active Unitrends Cloud Services subscription may purchase the Unitrends Disaster Recovery as a Service (DRaaS) for use with the Unitrends Cloud Services in the event of a Disaster.
Subject to Customer's payment of the applicable Fees and compliance with this Service Schedule, the DRaaS includes:

- Onboarding to establish Replication of Protected Servers to the Unitrends Cloud Services. A key focus of the onboarding and testing portion of the service is to validate critical systems readiness to transition operation to the Unitrends Cloud Services in the event of a Disaster.
- Disaster recovery (DR) testing on a periodic basis to validate Disaster recovery readiness, as well as to facilitate changes to the DR Environment. Frequency of DR testing is based the Customer's service level; see SCOPE OF DRAAS SERVICE for details. If frequent testing is needed, Elite or Premium DRaaS is recommended.
- Assisted Disaster recovery of protected systems in a pre-configured DR Environment on the Unitrends Cloud after Customer declares Disaster.
- Recovery Assurance as a Service, included with Elite or Premium DRaaS, provides regularly scheduled automated DR Testing and reports.
- Next business day shipment, after the data export is complete, of replacement Unitrends hardware in the event of a failure of the Unitrends hardware.

SCOPE OF DRAAS SERVICE

Unitrends will provide Customer a functional DR Environment to utilize the Replicated Customer Content for recovery within the Unitrends Cloud Services as follows:

Standard and Unlimited DRaaS Service

- Assisted failback in the onset of a DR Event.
- 30 days of operational or test use of the Unitrends Cloud per 12-month contract period.

- The number of free declarations used for manual DR testing is limited to one free declaration per 12-month contract period.

Elite DRaaS Service:

- Access to Protected Servers within twenty-four (24) hours after the Disaster declaration has been made to Unitrends.
- Assisted failback after the DR Event.
- 30 days of operational or test use of the Unitrends Cloud per 12-month contract period.
- Regularly scheduled automated DR testing and reports via Unitrends Recovery Assurance as a Service. Unitrends will assist the Customer in setting up automated tests based on the Customer's recovery objectives.

Premium DRaaS Service:

- Access to Protected Servers within one (1) hour after the Disaster declaration has been made to Unitrends.
- Assisted failback after the DR Event.
- 30 days of operational or test use of the Unitrends Cloud per 12-month contract period.
- Regularly scheduled automated DR testing and reports via Unitrends Recovery Assurance as a Service. Unitrends will assist the Customer in setting up automated tests based on the Customer's recovery objectives.

All DRaaS service levels require that the Customer purchases DRaaS and has an active subscription to Unitrends Cloud Services and Unitrends support services.

ONBOARDING SERVICES

1. DRaaS Onboarding Commencement Criteria

1.1 Customer contact will be provided to an authorized Unitrends technical contact and will act as a single point of contact.

1.2. Customer will provide all necessary requested information, such as (but not limited to) list of Protected Servers and their hostnames, IP addresses, network configuration, OS versions, application functions, and such other information as reasonably requested by Unitrends prior to DRaaS onboarding.

2. DRaaS Onboarding

2.1. Unitrends will conduct kickoff meetings with the Customer to discuss the expectations for DRaaS delivery, roles, responsibilities and dependencies, and DR Testing objectives.

2.2. Unitrends will work with customer to identify protected servers, and setup their network configurations as well as appropriate boot order in the event of a DR Event.

2.3. Unitrends will validate appropriate configuration of backup and replication of Protected Servers, including the proper use of Unitrends backup clients and agents.

2.4. Unitrends will implement DRaaS and configure Customer's SSL VPN access, as well as potential use of public IP's.

2.5. Customer will test and validate the functional use of Protected Servers.

2.6. Unitrends will deliver a functional DR Environment, which can be validated via scheduled manual testing or through Unitrends DR automation software, if available under the purchased DRaaS service option.

2.6.1. If the Customer has purchased an option that includes Recovery Assurance testing, Unitrends will configure the automation software with scheduled test, which will send Customer a status report upon completion.

2.6.2. Unitrends will work with Customer to identify and setup disaster recovery policies for Protected Servers, such as:

- Application Recovery Time Objectives
- Application Recovery Point Objectives
- Network mappings & IP reconfiguration
- Boot orders dependencies & VM time-out
- Critical and non-critical VMs
- User-defined Acceptance Tests

2.6.3. Unitrends will work with the Customer to set up application level orchestration scripts for Microsoft applications to be executed for automated DR Testing as well as for VM spin-ups during a DR Event.

ONGOING DRAAS SCHEDULED TESTING

3. DRAAS Testing

3.1. Scheduling a manual DR Testing Period. Testing of Unitrends DRaaS Protected Servers provides the Customer with the ability to validate the availability and functionality of their Protected Servers in the event of a DR Event. Manual disaster recovery testing can be done completely free once per 12-month period starting with the contract start date. Additional tests may be subject to a fee for the labor and infrastructure to perform failover and failback. In order to schedule a manual testing period the Customer must contact Unitrends Support to schedule DR Testing of the environment. Additionally, a moratorium of DR Testing may be placed in the event of another customer declaring a DR Event.

Note: For situations where frequent testing is needed, Unitrends recommends Elite o Premium DRaaS with weekly and monthly automated testing and reporting, which does NOT consume any of your 30-day run time allotment in the Unitrends Cloud. That test time is included in the Elite and Premium services.

3.2. Use of Recovery Assurance Automated Testing, included with Elite and Premium DRaaS. If Customer has enrolled in Elite or Premium DRaaS, or separately licensed Unitrends' Recovery Assurance software for their cloud instances, DR Testing will be automated and configured to run on a scheduled basis and includes delivery of a status email upon the completion of the automated DR Testing.

DISASTER EVENTS

4. Declaration of DR Event

A declaration event is used to initiate the full (or partial) spin up of a customer's DRaaS entitlement in the Unitrends Cloud based on the level of service purchased. Declaration events can be used for true disaster recovery, as well as manual disaster recovery tests. A declaration event, whether for testing or true failover, will consume the allotted 30-days of run time entitlement in the Unitrends Cloud. The declaration of a DR Event occurs when the Customer declares a disaster or testing event by notifying Unitrends support services via phone (email declarations will not be accepted). Declaration of a DR Event means that the entire list of Protected Services as validated during the last DR Testing period will be recovered and booted up on the Unitrends Cloud. There may be a delay for physical systems which may be in a testing state prior to the declaration of Disaster while re-initialization to a warm state is in progress.

Upon a DR Event declaration, Unitrends will perform the following:

- Recovery of Protected Servers
- Enablement of SSL VPN Account for customer employees' access into the DR Environment (number of simultaneous SSL VPN sessions may be limited based on overall DRaaS platform usage by all Unitrends customers)
- Configuration of a backup target for live Protected Servers running on the Unitrends Cloud
- Configuration of live Protected Servers to backup utilizing Unitrends Incremental Forever schedule.

5. Customer Failback

When the Customer notifies Unitrends that they are ready to failback, Unitrends will replicate the latest version of the Customer's VMs in Unitrends DRaaS and ship the data on a temporary replacement appliance via expedited shipping. Unitrends will provide a prepaid return label for the customer to ship the replacement appliance back to Unitrends once failback is complete.

6. Changes in Environment

For Elite and Premium service levels, Customer must notify Unitrends Support of any changes to the Protected Servers for DRaaS to ensure that full recovery testing is completed and that RTOs can be met in the event of disaster. For Unlimited service levels, which does not include automated testing or a recovery SLA, it is not necessary to notify Unitrends of changes to Protected Servers.

OPERATING SYSTEMS

7. Supported Operating Systems

The following systems can be protected by Unitrends DRaaS. A valid backup must be available on the target.

- Windows OS
- Hyper-V VMs
- VMware VMs
- Exchange Databases (with valid OS backup)
- SQL Databases (with valid OS backup)

ASSUMPTIONS AND CUSTOMER RESPONSIBILITIES

8. DRaaS Assumptions and Customer Responsibilities

Customer acknowledges and agrees to the following assumptions, which apply to the provision of DRaaS and the use of DRaaS with Unitrends Cloud Services. If Customer does not comply with the following assumptions, Unitrends may not be able to provide the DRaaS to the Customer or may not be able to provide DRaaS in a timely manner. Any failure of Unitrends as a result of Customer's failure to meet the following assumptions will not be deemed a breach of any implied or expressed service level agreement between Unitrends and the Customer or a breach of this DRaaS Service Schedule.

8.1 DRaaS Assumptions

1. Customer will have an active subscription to the Unitrends Cloud Service and, if Customer has elected to include Recovery Assurance functionality, shall have a valid current contract that includes this service.

2. Customer will make appropriate IT personnel available to Unitrends for the purposes of enabling restoration to the Unitrends Cloud in the event of a DR Event.

3. Customer must timely respond to Unitrends’ requests and provide any requested information in a timely manner. If this information is not received in a timely manner the Unitrends team will proceed based on best possible assumptions in order to meet delivery timeframes.

4. Customer will be responsible for any associated third party licensing fees.

5. Customer will be solely responsible for all administration of its live Protected Servers running within the DR Environment (such as Anti-Virus, Patch Management etc.) during DR Testing or a DR Event.

6. Customer is responsible for performing failover of network traffic to the DR Environment in the Unitrends Cloud during a DR Event.

7. Customer will be responsible for any and all costs and expenses, including any professional services fees resulting from additional effort required of Unitrends as a result of inaccurate or out of date information that was provided by the Customer during onboarding and implementation testing. Customer will be invoiced for such amounts by Unitrends at Unitrends’ then-current professional services rates and will pay all invoices within thirty (30) days of receipt.

8. All Customer systems and applications must be able to operate within a virtual environment.

9. All Customer systems and applications covered under DRaaS must be able to successfully spin up using Unitrends Instant Recovery or Replica technology locally.

10. Windows Replicas will be configured with Unitrends’ Incremental Forever Backups.

11. Additional hardware specific to the Customer’s operation will not be provided by Unitrends; e.g. load balancer, content filtering appliances etc. and will be the responsibility of the Customer.

12. Customer will have RDP and SSH enabled on protected systems in order for Customer administrators to access them during DR Testing or DR

Event.

13. Customer will enable and configure systems and applications to function with DRaaS and Unitrends Cloud Services.

14. Customer will install VMware Tools on its systems, to enable Customer to use its systems within the Unitrends Cloud on a DR Event.

15. Customer will install Windows Agent 7.4 or greater for Hyper-V and Windows physical systems.

16. All systems protected by DRaaS are limited to the documented support functionality within Unitrends Cloud Services and/or applicable Unitrends' software.

17. Unitrends will allocate and assign to Customer's Protected Servers in the Unitrends Cloud DR Environment the exact number of private IP addresses assigned to the source servers in the Customer's production environment.

18. One public address will be provided per Customer in the Customer's Unitrends Cloud DR Environment. Additional public IP's can be made available upon request during DRaaS onboarding or DR Testing.

8.2 Additional Customer Responsibilities

1. Customer is responsible for defining usable private IP addresses to be assigned to the Protected Servers.

2. The use of DHCP is currently not supported with Unitrends DRaaS.

3. Customer is responsible for the addition and/or modification of any access rules required to allow access to their DR Environment. This includes resolving any firewall and/or proxy issues, which might arise at the source location(s).

4. Customer is responsible for ensuring all replication schedules meet recovery objectives. Customer is responsible for providing adequate system resources and bandwidth on source site to ensure performance requirements can be met.

5. Customer is responsible for providing adequate bandwidth from Customer source location(s) to Unitrends data center(s) to ensure performance requirements can be met. Unitrends cannot guarantee performance at any location with insufficient bandwidth and Customer must commit to bandwidth upgrades required to meet any defined performance requirements.

6. Customer is responsible for the addition and/or modification of any DNS rules at the source location(s) required to support services during a failover DR Event.

7. Customer is responsible for contacting Unitrends by phone (e-mail is not permitted) to initiate a Disaster declaration and provide written confirmation of acceptance to remit payment of declaration fee.

8. Customer is responsible for contacting Unitrends to initiate and obtain failback service support.

9. A local account may be required to configure third-party multi-factor authentication (MFA) due to potential time drifts in DRaaS.

9. DRaaS Exclusions/Out of Scope Activities

The following are not included in the scope of DRaaS and are expressly excluded.

1. DRaaS assumes the following level of complexity:

    a. The scope of the Unitrends DRaaS only includes the recovery of Protected Servers and the associated Replicated Customer Content. No implementation of application level recovery is included, other than those provided through Unitrends' automation software for Customers who have purchased a DRaaS service level that includes Recovery Assurance.

2. Multiple public IP addresses for testing purposes.

3. The aliasing of file level backups is not supported for DRaaS failover functionality.

4. Troubleshooting of OS or third-party applications outside of Unitrends Cloud Services.

5. The use of Unitrends Cloud Services other than the spin up of DRaaS on the Unitrends Cloud.

6. Additional technical support other than what is set forth herein. Technical support can be separately purchased by Customer on a time and materials basis.

7. Architectural integration into the Customer's production environment and operations and management of the DRaaS and Unitrends Cloud Services.

8. The creation of an IPSec tunnel to the Customer's DR Environment.

9. Recoverability or performance of any system with inadequate memory and/or processing power. Customer must commit to any and all system upgrades required to meet minimum system requirements.