SERVICE SPECIFIC TERMS / CLOUD

# Backup and Disaster Recovery

Backup as a Service and Disaster Recovery as a Service, powered by Veeam

| VERSION | EFFECTIVE | REPLACES |
|---|---|---|
| v2026.10d | 1 November 2026 | Backup-As-a-Service.pdf, Cloud-Connect.pdf |

These Service Specific Terms form part of your agreement with FirstNet Technology Services (Pty) Ltd. Read them with the FirstNet Standard Terms and Conditions (or your signed Master Services Agreement), your Service Schedule and the Data Processing Annexure, all available at www.firstnet.co.za/legal-notices/.

These Service Specific Terms apply to FirstNet Backup as a Service (BaaS), FirstNet Disaster Recovery as a Service (DRaaS) in its Platform-Only and Managed DR forms, and the Veeam Cloud Connect repositories that FirstNet provides for them, all powered by Veeam.

## 1. Status and precedence

1.1 These Service Specific Terms ("SST") form part of the agreement between FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") and the Customer, being the FirstNet Standard Terms and Conditions or, where the Customer has signed one, the Customer's Master Services Agreement with FirstNet (the "Agreement").

1.2 These SST apply to each Service Schedule (including any scope of work or accepted quote) for the BaaS or DRaaS Service. The Service Schedule records what is ordered, the protected workloads, retention, the vault edition and region, the DR tier, the MRC and NRC, the Initial Period and the Service Commencement Date.

1.3 If documents conflict, they apply in this order: (a) the Service Schedule, only for commercial items that it expressly says override these SST; (b) these SST; (c) the Agreement (including the Data Processing Annexure and the Acceptable Use Policy); (d) the Vendor Terms. Where Vendor Terms impose a mandatory restriction on the use of a Vendor's product, the Customer must comply with it.

1.4 Words defined in the Agreement have the same meaning in these SST. The FirstNet Rapid Response Services Guide (www.firstnet.co.za/legal-notices/) governs how support and restore requests are logged, prioritised and escalated.

## 2. Definitions

2.1 In these SST:

2.1.1 **"Backup Job"** means a Veeam backup or backup copy job that protects a Protected Workload;

2.1.2 **"Change Rate Allowance"** means the maximum daily change rate of protected data (as a percentage of the protected data) on which the vault capacity and replication design in the Service Schedule are based, if the Service Schedule states one;

2.1.3 **"DR Event"** means an event that the Customer declares under clause 3.8, in which the Customer needs to run Protected Workloads from the DR Site;

2.1.4 **"DR Site"** means the FirstNet data centre in South Africa where replicas are held and reserved DR capacity is provided, as stated in the Service Schedule;

2.1.5 **"Failover Test"** means a planned test in which replicas are started in the DR Site and operated as production;

2.1.6 **"Immutable"** means that a recovery point cannot be modified or deleted by anyone (including the Customer and FirstNet) until its immutability period ends;

2.1.7 **"Managed DR"** means the optional managed service described in clause 3.7;

2.1.8 **"Platform-Only DRaaS"** means the DRaaS service described in clause 3.6;

2.1.9 **"Protected Workload"** means a virtual machine or physical server listed in the Service Schedule;

2.1.10 **"Recovery Point"** means a restorable copy of a Protected Workload at a point in time;

2.1.11 **"Repository"** means the Veeam Cloud Connect tenant repository that FirstNet provides for the Customer's backups or replicas, including the Vault where applicable;

2.1.12 **"RPO"** (recovery point objective) and "RTO" (recovery time objective) mean the maximum data-loss window and the maximum time to restore service that the Customer has asked FirstNet to design for;

2.1.13 **"Test Restore"** means a planned restore of a replica or backup to an isolated environment to check that it can be recovered, without running it as production;

2.1.14 **"Track 1"** means BaaS with Veeam licences supplied by FirstNet, and "Track 2" means BaaS where the Customer uses its own Veeam licences and FirstNet supplies the Repository;

2.1.15 **"Vault"** means Veeam Data Cloud Vault, Veeam's cloud storage service that FirstNet uses as the offsite Repository for BaaS, in the edition (Foundation or Advanced) and region catalogue (Core or Non-Core) stated in the Service Schedule.

## 3. Service description

Backup as a Service

3.1 What BaaS is. BaaS keeps an independent, encrypted, offsite copy of the Customer's Protected Workloads (VMware vSphere or Microsoft Hyper-V virtual machines, and physical servers protected by Veeam agents) so the Customer can restore files, application items, or whole virtual machines and servers to the original or an alternate location. The Customer's Veeam Backup and Replication server sends Backup Jobs to the Repository through Veeam Cloud Connect over an encrypted TLS channel.

3.2 Track 1 and Track 2. Under Track 1, FirstNet supplies the Veeam Data Platform Premium licences (including Veeam ONE monitoring and reporting) per Protected Workload, and the Vault. Under Track 2, the Customer licenses Veeam itself and is responsible for its own licence compliance, and FirstNet supplies the Repository.

3.3 Service models. The Service Schedule states whether BaaS is:

3.3.1 self-managed: the Customer configures and runs Backup Jobs, monitors them, fixes failures and performs restores, using the Veeam tools supplied, and FirstNet runs the Repository infrastructure; or

3.3.2 fully managed: FirstNet also designs and sets up the Backup Jobs, monitors jobs and vault capacity, remediates failures within the agreed scope and support hours, performs or assists with restores, runs periodic Test Restores at the frequency in the Service Schedule and provides backup health reports.

3.4 Retention and immutability. Retention (including any weekly, monthly or yearly GFS retention) and the immutability period are set in the Service Schedule. Recovery Points are Immutable for the immutability period where immutability is enabled. During that period no one can shorten retention or delete a Recovery Point, including at the Customer's request, for a data subject request or to reduce storage charges. Immutable and logically isolated (air-gapped) copies reduce, but do not remove, the risk that ransomware or a malicious administrator destroys backups.

3.5 Initial seeding. If the first full backup will not complete over the Customer's bandwidth in the required time, FirstNet and the Customer will agree a seeding approach (for example moving the first full backup offline) before go-live. Seeding media in transit is at the Customer's risk unless FirstNet transports it, and must be encrypted.

Disaster Recovery as a Service

3.6 Platform-Only DRaaS. FirstNet replicates the Customer's VMware vSphere or Microsoft Hyper-V virtual machines into the DR Site using Veeam Cloud Connect Replication, reserves in advance the vCPU, memory and replica storage stated in the Service Schedule for each Protected Workload, provides the replication tenancy and supports the DR platform. The Customer configures replication jobs from its own Veeam console, starts failover and failback, and plans and runs its own DR tests. Platform-Only DRaaS works with Veeam licences supplied by FirstNet or by the Customer.

3.7 Managed DR. Managed DR is an optional add-on to DRaaS, available only where Veeam Backup and Replication is licensed and supplied by FirstNet. Within the tier and support hours stated in the Service Schedule, FirstNet will:

3.7.1 monitor replica jobs and remediate replication failures;

3.7.2 run Test Restores from replicas quarterly (unless the Service Schedule states another frequency) and give the Customer a written test report after each test;

3.7.3 where the tier includes it, prepare and maintain a DR runbook with the Customer, setting out recovery order, dependencies, network and access model, roles and contact details, and review it at least annually and after material changes;

3.7.4 where the tier includes it, assist with failover during a DR Event and with controlled failback; and

3.7.5 provide DR readiness reports at the frequency stated in the Service Schedule.

3.8 DR Events. A DR Event starts when an authorised Technical Contact declares it to FirstNet by telephone and through the Client Zone (clientzone.firstnet.co.za) or support@firstnet.co.za, stating which Protected Workloads must be recovered. Under Platform-Only DRaaS the Customer starts failover. Under Managed DR FirstNet assists as set out in the runbook and tier. Systems run from the DR Site until failback, which is carried out under change control.

3.9 Failover Tests. Test Restores are not Failover Tests. A Failover Test is a separately scoped activity (unless the Service Schedule includes it) that needs the Customer's change approval, application owners and an agreed test window.

3.10 Physical servers. Physical-to-virtual and physical-to-physical replication are not supported. Physical servers are protected through BaaS and, in a DR Event, can be restored into virtual machines in the DR Site, which takes longer than replica failover.

3.11 Reserved capacity. DR capacity is reserved for the Customer and is not shared on a best-effort basis. If the Customer adds or grows Protected Workloads, the reservation must be resized (and the MRC adjusted) for the new workloads to be covered.

What is not included

3.12 Unless the Service Schedule says otherwise, the Service does not include: (a) secure access into the DR Site (such as a hosted firewall VDOM, VPN termination and firewall rules); (b) Failover Tests; (c) backup or replication of Microsoft 365, Google Workspace or endpoint data (covered by the Microsoft 365 Backup SST); (d) application-level recovery testing or application support; (e) connectivity between the Customer's site and FirstNet; (f) standalone Veeam licences (FirstNet does not sell standalone Veeam licences); or (g) recovery of data that was never successfully backed up or replicated.

## 4. Vendor Terms

4.1 The Service is powered by Veeam Software. The following Vendor Terms apply (checked on Veeam's website on 13 October 2026):

| Vendor document | URL | Applies to |
|---|---|---|
| Veeam End User License Agreement (last updated 25 August 2026) | https://www.veeam.com/legal/eula.html | Veeam software the Customer installs (Track 1 and Track 2) |
| Veeam Licensing Policy | https://www.veeam.com/legal/licensing-policy.html | Licence counting and use (Track 2 and Customer-installed software) |
| Terms for Veeam Data Cloud Vault Service Agreement (last updated 27 August 2026) | https://www.veeam.com/legal/veeam-data-cloud-vault-service-agreement.html | Vault restrictions (including encryption of uploaded data, restore allowances and early deletion), as passed through by FirstNet |
| Veeam Data Cloud Fair Use Policy | https://www.veeam.com/legal/veeam-data-cloud-fair-use.html | Vault use |

| Vendor document | URL | Applies to |
|---|---|---|
| Veeam Cloud Services Data Processing Addendum | https://www.veeam.com/legal/data-processing-addendum.html | Veeam's processing of data in the Vault |

Where Veeam requires further end-user terms to apply to Track 1, they form part of the Vendor Terms that apply to the Service, as provided or linked by FirstNet.

4.2 The Customer accepts the applicable Vendor Terms when it signs the Service Schedule or first uses the Service. Track 2 Customers remain bound by their own Veeam licence agreement.

4.3 FirstNet is not liable for changes Veeam makes to its products, editions, licensing or Vendor Terms, or to the Vault catalogue or regions. Where a change materially affects the Service, FirstNet will give as much notice as it reasonably can.

4.4 Veeam may suspend Vault access or licences for breach of its Vendor Terms. FirstNet passes through to the Customer only the warranties and service levels that Veeam gives FirstNet for the Vault and Veeam software, and adds none of its own for them, except any service level the Service Schedule states under clause 7.3 and any warranty that cannot be excluded under the CPA.

## 5. Customer responsibilities

5.1 The Customer must:

5.1.1 keep its Veeam Backup and Replication server, agents and proxies on a version supported by FirstNet's Cloud Connect platform, and (for Track 2) properly licensed;

5.1.2 provide connectivity with enough bandwidth for its Backup Jobs, replication and restores, and keep the Cloud Connect gateway reachable;

5.1.3 keep Cloud Connect credentials and encryption passwords secure, enable multi-factor authentication where available, and tell FirstNet immediately if it suspects they are compromised. FirstNet cannot recover data encrypted with a Customer-held encryption password that the Customer has lost;

5.1.4 tell FirstNet in writing (through a service request) which workloads must be protected, and of any change to them, retention, RPO or RTO targets. FirstNet protects only the Protected Workloads listed in the Service Schedule;

5.1.5 in the self-managed model and under Platform-Only DRaaS, monitor jobs, act on failure notifications, run its own restore and failover tests, and keep its runbook current;

5.1.6 ensure that data is in a consistent, uncorrupted state when it is backed up: FirstNet backs up and restores data in the state in which it was received, and corrupted or infected data will be backed up and restored in that state;

5.1.7 provide application owners, change approvals and test windows for Test Restores and Failover Tests; and

5.1.8 use the Service in accordance with the Acceptable Use Policy and the Vendor Terms, and not store content that is unlawful or that the Customer has no right to store.

5.2 Change Rate Allowance. Where the Service Schedule states a Change Rate Allowance and the Customer's actual change rate exceeds it on a sustained basis, FirstNet will notify the Customer. If the Customer does not reduce the change rate within 7 days of that notice, FirstNet may adjust the capacity (and MRC) to match actual use under clause 9.2, or agree a different RPO or schedule with the Customer.

## 6. Provisioning and lead times

6.1 Onboarding covers scoping, Repository or DR Site provisioning, connection details and credentials, Backup Job or replication setup (where managed), initial seeding, and handover to Rapid Response. Lead times depend on discovery, vault region availability, connectivity readiness and seeding, and any lead time FirstNet gives is indicative only.

6.2 The Service Commencement Date is the date FirstNet provides the Repository credentials (BaaS) or the replication tenancy (DRaaS), as recorded in the handover.

## 7. Service levels and support

7.1 Support is provided through FirstNet Rapid Response under the Rapid Response Services Guide. A ransomware event, suspected compromise of backup infrastructure, or inability to restore a critical Protected Workload is logged as Priority 1. A DR Event is a Major Incident under that guide.

7.2 Restore start. For fully managed BaaS and Managed DR, FirstNet will begin a requested restore within the response time that applies to the request under the Rapid Response Services Guide, or within any restore start time stated in the Service Schedule, after a valid restore request is logged by a Technical Contact, during the support hours of the contracted tier.

7.3 Service levels. Availability targets for the Repository or DR platform, RPO or RTO commitments and any service credits apply only if the Service Schedule states them. RPO and RTO in a solution design or runbook are design targets and not commitments, unless the Service Schedule expressly records them as committed service levels after scoping and testing. Where service credits are stated, they are the Customer's sole financial remedy for missing the service level, except where the failure is also a material breach of the Agreement. The Customer must claim a credit in writing within 30 days after the end of the calendar month in which the failure occurred.

7.4 No recovery guarantee. FirstNet will use reasonable skill and care to restore every Recovery Point that the backup software reports as successfully completed. FirstNet does not guarantee that every Recovery Point can be restored, that restored data will be free of corruption or malware present at the time of backup, or that a restore will complete within a particular time unless the Service Schedule commits to it.

7.5 Exclusions. Service levels do not apply to failures caused by: (a) the Customer's environment, Veeam server, agents, network, bandwidth or credentials; (b) data change rates above the Change Rate Allowance; (c) Vault or other Vendor platform outages outside FirstNet's reasonable control; (d) Microsoft, VMware or other software defects in the Customer's environment; (e) planned maintenance of which FirstNet gave the Customer reasonable advance notice; (f) suspension under clause 11; or (g) force majeure.

7.6 Notifications. FirstNet notifies the Customer's registered Technical Contacts of failed managed Backup Jobs after the configured retries. The Customer must keep its contact details current; FirstNet is not responsible for notifications that do not reach outdated contacts.

## 8. Data, privacy and security

8.1 Roles. For personal information in the Customer's backups and replicas, the Customer is the responsible party and FirstNet is its operator under POPIA. FirstNet processes that information only to provide the Service, on the Customer's instructions, and in accordance with the Data Processing Annexure. Veeam is FirstNet's sub-operator for data held in the Vault.

8.2 Location: DRaaS. Replicas are held in the DR Site in South Africa, unless the Service Schedule names another site.

8.3 Location: BaaS Vault. Data in the Vault is stored by Veeam on Microsoft Azure or Amazon Web Services infrastructure in Veeam's South African region. If the Customer asks for it, FirstNet can also provide a long-term archive tier in Veeam's region in the European Union. Only then is data stored outside South Africa: the Service Schedule will name that region, and the Customer instructs FirstNet to transfer the archived data there. In that case FirstNet relies on Veeam's Data Processing Addendum and the safeguards in the Data Processing Annexure to meet section 72 of POPIA, and the Customer remains responsible for any notice or consent its data subjects need.

8.4 Offshore support access. Veeam's support or operations personnel outside South Africa may access Vault metadata to operate the Vault, as described in Veeam's Data Processing Addendum. Backup content uploaded to the Vault must be encrypted under clause 8.5.

8.5 Encryption. Data is encrypted in transit (TLS) between the Customer and the Repository. Data stored in the Vault must be encrypted, and is encrypted at rest. Where the Customer holds the encryption password, only the Customer can decrypt the data.

8.6 Breach notification. If FirstNet becomes aware of a Security Compromise affecting Customer Personal Information in the Repository or DR Site, it will notify the Customer immediately, and in any event without undue delay, as set out in clause 8 of the Data Processing Annexure and section 21(2) of POPIA, so that the Customer can meet section 22 of POPIA.

8.7 Deletion and exit. When the Service ends, the Customer may restore or export its Recovery Points until the Service ends and for any further period stated in the Service Schedule or agreed with FirstNet in writing. After that, FirstNet will delete the Customer's Repository and replicas, except Recovery Points that are still Immutable, which are deleted when their immutability period ends, and data FirstNet must keep by law.

## 9. Fees, licences and changes

9.1 The MRC and NRC are stated in the Service Schedule. This document states no prices.

9.2 Usage. Depending on the Service Schedule, the MRC is calculated per Protected Workload (Veeam licences), per unit of Repository or Vault storage consumed after compression, and per unit of reserved DR capacity (vCPU, memory, replica storage). Storage consumption depends on retention, immutability, change rate and GFS settings, and is measured as stated in the Service Schedule. Restore, transaction or early-deletion charges that Veeam applies to the selected Vault edition are passed through as stated in the Service Schedule.

9.3 Track 1 licence counts. FirstNet reports Track 1 licence use to Veeam monthly. The Customer must not protect more workloads than it has ordered; additional workloads detected are billed from the month they were first protected.

9.4 Vendor price changes. Veeam and Vault pricing is linked to US dollars. Veeam price increases are passed on under clause 9.5 of the Agreement, and exchange-rate movements under clause 9.6 of the Agreement where the Service Schedule links the Charge to a foreign currency.

9.5 Annual escalation of the MRC applies under the Agreement.

## 10. Term, cancellation and early termination

10.1 Each Service Schedule runs for the Initial Period stated in it from the Service Commencement Date, and then continues month to month until either party gives at least 30 (thirty) calendar days' written notice, or 90 (ninety) calendar days' written notice where the Service Schedule states that an upstream provider requires that period.

10.2 If the Customer ends a Service Schedule before the end of its Initial Period (other than for FirstNet's breach), the early termination charges in the Agreement apply. In addition, any Vault capacity or term that FirstNet committed to Veeam for the Customer, and any minimum storage period charges under the Vault terms, remain payable to the extent FirstNet cannot cancel them without cost and they are not already included in that early termination charge. The same months are not charged twice.

10.3 Where the Customer is a Consumer, it may cancel on 20 Business Days' notice and FirstNet may charge only a reasonable cancellation penalty under section 14 of the CPA and regulation 5, as set out in the Agreement. FirstNet applies the same reasonable cancellation penalty to a Small Business Customer (clause 19.3 of the Standard Terms and Conditions).

## 11. Suspension

11.1 FirstNet may suspend the Service as allowed by the Agreement (non-payment after notice, breach of the Acceptable Use Policy or Vendor Terms, security risk, or a legal order).

11.2 During a suspension for non-payment, FirstNet will not delete Recovery Points while the Service is suspended, but may stop accepting new Backup Jobs and replication and may restrict restores. Veeam may move the Vault to a read-only state if amounts due to it are unpaid.

## 12. Liability specifics

12.1 FirstNet's liability is limited as set out in the Agreement. In addition, FirstNet is not liable for:

12.1.1 data that was not included in a Protected Workload, was excluded from a Backup Job by the Customer, changed after the last successful Recovery Point, or is older than the retention the Customer selected;

12.1.2 loss caused by a Backup Job or replication failure that FirstNet notified to the Customer (in the self-managed model or under Platform-Only DRaaS) and the Customer did not resolve;

12.1.3 inability to decrypt data where the Customer lost its encryption password;

12.1.4 failure to meet an RPO or RTO that the Service Schedule does not record as a committed service level; or

12.1.5 corruption or malware that existed in the source data when it was backed up.

12.2 Nothing in this clause limits liability for FirstNet's gross negligence, fraud or wilful misconduct, or liability that cannot be limited under the CPA.

## 13. Regulatory notes

13.1 The Customer is responsible for deciding how long it must keep records under laws that apply to it (for example the Companies Act 71 of 2008, tax legislation and sector rules). Retention in the Service is a technical setting and does not on its own make the Customer compliant with those laws.

13.2 FirstNet must comply with lawful requests and directions under RICA, the Cybercrimes Act 19 of 2020 and the Criminal Procedure Act 51 of 1977, including preservation directions. Where the law allows, FirstNet will tell the Customer about a request for its data.

## 14. Changes to these terms

14.1 FirstNet may update these SST for changes in law, a regulator's requirement, Vendor changes (including Veeam editions, licensing and Vault terms) or security requirements, or to clarify them, by publishing a new version at www.firstnet.co.za/legal-notices/. FirstNet will give at least 30 days' notice of material changes that are adverse to the Customer.

Backup and Disaster Recovery | Version v2026.10c | Effective date: 1 November 2026

Published by FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07), 26 Augrabies Road, Waterfall Office Park, Midrand, 1686 | 0861 989 896 | support@firstnet.co.za

Published by FirstNet Technology Services (Pty) Ltd, registration number 2006/031608/07. Backup and Disaster Recovery, v2026.10d. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.