



PRODUCT SPECIFIC TERMS – MANAGED FIREWALL

This document is concluded under the terms of the Master Services Agreement between CipherWave and the Customer, and these terms and the Master Services Agreement shall be read as one agreement.

Capitalised terms not defined herein have the same meaning as defined in the CipherWave Master Services Agreement.

Unless the Customer has entered into a reseller agreement with CipherWave, resale of the Service is not permitted.

1. Definition and Product Description

- 1.1. "Firewall System" shall mean any and all hardware, software, equipment, and related components, whether physical or virtual, that are supplied, configured, operated, maintained, and/or managed by CipherWave pursuant to and in accordance with the applicable Service Order;
- 1.2. "Service" means managed firewall, a managed service for Internet access customers comprising the provision of firewall configuration, administration, monitoring, support and use of a Firewall System owned, maintained and supported by CipherWave or where applicable, owned by Customer and maintained and supported by CipherWave.

2. Term

- 2.1. This Service shall commence on the Service Activation Date and shall endure for the Initial Period set out in the Service Order.

Cancellations:

- 2.2. Upon expiration of the Initial Term, the Customer may terminate the Services, or any part thereof, on 1 (one) calendar month's written notice to CipherWave. The second to last business day of the month is the final date for a cancellation notice to qualify as a full calendar month.
- 2.3. The Customer must send a cancellation request to cancellations@cipherwave.co.za.
- 2.4. Customer shall remain liable for any Charges raised by CipherWave against the Customer's account after the Customer has sent CipherWave a cancellation notice that is not processed in the manner set out herein.

3. Accuracy of Customer Information

- 3.1. Customer accepts that it is Customer's responsibility to provide all information reasonably requested by CipherWave in respect of the Service, and that all information provided is complete, accurate and kept up-to date.
- 3.2. CipherWave shall not be liable for any loss suffered because of the Customer's failure to provide accurate information or any relevant facilities, which may lead to a delay in installation or service repair.

4. Workshop

During the installation of the Service, CipherWave shall conduct a workshop with Customer to ascertain Customer's specific requirements regarding firewall rules.

5. Installation Requirements

- 5.1. The Firewall System must be located on the same local area network (LAN) segment as the edge router and/or switch.

- 5.2. Subject to clause 7.3 below, the Service is considered available if data can pass through the Firewall System. If one data protocol cannot pass whilst others can, the Firewall System is available. If the connection is not available whereas the Firewall System is able to pass data, the Firewall System is available.

6. Configuration Submission

CipherWave will configure the Service in accordance with Customer's configuration requirements as determined in the workshop with the Customer.

7. Service Activation Date

- 7.1. Billing will commence as of the Service Activation Date.
- 7.2. Unless otherwise agreed in writing, Customer will be required to connect the Firewall System to Customer's network and to a suitable power supply, as directed by CipherWave.
- 7.3. CipherWave reserves the right to commence billing the Customer if, without consent from CipherWave, the Customer fails to connect the Firewall System or has not arranged an agreed activation date within two (2) weeks of delivery of the Firewall System to the Customer.

8. Administration

After installation Customer may request CipherWave to administer the Firewall System (e.g., add or delete user accounts, modify firewall rules, update network configuration) by sending a request to support@CipherWave.co.za or via telephone at 0860 070 070.

9. Reports

For Firewall Systems that support reporting functions, CipherWave will make available such usage reports to Customer.

10. Configuration Backups

CipherWave will maintain backups of Customer's Firewall System configuration and regularly store such backups at a secure remote location.

11. Support and Maintenance.

- 11.1. CipherWave will remotely install Firewall System patches, bug fixes, and software upgrades when approved by CipherWave for general distribution to CipherWave Customers of the Service.
- 11.2. In the event of a Firewall System failure, CipherWave will either replace the Firewall System (or component), or at CipherWave's sole discretion, CipherWave will dispatch a technician to repair the Firewall System at Customer's Site.

12. Customer Service and Support

- 12.1. Unless agreed otherwise in writing, technical support is provided during business hours on Business Days.
- 12.2. For security reasons only a registered Technical Point of Contact ("TPOC") can raise a support query or request changes to any aspect of the Service.
- 12.3. Telephone calls must be logged with the call centre on 0860 070 070 during business hours on Business Days. After hour tickets can be logged by sending an email to support@CipherWave.co.za.

- 12.4. For configuration change requests, review of open support and change tickets and non-critical support queries contact should be made by sending a request to support@CipherWave.co.za.

13. Customer Obligations

- 13.1. Customer is responsible for confirming that the Firewall System is configured in accordance with Customer's preferences prior to and after the Service Activation Date.
- 13.2. Customer shall comply with all obligations set forth herein, including all obligations set forth in any end user software licenses for software provided by CipherWave or provided by third parties.
- 13.3. Firewall System components are manufactured by third parties (each a "Manufacturer"). Third party agreements (and/or licenses) shall be provided with the applicable products and services. Customer acknowledges that it is not relying on any representations or warranties made by a Manufacturer except for those warranties expressly made in a third-party agreement (and/or license) as applicable to Customer.
- 13.4. Customer shall ensure that the Firewall System provided to Customer's Site as part of this Service is adequately insured for the full replacement value thereof against theft and damage.
- 13.5. Unless otherwise agreed, Customer accepts that it is Customer's sole responsibility to connect the supplied Firewall System to Customer's network and to a suitable power supply.
- 13.6. CipherWave will accept and discuss Customer information only with the registered TPOC. Customer is responsible for ensuring that CipherWave is kept informed of any changes to the TPOC.
- 13.7. Customer must gain CipherWave's prior written approval before relocating a Firewall System.
- 13.8. If the Firewall System is faulty and needs to be returned to CipherWave, it is the Customer's responsibility to package the equipment in its original packing and to return to CipherWave taking out appropriate shipping insurance if required.
- 13.9. If the Customer has purchased the Firewall System from CipherWave (or any other supplier), then Customer acknowledges that CipherWave shall not, unless otherwise agreed in writing, carry spare stock and it shall be the Customer's responsibility to retain spare stock to ensure the speediest fault resolution. If the Customer elects not to carry spare stock and there is a delay in time to procure and install a new Firewall System for the Customer, the Customer shall nonetheless remain liable to pay the Charges of CipherWave, regardless of any reasonable delay in procuring and installing a new Firewall System.

14. Disclaimer

- 14.1. **The Service and the Firewall System are provided without warranty.**
- 14.2. **CipherWave's entire liability and Customer's sole and exclusive remedies regarding the Service and the Firewall System are to have CipherWave repair or replace any CipherWave provided Firewall System if it is defective.**
- 14.3. **Customer acknowledges and agrees that:**
 - 14.3.1. **the Service and the Firewall System constitute only one component of Customer's overall security program and are not a comprehensive security solution;**
 - 14.3.2. **there is no warranty that the Service or the Firewall System will be uninterrupted or error-free, that networks or systems connected to the Firewall System or supported by the Service will be secure or that the Service will meet Customer's requirements;**
 - 14.3.3. **there is no warranty that any communications sent by means of the Service or the Firewall System will be private;**
 - 14.3.4. **there is no warranty that any available content or URL blocking software will block all sites not desired by Customer or that such software will not block any sites that are desired by Customer;**
and
 - 14.3.5. **any available content or URL blocking software is used at Customer's sole risk and discretion.**

15. Acceptable Use Policy

Use of the Service shall at all times be subject to the CipherWave AUP, which may be located at <https://CipherWave.co.za/acceptable-use-policy/>.