

MYSECURE CLOUD FIREWALL – SPECIFIC TERMS AND CONDITIONS including Fortinet Terms of Use

The MySecure Cloud Firewall Specific Terms and Conditions set out the basis in which MyRepublic will provide this specific Service to you.

1. Service Description

1.1. MyRepublic cloud firewall services are available in two categories:

1.1.1. Standard Firewalls are a predefined firewall solution, including policy and configuration. The service is preconfigured to meet the customer’s business requirements; and

1.1.2. Advanced Firewalls offer a customizable solution which allows the agency’s technical staff to maintain an active role in the administration of the perimeter firewall

1.2. MyRepublic Responsibilities

1.2.1. The Service will be available 24-hours, 7-days-a-week.

1.2.2. Management and configuration access are granted by MyRepublic to authorized personnel.

1.2.3. Provide customer-specific access lists and firewall rules.

1.2.4. MyRepublic will secure the platform against known security risks. Any observed security breaches or suspicious activity will be reported to the Customer.

1.2.5. Comply with all applicable Singapore cybersecurity laws and regulations.

1.3. Customer Responsibilities

1.3.1. Customer agrees to comply with all applicable Singapore cybersecurity laws and regulations.

1.3.2. Customer agrees that Customer shall utilize the Service to engage only authorized servers and networks. Any attempt to utilize the Service to access unauthorized servers or networks is strictly prohibited and may result in the termination of Services.

1.3.3. If requested by MyRepublic, the Customer will designate at least one primary and one back up technical resource (the “Customer Firewall Technical Contact”) authorized to execute the following responsibilities:

1.3.3.1. to submit Firewall Service requests to set up, change or remove access control lists and firewall rules for their agency by submitting a request to the MyRepublic Support Centre;

1.3.3.2. to be the “authorized personnel” for administration of the agency’s perimeter firewall by agency staff in a delegated administration model;
to report all Firewall Service problems to the MyRepublic Help Desk Support;

2. Security

2.1. Customer agrees to provide MyRepublic with their the network architecture in order to provide the Service, including any and all changes to the architecture that could compromise the security of the Service.

- 2.2. Customer accepts sole accountability for all use of the Service by Customer's systems and users. Customer further agrees to assume full responsibility for restricting access to specific servers by policy, rules, filters and/or other reasonable methods including agreements with contractors or other third parties. In so doing, Customer agrees to comply with all applicable Singapore cybersecurity laws and regulations and shall ensure that each and every Contractor or third party complies with all the conditions set forth herein as well as the applicable Singapore cybersecurity laws and regulations.
- 2.3. Customer acknowledges and accepts that in accordance to the prevailing applicable Singapore cybersecurity laws and regulations, the Singapore regulators or government bodies may audit and/or inspect remote clients and/or servers accessed via the Service without any advance notice.
- 2.4. Customer acknowledges and accepts MyRepublic' right to suspend service without prior notice upon detection, confirmation, or notification of any unauthorized access, malicious traffic caused by infection or abuse deemed harmful. If unauthorized access, malicious traffic caused by infection or abuse occurs, MyRepublic and customer will attempt to resolve security issues to the satisfaction of MyRepublic and customer. If no satisfactory resolution of security issues is identified, MyRepublic reserves the right to terminate this Firewall Service to the Customer.
- 2.5. MyRepublic provides a security system infrastructure that reasonably protect its Customers from unauthorized external access to or broadcast on the Internet of the customer's intellectual property, proprietary and confidential data. In the event that MyRepublic becomes aware of a breach of the security of the system involving personal information maintained, but not owned by MyRepublic, MyRepublic shall immediately notify the agency that owns the information. Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Personal information, may include but is not limited to, a person's first name or first initial and last name plus any of the following:

3. **Firewall Disclaimer**

- 3.1. This Service is designed to prevent outsiders from gaining access and will provide an effective method of monitoring and limiting access. However, it may not prevent some instances of dedicated hackers, or an employee from gaining unauthorized access to the Internet or to confidential information stored on the network. MyRepublic does not and will not accept liability for any losses or damage to Customer's business or data that arise as a result of the Firewall not preventing unauthorized access.

4. **Exclusions**

- 4.1. MyRepublic does not support the following services. The following items are the sole responsibility of the Customer:
 - 4.1.1. implementation and management of Customer LAN environment (i.e., firewalls, hubs, servers, workstations, etc.);
 - 4.1.2. help desk support for client devices and applications;
 - 4.1.3. remote client internet access;
 - 4.1.4. data encryption; and
 - 4.1.5. protocols other than IP (Internet Protocol).

5. **Fortinet Terms**

- 5.1. MyRepublic is providing this service to you based on a licenced product we have from Fortinet. Accordingly, the Customer acknowledges and accepts the following special terms and conditions imposed by Fortinet:
- 5.1.1. Limitation on Use. You may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Firewall Service; (b) rent or lease any rights in the Firewall Service in any form to any third party or make the Firewall Service available or accessible to third parties in any other manner.
- 5.1.2. Proprietary Rights. All rights, title, interest, and all copyrights to the Firewall Service and any copy made thereof by you and to any Service remain with Fortinet or MyRepublic. You acknowledge that no title to the intellectual property in the Fortinet or other MyRepublic product or Service is transferred to you and you will not acquire any rights to the Firewall Service or other product unless expressly granted an intellectual property transfer agreement.
- 5.1.3. Term and Termination. Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement or in the ordering documents, the term of the licence granted by MyRepublic shall be subject to the term agreement we have with Fortinet. MyRepublic may terminate this licence and the other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions set out herein. You agree that, upon such termination, you will cease using the Firewall Service and any product and either destroy all copies of the Fortinet documentation or return all materials to MyRepublic. The provisions shall survive termination.
- 5.1.4. TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET, THROUGH ITS CONTRACT WITH MYREPUBLIC, IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
6. **Revision**
- 6.1. MyRepublic reserves the right to change, amend or revise this Specific Terms and Conditions. The revised Specific Terms and Conditions shall become effective once posted on the MyRepublic website.

Last updated and effective as on 15 April 2019.