Liquid Telecommunications South Africa (Pty) Ltd
401 Old Pretoria Main Road
Halfway House, Midrand 1685
South Africa

T +27 11 585 0000

MANAGED UTM
SERVICE SCHEDULE

1 APPLICABILITY

This Service Schedule is applicable only to the COF for the purchase of Managed UTM Services, to the extent selected in the relevant COF, which has been signed by the Customer and Liquid Telecom.

2 DEFINITIONS

2.1 Terms used herein but not otherwise defined shall have the meanings ascribed to them in the agreement.

2.2 For the purposes of this schedule, the following expressions shall have the meanings given to them hereunder:

2.2.1 "**Customer Equipment**" means all equipment or wiring including but not limited to cabling or other tangible items owned, leased or otherwise under the control of the Customer;

2.2.2 "**Customer Environment**" means the Customer controlled server/s, workstation/s and/or network that is protected by the Managed UTM Device/s in accordance with the Security Policy;

2.2.3 "**Customer Portal**" means the specific online web interface for Managed UTM Service Customers to access information and place requests;

2.2.4 "**Emergency Policy Change Request**" means a Security Policy Change Request that is qualified as such by the Customer in accordance with the number of Emergency Policy Change Requests permitted under the level of Service selected;

2.2.5 "**Firewall**" refers to the physical and/or logical device/s in conjunction with the implemented rule set employed to protect the Customer Environment from external network borne threats.

2.2.6 "**Internet Emergency**" means an incident has affected a significant portion of the Liquid Telecom Network, or the public internet. Such emergencies are declared through the SSOC;

2.2.7 "**Intrusion Detection**" refers to pre-emptive monitoring of network traffic to identify potential threats and "**Intrusion Detection System**" or "**IDS**" shall have the cognate meaning of a system capable of performing Intrusion Detection;

2.2.8 "**IP**" means 'Internet Protocol', which means the method or protocol by which data is sent from one computer to another over the Internet;

2.2.9 "**Managed UTM Device/s**" refers to the physical and/or logical device/s in conjunction with the implemented rule set employed to protect the Customer Environment from external network borne threats, with the added capability to scan for malicious or unwanted web and/or email content and are identified as such by the relevant IP address;

2.2.10 "**Planned Maintenance**" means any preventative, routine or scheduled maintenance which is performed with regard to the Services, the Network, the off-net network, or any of Liquid Telecom or its partners' hardware or software necessary for the provision of the Services, which Liquid Telecom or its agents reasonably believe is necessary in order to prevent or remedy a defect which may affect the Customer's use or access to the Services;

2.2.11 "**Policy Change Request**" means any request for the addition or modification of 1 rule-based Security Policy item with 5 or less IP address changes within the Customer Environment by a Liquid Telecom Security Analyst within a single request submission. Any change request that requires the addition of 6 or more network or IP entries, or the manipulation of 2 or more Security Policy items would be counted as 2 or more Policy Change Requests;

2.2.12 "**Security Incident**" means an external network borne threat and/or event that has the potential to affect the Customer Environment;

2.2.13 "**Security Platform**" means the combination of Firewalls, Managed UTM Devices and/or associated services employed to filter specific network traffic in line with the Security Policy;

2.2.14 "**Security Policy**" means the set of rules defined by the Customer that describes the acceptable and/or unacceptable network traffic that the Firewalls and/or Managed UTM Devices are required to filter;

2.2.15 "**Severity 1 Incident**" means a high-risk Security Incident that has the potential to cause severe damage to the Customer Environment. Investigations that result in classification to this category require the Customer to take immediate defensive actions – including instructing Liquid Telecom to make the necessary changes on the Firewall and/or Managed UTM Device/s. System Compromises, worm infections, and Denial of Service (DOS) attacks are grouped into this classification;

2.2.16 "**Severity 2 Incident**" means a Security Incident which requires the Customer to take action within 12-24 hours of notification from the SSOC. Incidents such as unauthorized local scanning activity, unverifiable security events (e.g. security events with unknown impact), and attacks targeted at specific servers or workstations are grouped into this category;

2.2.17 "**Severity 3 Incident**" means a Security Incident that encompasses activity on a network or server that is not directly actionable. Discovery and vulnerability scanning, information gathering scripts, and other reconnaissance probes are grouped into this category;

2.2.18 "**Service Credits**" means the credits due to the Customer for unscheduled Service Downtime calculated in accordance with clause 5;

2.2.19 "**Service Downtime**" means that period of time for which the Service was unavailable to the Customer;

2.2.20 "**SIEM**" means security information and event management, which is a term for software products and services that provides analysis of security alerts generated by the Managed UTM Devices.

2.2.21 "**SSL**" means 'Secure Socket Layer which refers to a security standard used for establishing an encrypted link between two elements;

2.2.22 "**SSOC**" means the Liquid Telecom Security Services Operations Centre, from where centralised monitoring, configuration and management of all Managed UTM Devices take place;

2.2.23 "**System Compromise**" means an event which results in unauthorized access, loss, disruption, or destruction of information resources within the Customer Environment where malicious intent is identified;

2.2.24 "**Third Party Product(s)**" means any software and/or hardware which are supplied to the Customer under this Service but which are not manufactured and/or produced by Liquid Telecom. Third Party Products may include hardware, software and other related products;

2.2.25 "**VPN**" means Virtual Private Network where encryption and specific network protocols are used to create a private network connection across a public network; and

2.2.26 "**Working Hours**" is defined as the period from 06h00 to 18h00 on Business Days.

3 SERVICE DESCRIPTION

3.1 For purposes of this Service Schedule, the term "Services" or "Managed UTM Services" means the following services to the extent selected in the relevant COF:

3.1.1 Procurement, supply and installation of Managed UTM Devices at the specified Customer Site/s within the borders of South Africa as well as basic configuration of the Managed UTM Devices

Features included in the Services	Basic Firewall Service	Basic Firewall + IDS	Full Unified Threat Management Services		
			Standard Level	Select Level	Premium Level
Device					
Supply and installation.	Yes	Yes	Yes	Yes	Yes
Base Configuration	Yes	Yes	Yes	Yes	Yes
Maintenance	Yes	Yes	Yes	Yes	Yes
Security Policy Changes					
Number of Policy Change Requests Per Month	1	10	5	10	20
Number of Emergency Policy Change Requests per Month	0	0	0	0	1
Maintenance Window for Policy/Configuration Changes	Yes	Yes	No	Yes	Yes
Functionality					
Firewall	Yes	Yes	Yes	Yes	Yes
Intrusion Detection	No	Yes	Yes	Yes	Yes
Site-to-site VPN Support	No	Unlimited	Up to 2 tunnels	Unlimited	Unlimited
Customer / SSL VPN support	No	Yes	No	Yes	Yes
Monthly Vulnerability Assessment	No	2 IPs	1 IP	2 IPs	3 IPs
Portal					
Customer Portal Access	No	Yes	Yes (Only for viewing Tickets)	Yes	Yes
Detailed Reporting	No	Yes, via Customer Portal	No	Yes, via Customer Portal	Yes, via Customer Portal
Extended Log Archival	No	Up to 1 year	No	Up to 1 year	Up to 2 years
Device Management	Yes	Yes	Yes	Yes	Yes
Health and Availability Monitoring	Yes	Yes	Yes	Yes	Yes
Application/Operating System Upgrades	Yes	Yes	Yes	Yes	Yes
SIEM					

Vulnerability Assessment	No	Additional Option only with IPS	No	Additional Option only with IPS	Additional Option
Intrusion Detection	No	Additional Option	No	Additional Option	Additional Option
Additional Services					
High Availability	Optional	Optional	Optional	Optional	Optional
IDS Services	No	Included			

3.1.1.1 to enable Liquid Telecom and its partners to manage the relevant device; and

3.1.1.2 in accordance with the rule-base supplied by the Customer.

3.1.2 Remote monitoring the Managed UTM Device for performance and malicious potential attacks.

3.1.3 Making changes to the Security Policy.

3.1.4 Service Functionality, including:

3.1.4.1 Firewall – monitoring and controlling of inbound and outbound network traffic based on the Security Policy.

3.1.4.2 Intrusion Detection System - assessing system vulnerabilities against known malicious attacks;

3.1.4.3 VPN Support - setting up of site-to-site and Customer-to-site virtual private network connections as requested by the Customer;

3.1.4.4 Vulnerability Assessment Services - the utilisation of various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities.

3.2 Liquid Telecom may use any Affiliate and/or 3rd party provider/s to deliver the Managed UTM Service to the Customer.

3.3 To enable Liquid Telecom to deliver the Service to the Customer, the Customer shall be responsible for the following:

	Customer Scope of Work
3.3.1	***The Customer will create the Security Policy (in terms of rule base, logging, configuration best practices) for its enterprise and pass it to Liquid Telecom for implementation.***
3.3.2	***The Customer is responsible for installation, configuration and troubleshooting of all additional software, agents, hardware required during Service provisioning and day-to-day operations other than SSOC Managed UTM Devices.***
3.3.3	***The Customer is responsible for keeping all support and maintenance contracts current for the Customer Equipment.***
3.3.4	***The Customer will manage the LAN environment and provide all the IP addressing scheme, subnets required to be configured on the Managed UTM Device.***
3.3.5	***The Customer needs to provide continuous access to the Managed UTM Device during provisioning. In the event of provisioning engineer not being given continuous access to the device, Liquid Telecom will not be responsible for delay in project delivery.***
3.3.6	***The Customer shall ensure that all the Managed UTM Devices under the scope of Managed UTM Services are reachable by Liquid Telecom through the Internet for management, monitoring and log collection. The connectivity from the SSOC to the Customer site will be provided by using a site to site Virtual Private Network over the Internet link.***
3.3.7	***Dedicated switches with the required number of switch ports per zone are required for connection to the Firewall/s in a high availability configuration. Static public IP address, patch cables and related infrastructure for connection of the Firewall/s is required to be provided.***
3.3.8	***Where the Firewall and/or Managed UTM Device is Customer Equipment that is managed by any other entity than Liquid Telecom, the applicable Customer Equipment may from time it time require a reinstallation of the applications/firmware, and overall configuration changes. The Customer is responsible for keeping all support and maintenance contracts/licenses current for the hardware and Customer Equipment. The Customer is required to ensure all default system user accounts and passwords have been reset to provide Liquid Telecom access to the system.***
3.3.9	***The Customer undertakes to comply with the terms and conditions of the licences applicable to the hardware, firmware, software or any other feature installed and/or running on the Firewalls and/or the Managed UTM Devices and which are utilised by Liquid Telecom to provide the Services.***
3.3.10	***The Customer hereby permits Liquid Telecom and/or any hardware or software provider of Liquid Telecom access to the Firewalls and/or the Managed UTM Devices in order to conduct random compliance audits. The Customer agrees to fully cooperate with the applicable auditors to ensure that the audits can be completed successfully, including but not limited to providing supervised access to Customer servers.***

4 SERVICE LEVELS

4.1 Liquid Telecom will provide Managed UTM Services in accordance with the Service Level(s) applicable to the type of Services ordered by the Customer. If a Service Level does not expressly provide Service Credits for a Service, then no service level commitments apply for that Service.

4.2 If the Customer is entitled to receive Service Credits on more than one Service due to the same service-affecting incident, then the Customer will receive the relevant Service Credits for each of the applicable Service Level(s). For all applicable Service Levels, the Customer may obtain no more than one Service Credit for each applicable Service Level per day. If the Customer is entitled to receive Service Credits on more than one element under a Service Level due to the same Service-affecting incident, the Customer will only receive the largest possible Service Credit that it would otherwise be entitled to receive under a single guaranteed criterion.

4.3 Service Levels shall not apply until the applicable Managed UTM Device has been designated 'live' by Liquid Telecom, and that Managed UTM Device has been successfully transitioned to 24 x 7 management within the SSOC which date shall be the date of the applicable Service Handover Form.

4.4 The Customer is solely responsible for providing Liquid Telecom with accurate and current contact information for the designated Security Contact(s). The current contact information on record is available to authorised contacts through the Customer Portal. Liquid Telecom will be relieved of its obligations for any notification to the Customer if the Customer's contact information is out of date or inaccurate due to his failure to update as necessary.

4.5 The Customer is responsible for providing Liquid Telecom advance notice regarding any changes to the Customer Environment. In the event advance notice cannot be provided, the Customer is required to provide Liquid Telecom with notification of changes within seven (7) calendar days of said changes. Notification is completed by the submission or update of a critical server ticket via the Customer Portal. If the Customer fails to notify Liquid Telecom as stated above, all service level remedies shall be null and void.

4.6 Service Levels and associated remedies for the Services are based on fully functional security platforms and properly configured Managed UTM Devices. If non-compliance with the service level assurances set forth in the applicable Service Levels is attributable to non-Liquid Telecom managed Customer Equipment, hardware and/or software failure, or Third Party Products, all remedies shall be considered null and void. None of the stated service level assurances shall apply to any System Compromises initiated by the Customer, its employees, its agents or sub-contractors.

4.7 The following table sets out the service levels for the Managed UTM Services:

Service Level	Standard Service	Select Service	Premium Service
Policy Change Request Acknowledgement	√	√	√
Policy Change Request Implementation	√	√	√
Emergency Change Request Implementation			√
Security Incident Identification			√
Security Incident Response			√
Proactive System Monitoring	√	√	√
Customer Portal	√	√	√
Internet Emergency Guarantee			√

4.8 Policy Change Requests

4.8.1 The Policy Change Request service levels are only available for Policy Change Requests submitted by a valid Security Contact in accordance with the Liquid Telecom Policy Change Request Submission Procedures available on the Customer Portal. Liquid Telecom will acknowledge a Policy Change Request or notify the Customer upon implementation of a Policy Change Request by a method elected by Liquid Telecom (i.e. telephone, email, fax, or electronic response via the Customer Portal).

4.8.2 The Policy Change Request Acknowledgement service level is to acknowledge receipt of the Customer's Policy Change Request within four (4) Working Hours of Liquid Telecom's receipt thereof in writing.

4.8.3 The Policy Change Request Implementation service level is to implement Customer Policy Change Requests within the time specified below and commensurate with the applicable service level. This service level is based on actual time taken to implement, and not on the time that the Customer was notified of the completion of the request:

4.8.3.1 Standard Service Levels: Liquid Telecom will implement Customer's Policy Change Requests within thirty six (36) Working Hours of Liquid Telecom's receipt thereof in writing, unless the request has been placed on a "hold" status due to insufficient information required to implement the submitted Policy Change Request.

4.8.3.2 Select/Premium Service Levels: Liquid Telecom will implement Customer's Policy Change Requests within twelve (12) Working Hours of Liquid Telecom's receipt thereof in writing, unless the request has been placed on a "hold" status due to insufficient information required to implement the submitted Policy Change Request.

4.9 Emergency Policy Change Request Implementation:

4.9.1 This service level applies to Premium Service Level Managed UTM Service only.

4.9.2 Liquid Telecom's Emergency Policy Change Request Implementation service level is to implement Emergency Policy Change Requests within four (4) Working Hours of Customer's telephonic declaration of emergency following change request submission via the Customer Portal.

4.9.3 This guarantee is based on actual time taken to implement, and not on the time that the Customer was notified of the completion of the request.

4.10 Security Incident Identification:

4.10.1 This service level applies to Premium Service Level Managed UTM Services.

4.10.2 Liquid Telecom's Security Incident Identification service level is that Liquid Telecom will identify all Severity 1, 2, and 3 level Security Incidents based on security agent event data received by the SSOC.

4.10.3 Under this service level, Liquid Telecom will determine whether or not an event is a Security Incident based on the Customer's business requirements, network configuration, and security agent configuration.

4.11 Security Incident Response:

4.11.1 This service level applies to Premium Service Level Managed UTM Services only.

4.11.2 Liquid Telecom undertakes to respond to all identified Security Incidents within forty-five (45) minutes of determination thereof by Liquid Telecom as a Security Incident.

4.11.3 Under this service level, Liquid Telecom will contact the Customer's Security Contact(s) by telephone for Severity 1 Incidents and via email for Severity 2 and 3 Incidents. During a Severity 1 Incident escalation, Liquid Telecom will continue attempting to contact the Security Contact(s) until a contact is reached or all escalation contacts have been exhausted.

4.11.4 Operational activities related to incidents and responses are documented and time-stamped within Liquid Telecom's trouble ticketing system, which shall be used as the sole authoritative information source for purposes of this service level.

4.12 Proactive System Monitoring:

4.12.1 Liquid Telecom's Proactive System Monitoring service level is that Liquid Telecom will notify the Customer within the time specified below and commensurate with the applicable service level:

4.12.1.1 Managed UTM Standard Service Level: Liquid Telecom will notify the Customer's Security Contact(s) within one (1) hour after Liquid Telecom determines that the Customer's managed network Firewall is unreachable via standard in-band connectivity for 15 consecutive minutes or longer.

4.12.1.2 Managed UTM Select/Premium Service Levels: Liquid Telecom will notify the Customer's Security Contact(s) within thirty (30) minutes after Liquid Telecom determines that the Customer's managed network Firewall is unreachable via standard in-band connectivity for 15 consecutive minutes or longer.

4.12.2 Liquid Telecom will use reasonable efforts to provide a 99.9% accessibility service level for the Customer Portal. Liquid Telecom shall not be liable for any failure to meet this service level and no Service Credits apply to this service level.

4.13 Internet Emergency:

4.13.1 This service level applies to Premium Level Managed UTM Service and IPS Service.

4.13.2 In the event Liquid Telecom declares an Internet Emergency, Liquid Telecom will use reasonable efforts to notify the Customer's Security Contact(s) through email within one (1) hour of emergency declaration. This notification will include an incident tracking number, telephone bridge number and the time that Liquid Telecom will conduct a situation briefing.

4.13.3 During a declared Internet Emergency, Liquid Telecom will provide a live telephone-conference situation briefing and summarized email designed to provide actionable information that the Customer can use to protect their organization. Situation briefings following the onset of an Internet Emergency will supersede any requirement for Liquid Telecom to provide specific escalations to the Customer for events directly related to the declared Internet Emergency. Liquid Telecom will communicate all other severity level incidents during an Internet Emergency via automated systems such as email, and voice mail only.

4.13.4 Standard level escalation practices will resume upon conclusion of the declared Internet Emergency. Termination of an Internet Emergency state is marked by an email notification to Customer's Security Contact(s).

5 SERVICE CREDITS

5.1 The following table sets out the Service Credits for Managed UTM Services.

Service Level	Service Credit
Policy Change Request Acknowledgement	1 day of the MRC for the affected Managed UTM Device.
Policy Change Request Implementation	
Emergency Change Request Implementation	
Security Incident Identification	
Security Incident Response	
Proactive System Monitoring	

6 VULNERABILITY ASSESSMENT SERVICES

Should the relevant COF include vulnerability assessment services, the customer understands and agrees that Liquid Telecom and its partners may use various methods and software tools to access and probe the customer's network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. The customer authorises Liquid Telecom and its partners to perform such vulnerability assessment services on network resources with the IP addresses identified by the customer. The customer shall obtain any necessary authorisation to perform such vulnerability assessment services. Liquid Telecom shall perform security services during a timeframe mutually agreed upon with the customer.

7 OTHER TERMS AND CONDITIONS

7.1 Disclaimers

7.1.1 Liquid Telecom will use commercially reasonable efforts to provide the services; however, Liquid Telecom does not guarantee the security of the Customer's network and/or data and shall have no liability in contract, delict or otherwise for any claim arising from or based on unauthorized access to, or alteration, theft or destruction of the Customer's facilities, equipment and/or data files.

7.1.2 The Customer Portal presents information that is created or generated by the Customer's Managed UTM Devices. Liquid Telecom does not warrant or otherwise guarantee that such information presented or made available on the Customer Portal will be accurate, complete or timely.

7.1.3 Liquid Telecom is not obliged to, but may, from time to time, provide notifications to the Customer that upgrades and/or software patches have been made generally available by the applicable vendor(s). The decision of whether to implement and install any such upgrades and/or patches is the Customer's final decision. Liquid Telecom is not liable for any damage or harm caused by such actions or inaction.

7.1.4 Liquid Telecom shall not be liable for any service failures or delays (including without limitation, delays in provisioning and implementation) resulting from inaccurate or incomplete data or information provided by the Customer.

7.2 Service Limitations

The Services are not warranted to operate uninterrupted or error free. New security threats are constantly evolving and it is not possible for the Service to provide protection from all security threats and vulnerabilities, or to guarantee against unsolicited e-mails and undesirable Internet content. Services are not fault tolerant and are not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which product or Service failure could lead to death, personal injury, or property damage. The Customer acknowledges the Services involve the testing, assessing, scanning or monitoring the security of network resources, including implementation and deployment, which may disclose or create problems in the operation of such resources; therefore, the Customer may experience down time, loss of connectivity or data, system crashes, performance degradation or similar circumstances.

7.3 Third Party Products

The use of Third Party Product(s) supplied hereunder, if any, will be subject solely to the manufacturer's terms and conditions. Liquid Telecom will pass any Third Party Product warranties through to the Customer to the extent Liquid Telecom is authorised to do so. The Customer agrees to indemnify Liquid Telecom against any claims made by third parties with respect to the end customer's misuse of Third Party Product(s) supplied hereunder.

8 EXCHANGE RATE FLUCTUATIONS

8.1 For Charges for any element of the Service that is based on a foreign currency, the exchange rate to be used to determine a variation shall be the South African Rand / US Dollar exchange rate set out in the relevant COF. In the event that the COF does not stipulate the exchange rate, then the exchange rate as downloaded by Liquid Telecom from Reuters on the morning of the date of signature by the Customer of the COF relevant COF shall be used.

8.2 Liquid Telecom shall be entitled to adjust the MRC in question in the event that the variance, when the exchange rate referred to in 8.1 above is compared against the exchange rate as downloaded by Liquid Telecom from Reuters on the morning of the relevant invoice generation date, is greater than 5% (5 percent).

9 EXCLUSIONS

9.1 The Customer shall not be entitled to receive any Service Credits or exercise any right of termination for anything which is caused or is associated with, in whole or in part, the exclusions set out below:

9.1.1 anything which is associated with or caused by Planned Maintenance events or cable cuts on the Network which are not otherwise due to the fault or negligence of Liquid Telecom;

9.1.2 anything which is associated with or caused by interruptions or delays of any other Service procured from Liquid Telecom by the Customer, and as a consequence of such interruption or delay, the Customer is entitled to a service credit from Liquid Telecom; or

9.1.3 anything attributable to circuits comprising a part of the Service that are provided by a third party, including Local Loops and local access facilities procured by the Customer.

9.2 Service Downtime shall not include any unavailability resulting from:

9.2.1 scheduled downtime for Planned Maintenance;

9.2.2 interruptions or delays resulting from any third party services procured by the Customer;

9.2.3 any supplies, power, equipment or local access facilities provided by the Customer or their suppliers, which is required in the provision of the Services;

9.2.4 any incident that affects the availability during any period when the Customer elects not to allow Liquid Telecom to conduct Planned Maintenance on the Service at the request of Liquid Telecom, acting reasonably;

9.2.5 delay or failure by the Customer to perform recommended upgrades or download recommended software patches;

9.2.6 delay or failure by the Customer to provide accurate or complete data or information required by Liquid Telecom to provide the Services;

9.2.7 the Customer's applications, equipment, or facilities;

9.2.8 interruptions due to the failure of equipment provided by the Customer or other third party on behalf of the Customer;

9.2.9 acts or omissions of the Customer, its agents, contractors or vendors (including the provision of inaccurate information knowingly or unknowingly), or user of the Service or Customer-caused outages or disruptions;

9.2.10 suspensions due to non-payment of any amount payable by the Customer to Liquid Telecom under this Schedule; or

9.2.11 force majeure.

9.3 Certain service level guarantees focus on the identification of and response to Security Incidents. These guarantees assume that traffic has successfully reached the Security Platform, and therefore the Managed UTM Device has the ability to process the traffic against the Security Policy and generate a logged event. Traffic that does not logically or electronically pass through a Security Platform, or that does not generate a logged event is not covered under these service levels.

9.4 Where it is necessary to do so in Liquid Telecom's reasonable opinion, Liquid Telecom may take, or may require the Customer to take, proactive measures to adjust the Customer's security agent configuration in the event that there is an excessive amount of IDS data.

10 FAULT REPORTING

10.1 The Customer shall raise an outage trouble ticket with Liquid Telecom in the event of any Service outage detected.

10.2 The logging of calls, queries and/or complaints shall be directed to the Liquid Telecom Enterprise Service Desk using any of the following:

TELEPHONE NO.	E-MAIL
+27 11 585 0652 (outside of South Africa) 080 11 11 636 (within South Africa only)	**EnterpriseService@liquidtelecom.co.za**

10.3 Should a call logged in accordance with clause 10.2 not be handled to the reasonable satisfaction of the Customer, the Customer shall be entitled to direct their concerns to service.management@liquidtelecom.co.za, which is managed during Business Hours.

10.4 In addition, the Customer shall be entitled to approach an assigned Liquid Telecom account manager if the feedback or progress on the outage resolution is not satisfactory.

10.5 Liquid Telecom shall use reasonable endeavours to provide a root cause analysis report regarding the cause of the Service Downtime and the preventive measures put in place in an effort to mitigate a reoccurrence thereof. Liquid Telecom shall use reasonable endeavours to perform the following actions and shall provide the reports (as applicable) detailed in the following table:

FAULT MANAGEMENT AND REPORTING	TIME TARGETS
Assignment of Customer Fault Reporting Trouble Ticket	Within 15 minutes of the notification of fault
Regular problem status update	Daily
Root Cause Analysis Report	< ten (10) business days of request

10.6 In the event that Liquid Telecom attends to a Service fault and/or Service outage ("Fault") reported by the Customer, and Liquid Telecom subsequently establishes that the Fault was not due to any fault on the Liquid Telecom Network and/or Liquid Telecom infrastructure deployed in the delivery of the Service, Liquid Telecom shall have the right to charge the Customer for the time and materials and/or travel costs associated with attending to the Fault at Liquid Telecom's current standard rates and charges at the time of the incident.

11 SERVICE CREDIT REQUEST AND SETTLEMENT PROCEDURES

11.1 To initiate a claim for Service Credits with respect to the parameters defined above, the Customer shall submit a request in writing within thirty days after the end of the month during which the event occurred which gave rise to the claim for Service Credit.

11.2 For purposes of calculating the Service Credit, the problem occurrence will be deemed to have commenced when the trouble ticket is lodged by the Customer with Liquid Telecom. If the Customer does not initiate a trouble ticket with Liquid Telecom, Liquid Telecom shall not be obligated to log a

trouble ticket, and the Customer shall not be eligible to receive Service Credits for the non-compliance.

11.3 The duration of the Service outage will be determined by the Parties, acting reasonably, based upon the Parties' internal records and Liquid Telecom's trouble ticket.

11.4 In no event shall the total amount of all Service Credits issued to the Customer per month exceed twenty five percent (25%) of the MRC invoiced to the Customer for the affected Service for that month.

11.5 Service Credits are calculated after the deduction of all discounts and other special pricing arrangements, and may not be applied to governmental fees, taxes, surcharges, local access charges or any other charges other than MRC.

11.6 Service Credits are processed quarterly and are passed as a credit against the Customer's next invoice. If Liquid Telecom approves the claim, Liquid Telecom shall notify the Customer of the value of Service Credits to which the Customer will be entitled.

11.7 Any Service Credits calculated on the basis of a month shall be calculated with regard to a month being deemed to begin at 00h00 S.A. time on the first day of a calendar month, and ending at 23h59 S.A. time on the last day of the applicable calendar month.

11.8 Liquid Telecom's failure to achieve or maintain the above service objectives set out in this Service Schedule is not a breach of the Agreement, and the award of Service Credits shall be the Customer's sole remedy and Liquid Telecom's sole liability for any such failure or corresponding degradation, interruption or loss of Service.

12 SERVICE PROVISIONING

12.1 The Customer shall be responsible for making available, at no cost to Liquid Telecom, accommodation, power, space, including mast space, ducting and other facilities as may be more fully set out in the CSRS document for each Customer Site, for the Contract Term of the applicable COF, for the purposes of housing Liquid Telecom's equipment required for the provision of the Services to the Customer.

12.2 The Customer shall be responsible for obtaining all third party approvals and consents necessary for the implementation and use of the Services.

12.3 The Customer shall ensure that all necessary Customer controlled server system changes and configurations are completed as may be required by Liquid Telecom to fulfil its obligations in terms hereof.

12.4 Within seventy two (72) hours of completing the implementation for the applicable Service, Liquid Telecom will provide a Service Handover Form containing essential information required to configure and use the Service as well as the Service Identity Number ("Service ID"). The Service ID should be used in all interactions with Liquid Telecom regarding the Service.

12.5 The Customer shall then conduct acceptance tests on the newly provided Service for a period of two (2) Business Days following receipt of the Service Handover Form.

12.6 Should the Customer detect a fault on the Service during these acceptance tests, then the Customer shall notify Liquid Telecom of such fault in writing.

12.7 The Customer may only reject a Service on the basis that the agreed technical specifications as set forth in the Service configuration diagram in the COF for the Service have not been met. If the Customer notifies Liquid Telecom of its non-acceptance, further tests of the Service shall be conducted and a revised Service Handover Form shall be provided to the Customer.

12.8 The Service shall be deemed accepted by the Customer if no objection has been raised by the Customer within two (2) Business Days following receipt of the SHF.

13 CUSTOMER REQUESTED CHANGES AND PLANNED MAINTENANCE

13.1 Liquid Telecom shall use reasonable endeavours to perform any agreed change as per agreed specifications as per the below specified target timelines. The Customer must raise a change request stating the reason for the change, the type of change (Critical/Normal as defined by the Customer) and the impact on its Customer Sites. The change request shall follow the normal change management process as communicated from Liquid Telecom to the Customer from time to time and the below commitments are applicable only for Class C type changes (as defined in the following table) excluding any impact analysis:

LEVEL OF CHANGE	DESCRIPTION OF CHANGES REQUIRED
Class A	• Changes to DNS entries • Changes to email routing • Changes to VPNs • Changes to proxy settings and configuration files
Class B	• Changes to configuration rules • Changes to authentication schemas and systems
Class C	• Changes that are not specified in Class A and Class B.

13.2 The Customer hereby understands and agrees that any change requests mentioned above in Class A and Class B are Service affecting in nature. Hence, the Customer understands and agrees that the Service can be unavailable for a minimum period of two (2) hours during the implementation of any such change requests. The time and date of the Service Downtime shall be discussed between the Parties. In any case, the Service Level targets set out in this Service Schedule shall not be applicable during any such change request implementation and as such, Liquid Telecom cannot be held responsible for any damages or losses which may occur during such implementation time.

13.3 Planned Maintenance which falls outside the scheduled maintenance window will be arranged with the Customer at least forty eight (48) hours before the Planned Maintenance commences.

13.4 Liquid Telecom is not responsible for any breach of rights which may be related to any Customer transmitted or received content that has been carried on the Liquid Telecom Network and the Customer agrees that Liquid Telecom can view the content to identify Service related issues.

14 CONTENT REGULATORY COMPLIANCE

14.1 The Customer hereby agrees that the relevant permissions, approvals, licenses and/or related consents that may be required by the relevant government authority of the source and/or destination country/ies shall be obtained, as applicable, as per the local laws in such country and a copy of such permissions, approvals, licenses and/or related consents shall be available for inspection by Liquid Telecom prior to the commissioning of the Service.

14.2 In the event that the Customer is sourcing content from a third party in relation to the Service, the Customer shall be responsible for providing the permissions, approvals, licenses and/or related consents of such third party. The Customer further indemnifies Liquid Telecom from any costs, damages and/or penalties caused due to any non-compliance with this provision.

14.3 The Customer authorizes Liquid Telecom to monitor the Service at Liquid Telecom's Network Operating Centre and SSOC facilities.

15 SERVICE TERMINATIONS – EARLY TERMINATION COSTS

Section 3.01 Notwithstanding any early termination provisions set out in the agreement, the termination fee for the terminating services which are specified as customer specific services in the relevant COF or where the service either originates from or terminates at an international location shall be calculated as at the termination date and shall be equal to 100% of the MRC for the remainder of the contract term thereof.