ITEC SA (PTY) LTD CYBERSECURITY SERVICES LEVEL AGREEEMENT

– MASTER SERVICES TERMS AND CONDITIONS

These are the Cybersecurity Services Terms and Conditions and shall apply to all Cybersecurity Services Agreements entered into between Itec and the Customer for the Equipment and/or Services as if specifically set out therein. The conclusion of further Cyber Security Services Agreements shall create separate agreements relating to the Equipment and/or Services described therein. Should any Cybersecurity Services Agreements be terminated by any cause whatsoever and howsoever arising, it will not affect the validity of any other existing Cybersecurity Services Agreement. Both Parties will continue to fulfil their obligations in respect thereof and the terms of these Terms and Conditions will remain in force in respect of any existing Cybersecurity Services Agreement. These Terms and Conditions, including the applicable product Schedules thereto, will be read together with the Cybersecurity Services Agreement. In the event of a conflict between the provisions of these Terms and Conditions, the provisions of any Schedule and/or the provisions of any Cybersecurity Services Agreement, the following order of precedence would apply:

a) these Terms and Conditions;
b) the specific Schedule of Equipment and/or Services (and their associated SLA's or Best Effort support) which the Customer has purchased;
c) Cybersecurity Services Agreement(s) and
d) any other documents agreed between the Parties.
e) The Parties agree that in terms of any operational matters, functionality of the Equipment or the associated SLA's or Best Effort support the applicable Schedule will prevail in terms of an associated dispute.

CONTENTS

1. DEFINITIONS

1.1. In these Terms and Conditions –

1.1.1. clause headings are for convenience purposes only and shall not be used in its interpretation;

1.1.2. unless the context clearly indicates a contrary intention –

1.1.3. an expression which denotes any gender includes the other genders, a natural person includes a juristic person and vice versa and the singular includes the plural and vice versa;

1.1.4. where any term is defined within a clause, other than the interpretation clause, that term shall bear the meaning ascribed to it in that clause wherever it is used in these Terms and Conditions;

1.1.5. the following expressions shall bear the following meanings and related expressions shall bear corresponding meanings (all other undefined words, expressions and phrases will have the generally understood meaning in the ICT industry) –

1.1.5.1. "**Activation Date**" means the date on which the Service has been activated and access has been provided to the Customer;

1.1.5.2. "**Applicable Laws**" means any law, regulation, binding code of practice, rule, order, or requirement, including Data Protection Legislation, of any relevant government, professional or regulatory authority which is applicable to either Itec or the Customer's business practises,

1.1.5.3. "**AUP**" means Acceptable Use Policy described in clause 8;

1.1.5.4. "**Charges**" means the delivery charges, installation charges, monthly service charges, usage charges, interest charges and any other charges relating to the provision of the Services by Itec to the Customer payable by the Customer to Itec in terms of these Terms and Conditions, the relevant Schedules and the Cybersecurity Services Agreement, exclusive of VAT and any similar tax or duty payable by the Customer at the then prevailing rate;

1.1.5.5. "**CPE**" or "**Customer Premises Equipment**" means any telecommunications, networking, security, or information technology hardware that is physically located on the Customer's premises and which connects to, interfaces with, or enables access to the service provider's network at the applicable demarcation point.

1.1.5.6. "**Customer**" means the entity identified as Customer in the Cybersecurity Services Agreement;

1.1.5.7. "**CyberHeal**" means endpoint-based automation service identifies outdated applications and automatically initiates update workflows. Priced per endpoint, focused on reducing exposure caused by unpatched or legacy software;

1.1.5.8. "**Cybersecurity**" means the technical and organisational measures implemented to protect information systems, networks, data, and digital assets against unauthorised access, use, disclosure, disruption, modification, or destruction, and to preserve the confidentiality, integrity, and availability of such systems and data;

1.1.5.9. "**Dark Web Monitoring**" means the surveillance of indexed dark web sources to detect the possible exposure of the Client's credentials, data, or identifiers;

1.1.5.10. "**Dark Web Threat & Leakage**" means dark web reconnaissance to identify leaked organizational data, credential dumps, impersonation activities, and marketplace exposure. Offers a concise overview of current underground visibility;

1.1.5.11. "**DMZ**" means a perimeter or buffer network segment situated between the Customer's internal, trusted network and external, untrusted networks, including the Internet. The DMZ hosts public-facing systems or services and provides an additional layer of protection by isolating such systems from the internal network. Access to and from the DMZ is strictly controlled and filtered through firewalls or other approved security gateways to ensure that external users may only access authorised DMZ-based services and cannot directly access the internal network. The DMZ thereby reduces the Customer's exposure to external threats while ensuring that public-facing services remain operational.

1.1.5.12. "**Endpoint Management**" means the coordinated administration, monitoring, and maintenance of authorised endpoint devices to ensure security compliance, software integrity, and operational performance;

1.1.5.13. "**Entry-Level Firewall Support**" means the provision of foundational administrative and operational support for small-scale firewall appliances. This includes basic policy management, standard NAT and VPN configuration, routine firmware updates, and monitoring of device health during Business Hours. Entry-Level Firewall Support is intended to maintain general operational stability;

1.1.5.14. "**Equipment**" means the cybersecurity and network security equipment, whether owned by the Customer or supplied and owned by Itec, that is installed at the Customer's or User's Site for the purpose of enabling or securing access to the Services. This includes, without limitation, any firewalls, security appliances, intrusion-prevention devices, network security hardware, embedded firmware, associated management modules, software components, security licenses, cables, connectors, interfaces, power supplies, mounting hardware, and any other security-related equipment or components embedded in, attached to, or used in conjunction with such Equipment, as further detailed in the applicable Schedules or Cybersecurity Services Agreement;

1.1.5.15. "**Exposure Assessment**" means the evaluation of systems and configurations to identify security gaps or conditions that may expose the environment to increased cyber risk;

1.1.5.16. "**Firewall**" means a network security device, whether hardware or virtual, deployed to monitor, filter, and control incoming and outgoing network traffic based on predefined security policies. A Firewall functions as a protective security layer between trusted and untrusted networks and may include features such as intrusion prevention, web filtering, VPN services, application control, and advanced threat inspection. A Firewall reduces risk but does not guarantee the prevention, detection, or mitigation of all cyber-attacks, security breaches, malware infections, or zero-day threats;

1.1.5.17. "**Firewall Management**" means the configuration, monitoring, and administration of firewall devices to enforce approved security policies and control network traffic;

1.1.5.18. "**Force Majeure Event**" means any event beyond a Party's reasonable control affecting the performance of its obligations in terms of these Terms and Conditions including any Acts of God, such as cloud cover and/or rain, earthquake, solar flares and any other natural phenomenon, fire, flood, extraordinary storm, lightning, and/or the like; civil disorder, war (whether declared or undeclared and including the serious threat of same) or military operations or armed conflict; invasion and acts of foreign enemies; nuclear, chemical or biological contamination; plague; epidemic; pandemic; national or local emergency; riots; sabotage blockages and embargos; commotion or rebellion; acts of terrorism; acts or omissions of government agencies or of other telecommunication service providers; major pro-longed power interruptions, including but not limited to load shedding; strikes, lockouts and industrial disputes of any kind; explosions or any other acts or omissions of persons beyond the reasonable control of the affected Party;

1.1.5.19. "**FUP**" means Fair Use Policy described in clause 9;

1.1.5.20. "**Help Desk**" means the designated Itec Customer Service and Operations Centre;

1.1.5.21. "**High-Level Firewall Support**" means the provision of comprehensive enterprise-grade firewall administration for large

or complex firewall deployments, including high-availability configuration, advanced routing (such as BGP and OSPF), deep inspection tuning, multi-site policy orchestration, and integration support for SIEM/SOAR platforms. Services are delivered during Business Hours only unless otherwise contracted. High-Level Firewall Support improves system resilience and governance but does not guarantee the prevention or detection of cyber-attacks, security breaches, or zero-day threats and does not replace a dedicated 24/7 Security Operations Centre or Managed Detection and Response service;

1.1.5.22. "**ICT industry**" means the information and communication technology industry;

1.1.5.23. "**Organization Exposure Assessment**" means baseline assessment of an organization's external attack surface, identifying exposed services, misconfigurations, outdated technologies, and domain-level security posture. Produces an executive-ready exposure report;

1.1.5.24. "**Parties**" means Itec and the Customer, and "Party" shall mean either one of them;

1.1.5.25. "**Patch Management**" means the process of acquiring, testing, and deploying vendor-released software updates and security patches to supported systems within agreed maintenance windows;

1.1.5.26. "**Mid-Level Firewall Support**" means the provision of intermediate administrative, security, and configuration services for mid-range firewall appliances. This includes advanced policy design, network segmentation, SD-WAN configuration, central management integration (where applicable), enhanced security profile tuning, and Business Hours troubleshooting of more complex network-related issues. Mid-Level Firewall Support enhances the security posture of the environment; however, it does not provide 24/7 threat monitoring, does not guarantee protection from cyber-attacks or breaches, and does not constitute a managed detection and response service;

1.1.5.27. "**Multi-Factor Authentication**" or "**MFA**" means a security control requiring users to verify their identity using two or more independent authentication factors, such as something they know, something they have, or something they are;

1.1.5.28. "**NAT**" or "**Network Address Translation**" means a routing and firewall-based function that translates private IP addresses used within the Customer's internal network into a public IP address for communication with external networks, and vice versa. NAT enables multiple internal devices to share a single public IP address and provides an additional layer of security by obscuring internal network addresses from external parties.

1.1.5.29. "**Network Security Equipment**" means any hardware, appliance, device, or embedded system used to protect, secure, monitor, or control network traffic, access, or communications. This includes, without limitation, firewalls, security gateways, intrusion-prevention devices, secure routers, switches with security functions, and any associated components, firmware, or modules required for the operation of such security equipment;

1.1.5.30. "**OEM**" means the original equipment manufacturer that designs, produces, and supplies the Equipment or Software, and is responsible for issuing the applicable warranties, support terms, and RMA processes;

1.1.5.31. "**RMA Process**" means the manufacturer's formal Return Merchandise Authorisation procedure governing the assessment, approval, return, replacement, or repair of faulty Equipment, including all diagnostic requirements, eligibility criteria, documentation, and timelines prescribed solely by the manufacturer or vendor;

1.1.5.32. "**Services**" means the services, managed or otherwise, and/or the maintenance of Equipment provided by Itec to the Customer governed by these Terms and Conditions and the Schedules as described in the Cybersecurity Agreement;

1.1.5.33. "**Service Levels**" or "**SLA**" means the service level agreement described in the Schedules and the Cybersecurity Services Agreement;

1.1.5.34. "**Software**" means any computer program, cybersecurity application, agent, script, tool, firmware, or other digital material supplied, licensed, installed, or provided by Itec or on its behalf for the purpose of delivering, enabling, securing, operating, monitoring, or managing the Equipment or the Services. This includes, without limitation, any endpoint protection agents, threat-detection modules, security analytics components, management consoles, integration connectors, embedded firmware, configuration files, or any other software used in conjunction with the Equipment and/or any electronic communication, cybersecurity, monitoring, or management system operated, supported, or maintained by Itec;

1.1.5.35. "**Supplier**" means the third-party ICT supplier(s) from whom Itec sources, procures, licenses, or acquires any ICT equipment, software, security technologies, or services required for the provisioning, delivery, or support of the Services to the Customer;

1.1.5.36. "**System Manager/s**" means the Customer's authorised representative responsible for managing and administering the Customer's systems, networks, and security settings, and for serving as the primary contact for all cyber-related and/or technical matters;

1.1.5.37. "**User**" and/or "**Users**" means the individual and/or party who uses the Services provided by Itec to the Customer in accordance with the Cybersecurity Agreement;

1.1.5.38. "**Vendor**" means the authorised supplier, distributor, or provider of the Equipment or Software, including any entity appointed by the OEM to sell, distribute, or support such Equipment or Software in accordance with the OEM's terms, warranties, and RMA processes;

1.1.5.39. **"'VPN"** or **"Virtual Private Network"** means a secure and encrypted communications mechanism that establishes a protected connection ("tunnel") between a user's device and a remote network or server over the Internet. A VPN encrypts data in transit, masks the user's IP address, and prevents unauthorised interception, monitoring, or access to such data. VPN technology is utilised to ensure the confidentiality, integrity, and security of information transmitted over public or untrusted networks, and to facilitate secure remote access to corporate resources in accordance with accepted cybersecurity practices.

1.1.5.40. "**Vulnerability Scanning**" means the automated assessment of systems to identify known security vulnerabilities based on recognised threat signatures and configuration weaknesses;

1.1.5.41. "**Warranty Period**" means the period during which the Equipment is covered under the manufacturer's warranty against defects in materials or workmanship, as determined solely by the applicable vendor warranty terms and commencing on the date specified by the vendor or as set out in the relevant Schedule.

1.1.6. should any provision in a definition be a substantive provision conferring rights or imposing obligations on any Party, then effect shall be given to that provision as if it were a substantive provision in the body of these Terms and Conditions;

1.1.7. any reference to an enactment, regulation, rule or by-law is to that enactment, regulation, rule or by-law as at the Effective Date, and as amended or replaced from time to time;

1.1.8. reference to 'days', 'months' or 'years' shall be construed as calendar days, months or years unless qualified by the word 'business', in which instance a "business day" shall be any day other than a Saturday, Sunday or public holiday as defined under the Public Holiday Act, 36 of 1994. Any reference to "business hours" shall be construed as being the hours between

08h00 and 17h00 on any business day from Mondays to Thursdays and 08h00 to 16h00 on Fridays. Any reference to time shall be based upon South African Standard Time;

1.1.9. when any number of days is prescribed, such number shall exclude the first and include the last day, unless the last day falls on a day which is not a business day in which case the last day shall be the next succeeding business day;

1.1.10. where figures are referred to in numerals and in words, and there is any conflict between the two, the words shall prevail, unless the context indicates a contrary intention;

1.1.11. in these Terms and Conditions, the word "clause" or "clauses" refer to clauses of these Terms and Conditions;

1.1.12. the use of the word "including" followed by a specific example/s shall not be construed as limiting the meaning of the general wording preceding it and the eiusdem generis rule shall not be applied in the interpretation of such general wording or such specific example/s;

1.1.13. expressions in any Schedule and Cybersecurity Services Agreement shall bear the same meaning as in these Terms and Conditions and vice versa. In the event of a conflict between the provisions of these Terms and Conditions and the provisions of any Schedule or Cybersecurity Services Agreement, the provisions of these Terms and Conditions shall prevail.

1.1.14. the expiration or termination of these Terms and Conditions shall not affect those provisions of these Terms and Conditions which expressly provide that they will operate after any such expiration or termination or which of necessity must continue to have effect after such expiration or termination, notwithstanding the fact that the clauses themselves do not expressly provide this;

1.1.15. the use of any expression covering a process or proceeding available under South African law including winding-up or sequestration shall, if any of the Parties is subject to the law of any other jurisdiction, be construed as including any equivalent or analogous process or proceeding under the law of such other jurisdiction;

1.1.16. in its interpretation, the contra proferentem rule of construction shall not apply; and

1.1.17. recordals shall be binding on the Parties and are not merely for information purposes.

2. COMMENCEMENT AND TERMINATION

2.1. The Customer appoints Itec, which appointment Itec accepts, to supply the Services to the Customer for the Initial Period in accordance with the terms and subject to the conditions set out in these Terms and Conditions and the Cybersecurity Services Agreement commencing from the Activation Date.

2.2. The Parties may terminate a Cybersecurity Services Agreement at the expiry of the Initial Period, by giving the other Party 30 (thirty) days' prior written notice before the end of the Initial Period, failing which, Itec shall continue to provide the Services and/or maintain the Equipment after the Initial Period on a month to month basis subject to the conditions of these Terms and Conditions and such Cybersecurity Services Agreement which shall continue indefinitely until terminated by either Party on 30 (thirty) days' prior written notice to the other Party. The Customer must send all notices of termination to Itec by email to cancellations@itecgroup.co.za.

2.3. At any time for the duration of this Agreement, Itec shall notify the Customer in writing of any material changes to the Cybersecurity Services Agreement as and when applicable.

2.4. Itec reserves the right to amend, modify and/or update these Terms and Conditions at any time, in its sole discretion and as required as per its operational, legal, or business needs. Any such amendments shall take effect immediately upon publication on the official Itec website. The Parties acknowledge and agree that all previous versions of the Terms and Conditions shall effective immediately be superseded and replaced by the most recent version once published on the official Itec website. Continued use of the services following publication shall constitute acceptance of the amended Terms and Conditions.

2.5. Should the Customer terminate any Cybersecurity Services Agreement prior to the expiry of the Initial Period for any reason whatsoever other than expressly provided for in these Terms and Conditions, the Customer shall remain liable for all amounts owing to Itec which would have been due up to the earliest possible date of valid termination of such Cybersecurity Services Agreement.

2.6. Itec will be entitled to cancel any Cybersecurity Services Agreement at any time on 30 (thirty) days' prior written notice to the Customer should Itec's obligations herein become impossible to fulfil, including in the event of –

2.6.1. Itec being unable, due to no fault of its own, to supply the Services or parts required for and/or consumables used in the Equipment;

2.6.2. the technology used in such Equipment being rendered outdated or obsolete and Itec no longer having such personnel with the necessary technical expertise to provide the Services, and/or spares and/or consumables no longer being available;

2.6.3. the Cybersecurity Services Agreement no longer being economically viable for Itec due to changes in legislation and/or changes in rate of exchange, and/or other external factors beyond Itec's control or a Force Majeure Event; and/or

2.6.4. Itec no longer having the required licenses due to no fault of its own to enable it to provide the Services and/or maintain the Equipment to the Customer.

2.7. On such cancellation by Itec in terms of clause 2.6, neither Party will have further rights and/or obligations in respect of the other arising out of and/or in terms of these Terms and Conditions, other than Itec's right to claim payment of any amounts that are already due by the Customer to Itec in terms of these Terms and Conditions, and the Customer's reciprocal obligation to make payment thereof to Itec.

2.8. Contract settlement cancellation quotations are valid for 7 (seven) calendar days. If the Customer does not return a signed acceptance, retract the cancellation, or lodge a bona fide, properly motivated written dispute within this period, the quotation shall be deemed accepted and processed. All cancellation charges or penalties specified in the quotation will then be invoiced accordingly.

2.9. The Customer shall have 3 (three) business days from the Activation Date to test the Equipment or Service and to notify Itec, in writing, of any disputes or issues in relation to the Equipment and/or Service. In the event that no disputes or issues have been raised in writing by the Customer, such Equipment or Service will be deemed as accepted and duly signed off by the Customer and Itec will start billing for the Charges.

2.10. In the event that activation of the Services that are installed on the Commissioning Date and/or Activation Date is delayed by the Customer for any reason, the Customer agrees to pay all Charges incurred from the Activation Date.

2.11. Any new or additional services, equipment and/or software to be provided by Itec to the Customer will be agreed to in a new and additional Cybersecurity Services Agreement, which will commence on the Activation Date set out therein and shall be subject to these Terms and Conditions.

2.12. The Parties acknowledge that the Services are subject to government or relevant authority regulated limitations and may be temporarily or permanently interrupted as necessary or appropriate and hereby indemnify one another against any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of such disruptions.

3. ITEC'S OBLIGATIONS & SERVICES

3.1. Itec shall implement, manage, and maintain the following services:
- 3.1.1. Endpoint Management: Deployment, monitoring, alerting, configuration management, and agent health monitoring.
- 3.1.2. Vulnerability Scanning: Scheduled internal and/or external scans, identification of risks, and provision of remediation recommendations.
- 3.1.3. Patch Management: Deployment of critical, security, and OS/application patches based on vendor schedules and agreed maintenance windows.
- 3.1.4. Exposure Assessment: Periodic assessment of attack surface visibility, exposed services, and misconfigurations.
- 3.1.5. Dark Web Monitoring: Monitoring for leaked credentials, organisational data exposure, and alerting on discovered findings.
- 3.1.6. Firewall Management: Configuration management, rule updates, policy optimisation, log monitoring, event triage, and backup of configurations.

3.2. Itec shall notify the Customer of any material risks or vulnerabilities identified during service delivery.

3.3. Itec shall maintain all relevant security controls, tools, and platforms necessary for fulfilling this Agreement, except where Customer-owned tooling is specified.

3.4. Itec does not guarantee uninterrupted or error-free operation of any security tooling due to the nature of cybersecurity threats.

3.5. Itec does not warrant that any Customer-owned or third-party hardware, software, or cloud platforms are without any vulnerabilities or are fit for purpose in providing the Services.

3.6. For the duration of the Initial Period as contracted, the Services, as defined in this Agreement, shall be provided exclusively by Itec. The Customer may not appoint, engage, or permit any third party to perform, support, maintain, manage, or otherwise deliver any of the Services or the maintenance of the Equipment supplied under this Agreement without Itec's prior written consent. The Customer may request to move the Services to another provider only where a valid and substantiated contractual ground exists, including a material breach by Itec of its obligations under this Agreement which remains uncured after the expiry of any applicable remedy period. Any preference, termination for convenience, or commercial motivation alone shall not constitute valid grounds for engaging an alternative provider. If Itec performs its obligations in accordance with this Agreement, the Customer shall remain bound by the exclusivity provisions herein for the full Initial Period.

3.7. The Services are provided for the exclusive use of the Customer and/or the User and is not provided for resale or use by third parties.

3.8. Itec will provide the Services and will maintain the Equipment during Business Hours in an efficient operating condition using standards and practices, methods and procedures exercising a degree of skill, care and diligence in accordance with good industry practice, save for circumstances beyond the control of Itec and any Force Majeure Event.

3.9. Itec shall deliver the Equipment to the Customer at the address set out in the Cybersecurity Services Agreement.

3.10. Itec cannot and does not guarantee or undertake that the provision of the Services will be provided at all times. In the event of any malfunction, failure, fault and/or interruption of any of the Services and/or the Equipment from any cause whatsoever –
- 3.10.1. Itec will, to the fullest extent permissible in law, not be liable for any direct or indirect loss or damages of any nature whatsoever or howsoever arising that may be sustained by the Customer and/or the User as a result of such malfunction, failure, fault and/or interruption; and
- 3.10.2. such malfunction, failure, fault and/or interruption will not constitute a breach by Itec of these Terms and Conditions, except where it can be proven that it was caused by Itec's gross negligence, with the Customer hereby waiving all claims it may have against Itec in respect of any such loss so arising from such malfunction and/or failure.

3.11. Itec's compliance with these Terms and Conditions will be measured monthly by reference to the Service Levels.

3.12. Itec will not be under any obligation to maintain the Equipment and/or Services in the event of the Customer not complying with any of the obligations placed upon it in terms of these Terms and Conditions.

3.13. Itec will respond in accordance with Response and Fault Procedures after a call has been logged by the Customer and/or the User with Help Desk and a service reference number has been furnished to the Customer and/or the User by Help Desk.

3.14. Itec will implement accepted industry-standard security precautions in relation to the Services. Notwithstanding such security precautions, Itec does not guarantee that the Services are invulnerable to all security breaches. Itec makes no warranty, guarantee or representation that the Services are entirely protected from all destructive elements, security threats, be it physical or cyber-attack, and/or other vulnerabilities.

3.15. Itec may, at its sole discretion, perform any Services by utilising remote access to Equipment using secure connections in line with Itec's Privacy Policy and as such a technician from Itec does not have to be physically present at the Site to provide the Services in terms of these Terms and Conditions.

3.16. Itec will charge a travelling fee in respect of the Services to be provided, where the Service and/or Equipment is situated outside Itec's standard service radius of 50 (fifty) kilometres from any authorised Itec service centre.

3.17. Any Services required by the Customer outside business days will be charged to the Customer in addition to the Charges at Itec's prescribed overtime service rates.

3.18. If Software is outside of its software maintenance term, as specified by Itec and/or the supplier of such Software, then Itec shall be under no obligation whatsoever to provide maintenance in respect of such Software.

3.19. When supplying the Equipment to the Customer, Itec will provide the Customer with instructions on how to use the Equipment in accordance with clause 4.22. Not complying in terms of clause 4.22 will result in a material breach of these Terms and Conditions and Itec will have the right to cancel these Terms and Conditions with immediate effect.

3.20. Itec will modify or replace, in accordance with the Schedules and the Cybersecurity Services Agreement, subject to clause 3.16, parts and/or modules of the Equipment where required when maintaining the Equipment and ownership in any such old parts and/or modules which have been so replaced will vest with Itec.

3.21. Itec endeavours to make available a replacement security appliance or an equivalent workaround solution in the event of a hardware failure of the firewall or network security equipment caused by normal operation, subject to the following conditions:
- 3.21.1. **Equivalent Replacement or Workaround**
  - 3.21.1.1. Itec reserves the right to provide an equivalent or functionally similar security appliance, virtual appliance, temporary loan unit, or alternative workaround solution to restore the Services. As firewalls and cybersecurity appliances generally do not include replaceable internal spares or field-replaceable modules, replacement is typically fulfilled on a device-swap or RMA basis.
- 3.21.2. **Exclusions and Customer Liability**
  - 3.21.2.1. Itec shall not be liable for any hardware failure resulting from abnormal operation, misuse, improper configuration, physical damage, unauthorised modifications, or negligence by the Customer, as referenced in clause 4.16.
  - 3.21.2.2. Where failures arise from such causes, the Customer shall be liable for all costs associated with the replacement unit, RMA rejection, or any other charges attributable to such circumstances, including those described in clause 7.

3.21.3. **Availability and Replacement Timeframes**
3.21.3.1. All replacement of firewalls or security appliances is subject to availability from the manufacturer and may depend on international logistics, OEM RMA processing times, and shipping lead times.
3.21.3.2. During the Warranty Period, all travel, callout fees, and labour costs associated with the RMA process shall be provided to the Customer at no additional charge, provided the Customer is subscribed to an applicable Managed SLA Service with Itec.
3.21.3.3. For Customers who are not subscribed to a Managed SLA Service, or where the Warranty Period has expired, or where the Manufacturer rejects the Warranty claim due to Customer negligence or wilful misconduct, the costs associated with travel, callouts, labour, and any related services will be billed at Itec's prevailing prescribed rates.
3.21.3.4. Itec shall not be liable for any loss, damage, or operational impact suffered by the Customer as a result of delays in obtaining replacement units.

3.22. At the Customer's request and cost (unless otherwise specified in a Schedule), Itec may provide a temporary loan firewall at Itec's then-applicable rates until a permanent replacement is supplied.

3.23. **Warranty Conditions:**
3.23.1. Any replacement or RMA of security appliances is subject to the applicable OEM warranty terms and the warranty conditions recorded in Schedule 2, including but not limited to the manufacturer's RMA acceptance criteria.

3.24. **Data Loss and Security State:**
3.24.1. Itec shall bear no liability for any loss of configuration, logs, policies, stored data, or security-related information residing on the firewall or security appliance, except where such loss is caused by Itec's gross negligence.
3.24.2. Any such liability shall be limited to the amounts charged to the Customer under the Cybersecurity Services Agreement.

3.25. **Hardware Failure and Replacement of Security Appliances:**
3.25.1. Itec agrees to facilitate the replacement of a faulty firewall or network security appliance in the event of a hardware failure arising from normal operation, strictly in accordance with the applicable vendor's RMA process, and subject to the following conditions:
3.25.1.1. All replacements or repairs of firewalls and security appliances shall be performed in line with the vendor's official RMA procedures, turnaround times, and approval requirements.
3.25.1.2. Itec does not guarantee the availability of local replacement stock and shall not be obliged to hold, reserve, or supply immediate replacements from its own inventory.

3.26. **Equivalent Device or Workaround**
3.26.1. Where permitted under the vendor's RMA terms, Itec may provide an equivalent or functionally similar device, virtual appliance, or temporary workaround to restore Services, at Itec's sole discretion.

3.27. **Exclusions and Customer Liability**
3.27.1. Itec shall not be liable for any hardware failure caused by abnormal operation, misuse, unauthorised modification, physical damage, environmental factors, or negligence by the Customer, as referenced in clause 4.16.
3.27.2. Where failures arise from such causes, all costs relating to replacement, RMA rejection, logistics, or new device procurement shall be for the Customer's account.

3.28. **Availability, Lead Times, and Logistics**
3.28.1. Replacement timelines are dependent on the vendor's RMA approval, international shipping, customs clearance, and stock availability.
3.28.2. Itec shall not be liable for any loss, damage, downtime, business interruption, or consequential loss resulting from delays in vendor RMA processing or delivery.
3.28.3. At the Customer's request and cost (unless otherwise specified in a Schedule), Itec may provide a temporary loan firewall at Itec's then-applicable pricing.

3.29. **Warranty Conditions**
3.29.1. All firewall replacements are subject to the applicable vendor warranty and the terms set out in Schedule 2, including any vendor requirements for diagnostics, logs, return of equipment, or advance replacement eligibility.

3.30. **Data and Configuration Loss**
3.30.1. Itec shall bear no liability for any loss of data, configurations, logs, policies, or security information stored on any firewall or security appliance, except where such loss results from Itec's gross negligence.
3.30.2. Such liability, if applicable, shall be limited to the amounts charged to the Customer under the Cybersecurity Services Agreement.

3.31. The Customer consents –
3.31.1. to Itec and Affiliates retaining all "Consumer Data" (being the information trail the Customer and/or the User leave behind as a result of using a public sources and channels as social media networks, marketing campaigns, the Customer service requests, call centre communication, online browsing data, purchasing history and preferences, etc.) and "Customer Profile Data" (being information for the Customer or set of Customers that includes demographic, geographic and psychographic characteristics, connectivity performance statistics, call records, hosted firewall records as well as buying patterns, creditworthiness and purchase history) provided by the Customer and/or the User and/or generated through the provision of the Services during the period of these Terms and Conditions;
3.31.2. that Itec and its Affiliates may, to the extent permitted by law, and for the purpose of these Terms and Conditions only, receive or disclose the Consumer Data and/or Customer Profile Data, including personal information, documents, detailed usage records, credit profile information and/or any other credit information; and
3.31.3. that Itec may, to the extent permitted by law, receive or disclose Consumer Data and/or Customer Profile Data to any law enforcement agencies that require the information for the prevention or investigation of criminal activities.
3.31.4. Accordingly, Itec will ensure that it is compliant with any Data Protection Legislation applicable from time to time within the appropriate jurisdiction.

4. THE CUSTOMER'S OBLIGATIONS

4.1. The Customer will pay Itec all the Charges as and when they become due and payable.
4.2. The Customer will ensure that any User will at all times comply with these Terms and Conditions and the Customer's obligations in terms hereof and as such will procure that the User is aware of these Terms and Conditions and has agreed, in writing, to comply with the terms of these Terms and Conditions at all times. The Customer will be liable for any breach of the terms of these Terms and Conditions by any User and hereby indemnifies Itec against any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of a breach by the User of any of the terms of these Terms and Conditions.

4.3. The Customer is responsible for the security of its own LAN and will not use, or permit the Services to be used, directly or indirectly, to carry or transmit (or facilitate the carriage or transmission) of any message, data or information which does not belong to or originate from the Customer, permit any person to utilise the Services or any Equipment or Software or retain possession of any Equipment or Software without the explicit consent of the Customer and any other unauthorised or fraudulent use of the LAN, the Services and/or the Equipment. The Customer shall be liable for all acts or omissions of any third-party utilising the Services with or without the Customer's permission. The Customer indemnifies Itec against any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of any such unauthorised or fraudulent use whatsoever.
4.4. Provide Itec with accurate information, access credentials, network diagrams, and system visibility required to deliver the Services.
4.5. Ensure endpoints, servers, and systems remain powered on and accessible for patching, scanning, and updates.
4.6. Implement the remediation recommendations provided by Itec within reasonable timeframes.
4.7. Maintain internal security hygiene, including user training, MFA enforcement, password policies, and removal of dormant accounts.
4.8. Ensure that unsupported, legacy, or end-of-life systems are either upgraded, isolated, or risk-accepted.
4.9. Notify Itec timeously of any suspected security incidents or material changes in environment or IT infrastructure.
4.10. In the event of any unauthorized, unlawful, or fraudulent use of the Services arising from, or attributable to, a security breach, compromise, or unauthorized access of the Customer's internal network, systems, or infrastructure (including but not limited to the Customer's LAN), the Customer shall remain fully liable for all associated costs, fees, charges, losses, or expenses incurred during such breach or unauthorized activity. This includes, without limitation, all data usage charges, call termination charges, service utilisation fees, and any other Charges accrued as a result of the unauthorized or fraudulent use.
4.11. The Customer shall –
4.11.1. not use the Services, nor permit any third party to use the Services, for any unlawful, unauthorized, malicious, or fraudulent purpose, including any activity that may compromise the security, integrity, or availability of any information system, network, or data.
4.11.2. only use the Equipment in accordance with the manufacturer's instructions and specifications and for the purposes and in the manner for which it is intended;
4.11.3. use the Equipment strictly in accordance with the manufacturer's instructions, specifications, and cybersecurity best-practice guidelines, and only for its intended purpose and in the manner for which it is designed.
4.11.4. not act or omit to act, or allow others to do so, in any way likely to damage, disrupt or interfere with the Services or to injure or damage any person or property or to cause the quality of the Services to be impaired or interrupted in any manner whatsoever.
4.11.5. obtain all necessary approvals, authorisations, or consents required under applicable legislation, regulations, cybersecurity standards, or instructions issued by any governmental authority or by Itec relating to the use, configuration, deployment, and security of the Services and Equipment.
4.11.6. Itec shall not be liable for any loss or damages arising from the Customer's failure to obtain such approvals. The Customer hereby indemnifies and holds Itec harmless against any direct or indirect loss, damage, liability, penalty, or claim arising from such failure.
4.11.7. not engage in, permit, or omit to prevent any act that may:
4.11.8. compromise, damage, degrade, disrupt, or interfere with the security, functionality, integrity, or performance of the Services, the Equipment, or any related network;
4.11.9. cause harm, injury, or damage to any person, system, infrastructure, or property; or
4.11.10. impair, interrupt, or negatively affect the quality, confidentiality, availability, or resilience of the Services in any manner whatsoever.
4.11.11. The Customer will provide Itec with remote access at all times to all Equipment and relevant systems, as well as reasonable access to the Site during business hours, to any authorised representative of Itec for any of the purposes of these Terms and Conditions, including –
4.11.12. installation, removal and collection of the Equipment (where required);
4.11.13. to carry out any inspection, repair, testing or maintenance of the Equipment relevant to the provisioning of the Services;
4.11.14. to verify that the manner in which the Services being utilised by the Customer and/or the User is in compliance with these Terms and Conditions and the Cybersecurity Services Agreement as well as all applicable South African laws; and
4.11.15. any other reasonable purpose as determined by Itec and/or to enable Itec to comply with its obligations in terms of these Terms and Conditions.
4.11.16. Itec will not be liable, and the Customer hereby indemnifies, and keeps Itec indemnified against any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of the Customer not providing Itec with remote access or actual access to its Site as required in terms of these Terms and Conditions.
4.11.17. The Customer will provide –
4.11.17.1. a suitable and clean environment for the housing and operation of the Equipment, and a stable standard and/or specialized power supply and connection points in compliance with the relevant installation standards and manufacturer's instructions and/or any specifications required by Itec, which power point will be utilized exclusively for the Equipment. The Customer indemnifies Itec against any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of the Customer's failure to provide such a stable and/or specialized power supply; and
4.11.17.2. unless provided by Itec as part of the installation of the Equipment, all required trunking, cabinet space, conduits, cable trays, certified fit-for-use network points, as well as an uninterrupted power supply as is required for the Services and Equipment.
4.11.17.3. The Customer will take up or remove such fitted or fixed floor coverings, ceiling tiles, suspended ceiling and partition covers as may be necessary to install the Equipment and the Customer will be liable to carry out and make good any repair work required at its Site subsequent to such installation.
4.11.17.4. The Customer will be present at any installation or maintenance of the Equipment by Itec, its personnel or contracted installer and shall sign the relevant delivery note and/or job card on completion thereof.
4.11.17.5. The signature by the Customer of any acceptance certificate provided by Itec and/or its service providers upon the installation of the Equipment, shall be deemed to be an acknowledgement by the Customer that it has fully inspected and approved the Equipment and all of its components and that the Equipment and components have been received to the full satisfaction of the Customer.
4.11.17.6. The Customer will ensure that the Services are used strictly in accordance with Itec's AUP, which is available on request, and the Customer will at all times comply with all applicable South African laws and the Response and Fault

Procedures and will report all service requests through Help Desk and/or any such other point of contact indicated by Itec.

4.11.17.7. The Customer will ensure that all equipment connected to or used in conjunction with the Services, is connected or used in accordance with Applicable Law and shall obtain the prior written approval of Itec before connecting or permitting any third-party to connect any equipment to any Equipment.

4.11.17.8. The Customer will ensure that all equipment and software installed by or for the Customer and/or the User and used in conjunction with the Services is compatible with, and will function with all Equipment, Services and Software.

4.11.17.9. The Customer will not abuse the Services or damage the Equipment or do anything to prevent or preclude Itec from being able to provide the Services.

4.11.17.10. The Customer will be responsible for its own LAN and other infrastructure and shall implement such reasonable security measures in respect thereof to ensure that the security of the Services provided is not compromised either directly and/or indirectly via any third-party connected equipment.

4.11.17.11. The Customer will promptly comply with all notices, instructions or directions given by Itec in respect of the installation, use or operation of the Services, Software and/or the Equipment.

4.11.17.12. The Customer will, subject to the provisions of these Terms and Conditions, install, use and maintain all Equipment necessary for the provision of the Services in a good working order (fair wear and tear excepted) in accordance with the specifications, guidelines and recommendations of Itec and the Supplier thereof.

4.11.17.13. All risk in and to the Equipment will pass to the Customer upon delivery thereof to the Site and it is the responsibility of the Customer to have such equipment comprehensively insured. The Customer will be liable for any loss, theft and/or damage to the Equipment.

4.11.17.14. The Customer will at all times retain custody and control of the Equipment at the Site or such other site as Itec may have approved for such purpose.

4.11.17.15. The Customer will not use or permit the use of the Services or install, connect, link or use any electronic communication equipment in contravention of any Applicable Laws.

4.11.17.16. The Customer will not carry out or permit to be carried out any additions, improvements, adjustments, modifications, alterations or replacements to the Equipment and/or Services without the prior written consent of Itec.

4.11.17.17. The Customer will appoint at least 1 (one) person and at most 3 (three) persons as “System Manager/s” for the Equipment and Services. Itec will provide initial training to the System Manager/s in respect of the use and functionality of the Equipment as well as training for any major upgrades. The Customer will be liable to pay, at Itec’s then prescribed rate, for any additional or further training on the Equipment and/or should additional training be required as a result of new System Manager/s being appointed by the Customer. The Customer shall immediately notify Itec in writing of any changes in the System Manager/s.

4.11.17.18. The Customer warrants that it will not do anything or allow anything to be done which may in any way prejudice the proprietary rights of Itec or any of its service providers or suppliers.

4.11.17.19. The Customer will be liable for any repairs and/or damages to the Equipment, if such repairs are due to negligence, recklessness, misuse, accident, wilful act or omission, and/or any causes other than ordinary use of the Equipment by the Customer. Itec will charge the Customer, at its then prescribed rate, for repairs necessitated by any such cause. In the case of a call-out being performed and the reason for fault is deemed, in the sole discretion of Itec, to be the Customer’s, the Customer will be liable for a call-out fee, labour, parts, replacement Equipment, and any other fees, on the rate Itec charges for call out fees at the time of the call out, and all travelling fees, regardless of the distance.

4.11.17.20. The Customer will correctly operate the Equipment, including complying with the proper implementation of all operator configuration, settings and adjustments, as per the supplied operation manuals and all instructions from Itec, and will take all reasonable steps to ensure that the Equipment is not being damaged or tampered with.

4.11.17.21. The Customer will inform Itec in writing at least 1 (one) month in advance of any required re-siting of the Equipment and will ensure that no other party (other than Itec or its duly authorised agent) attends to such re-siting. If the Equipment is being re-sited by any person other than Itec or its duly authorised agent, the Customer will be responsible for any damage/s to the Equipment during such re-siting (without prejudice to any other rights and/or remedies Itec may have in such circumstances) and for this purpose it will be presumed that any defect/s and/or damage/s to the Equipment, were incurred during such re-siting.

4.11.17.22. In the event of any changes in the Customer’s LAN configuration, or the Customer’s network environment affecting the performance of the Equipment and/or the quality of the Services in any way, Itec will not be held liable for any loss in productivity or any other loss or damage suffered by the Customer, and the Customer indemnifies Itec against any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of the changes in the performance of the Equipment and/or the quality of the Services. The Customer agrees that the Customer will be liable to pay Itec any Charges billed by Itec to adapt the Equipment to the changes in the Customer’s LAN configuration, or the Customer’s network environment.

4.11.17.23. The Customer will not instruct Itec’s employees or Itec’s suppliers to deviate from the original approved Scope of Work at any time during the implementation and installation of Services, unless otherwise agreed to, in writing, between both parties. The Customer will be liable to pay all Charges relating to the correction and/or modifications needed to rectify such deviation if such deviation results in Itec not being able to deliver and/or implement the Service.

5. CHARGES AND PAYMENTS

5.1. Itec will invoice the Customer for each Service provided.

5.2. The Customer will pay to Itec each month, per debit order, on or before the due date indicated by Itec on each statement, all amounts due to Itec in terms of these Terms and Conditions, without delay, deduction or set-off, including the Charges due for each month, failing which payment Itec will have the right, on notice, to suspend the provision of the Services to the Customer until all outstanding amounts due to Itec are paid (without prejudice to any of Itec’s other rights and/or remedies). In terms of the Cybersecurity Services Agreement, the Customer gives Itec authority to draw against the Customer’s bank account, wherever it may be, the amounts due to Itec in terms of these Terms and Conditions, save where a different payment method has been agreed between the Parties in writing. On written agreement between both parties, the Customer will pay to Itec each month per Electronic Funds Transfer, within 30 days of the Due Date indicated by Itec on each statement of account, all amounts due to Itec in terms of the Cybersecurity Services Agreement, without delay, deduction or set-off, including the charges due for each month, failing which payment Itec will have the right, on notice, to suspend the provision of the Services to the Customer until all outstanding amounts due to Itec are paid (without prejudice to any of Itec’s other rights and/or remedies).

5.3. Should the Customer elect not to sign the debit order confirmation the Customer and/or a director of the Customer will be obliged to sign a personal guarantee and/or surety.
5.4. The Customer shall be liable to pay to Itec a once-off installation/provisioning fee which shall be billed and invoiced to the Customer together with the Charges due for the first month following activation.
5.5. Itec will be entitled to charge interest on any overdue amount at the Prime Rate plus 6% (six percent).
5.6. The Customer will be liable for any bank charges or any other fees, which Itec may have incurred if a debit order is returned and left unpaid and will pay Itec an administrative fee of R 50.00 (fifty Rand), excluding VAT, for any payments made by a method other than by debit order.
5.7. The Customer agrees that the service charge may fluctuate from time to time with changes in Itec's weighted average costs of conforming to statutory obligations and/or regulations, forex fluctuations and all other similar costs. Itec will provide reasonable notice if such changes in forex fluctuations or other statutory regulations occur. Changes in the service charge as aforesaid may be decreased or increased (in order to recover any increased cost to Itec and/or to maintain the internal rate of return enjoyed by Itec immediately prior to the said change), by such amount as is necessary.
5.8. The Customer agrees that the prevailing service charge will increase once per year on the anniversary of the Activation Date, which rate will be maintained at market related levels.
5.9. The Customer will pay to Itec its re-siting and installation charges for any re-siting of Equipment and/or Services at Itec's then prescribed pricing in the event that any re-siting of the Equipment and/or Services is required.
5.10. Itec will charge Pro-rata Billing as from the Activation Date in the following instances:
5.10.1. the Customer changes a Service in a billing cycle. Itec will charge the Customer part of the current Service rate for the current Service and will charge for the new Service as from the Activation Date in that month;
5.10.2. the Customer upgrades or increases a Service. Itec will charge the Customer for the upgraded/increased Service as from the Activation Date for the new Service in that month.

6. DOWNTIME AND DELAY

6.1. Whereas Itec undertakes to use reasonable endeavours to keep the Services available at all times, the Customer acknowledges that –
6.1.1. maintenance activities, including but not limited to security patching, signature updates, software upgrades, incident response tuning, infrastructure remediation, and other operational or technical adjustments to the Cybersecurity Services and/or Equipment, may be required from time to time and may result in temporary service suspension. Itec will, where reasonably possible, provide the Customer with reasonable prior notice of any such suspension and will use reasonable efforts to ensure that interruptions are minimal and performed outside standard business hours. Notwithstanding any interruption or delay, these Terms and Conditions will remain valid and enforceable during the period of such interruption. Itec will not be liable for any claim, loss or damages as a result of a delay or suspension of the Services caused by a third- party, an outage on a third-party's network or by any reason not within Itec's control;
6.1.2. any suspension of the Services resulting from the Customer's actions, negligence, misconfiguration, failure to follow security recommendations, unauthorised access, unlawful use, or physical or logical damage to the Equipment and/or Services shall not entitle the Customer to terminate the Cybersecurity Services Agreement. The Customer fully indemnifies and holds Itec harmless against all losses, damages, costs or claims arising from such actions or misuse.
6.1.3. The Customer acknowledges that the Services may rely on third-party networks, cloud platforms, data centres, monitoring feeds, or other infrastructure components that operate on a "Best Effort" basis. Itec shall not be liable for any disruption, delay, reduced performance, or downtime caused by failures or service interruptions on such third-party infrastructure and/or services.
6.1.4. In the event that the firewall or security appliance fails, becomes inoperable, or is required to be removed for diagnostics, repair, or vendor RMA, the Customer acknowledges that the security posture of the environment may be reduced or temporarily unavailable. Itec shall not be liable for any security incident, breach, loss, or damages experienced during such periods of downtime. The Customer accepts the associated risk and remains solely responsible for any exposure during the outage.

7. EXCLUSIONS

7.1. Without derogating from and in addition to any other provisions herein contained, the Charges do not cover maintenance activities relating to firewall infrastructure and may include, but are not limited to:
7.1.1. firmware upgrades and security patch installations;
7.1.2. rule-base and policy updates;
7.1.3. IPS signature updates;
7.1.4. threat-intelligence feed synchronisation;
7.1.5. HA failover testing;
7.1.6. log retention/archiving and system optimisation;
7.1.7. corrective actions due to detected vulnerabilities or security risks.
7.1.8. Full incident response or digital forensics
7.1.9. Recovery from ransomware or data corruption
7.1.10. Customer negligence or failure to follow recommendations
7.1.11. Protection against zero-day threats not yet known to industry
7.1.12. Systems not disclosed to or onboarded by Itec
7.1.13. Support for non-standard, unsupported, or end-of-life systems
7.2. These activities may result in temporary interruption or degraded performance of the Firewall or related Cybersecurity Services.
7.3. All Terms and Conditions remain valid during any interruptions or delays.
7.4. Itec shall not be liable for any claim, damages, or loss caused by:
7.4.1. failures, downtime, or performance degradation of third-party networks (including ISP links, cloud platforms, upstream carriers, or SD-WAN underlays);
7.4.2. outages affecting security vendors (e.g., threat-intelligence feeds, sandboxing services, endpoint integrations, SOC/MDR providers);
7.4.3. DDoS attacks or other cyber events targeting upstream infrastructure;
7.4.4. environmental factors or power failures;
7.4.5. causes beyond Itec's reasonable control.
7.5. Suspension of Firewall or Cybersecurity Services resulting from the Customer's actions — including but not limited to:
7.5.1. misconfiguration of firewall rules by non-authorised personnel;

7.5.2. the customer bypassing, disabling, or interfering with security controls;
7.5.3. connecting unauthorised devices or networks;
7.5.4. unlawful use, high-risk changes, or deliberate circumvention of security features;
7.5.5. physical or logical damage to the firewall equipment,
7.5.6. shall not entitle the Customer to terminate the Cybersecurity Services Agreement.
The Customer indemnifies Itec against all losses, claims, costs, or damages arising from such actions.

7.6. The Customer acknowledges that the Firewall and Cybersecurity Services may rely on:
7.6.1. upstream ISP links or MPLS underlays;
7.6.2. cloud-based management platforms (e.g., FortiManager, Sophos Central, or similar);
7.6.3. vendor threat-intelligence networks;
7.6.4. external sandboxing or malware-analysis engines;
7.6.5. DNS, PKI, or authentication services.
Some of these components operate on a "Best Effort" or shared-infrastructure basis.

7.7. Itec will not be liable for any disruption, delay, reduced performance, or downtime resulting from failures within such third-party infrastructure.

7.8. Without derogating from and in addition to any other provisions herein contained, the Charges do not cover –
7.8.1. damages, repairs and/or service necessitated by and/or arising out of –
7.8.1.1. service, repairs, alterations and/or specification changes performed without the prior authorisation of Itec;
7.8.1.2. tampering with and/or unauthorised movement or relocation of the Equipment by any person not authorised by Itec;
7.8.1.3. unauthorised connection or integration of the Equipment to other equipment, devices, lines and/or Software; unsuitable environmental influences; and
7.8.1.4. Force Majeure Events, water, lightning, power surges or dips, accidents, negligence, misuse, abuse, any conditions arising out of other connected Equipment, or any use other than that for which the Equipment was designed; and
7.8.1.5. construction of additional facilities which are required to connect the Customer to the Itec network;
7.8.1.6. network connectivity and/or support thereof, Software upgrades or reloading of Software to Equipment, Software functions not covered by the Customer's software licence and/or Software maintenance other than in accordance with the relevant software licence;
7.8.1.7. adjustments, alterations and/or repairs required to protect the Equipment against external interferences caused by radio waves, induction and/or other sources;
7.8.1.8. any firewall or cybersecurity system additions, moves, changes, or deletions requested after the initial Scope of Work sign-off will be treated as out-of-scope work. This includes, but is not limited to, firewall rule changes, VPN user updates, network segmentation changes, and security policy modifications.
7.8.1.9. developments, repairs, additions, adjustments or modifications to the Equipment that are not produced by, or in co-operation with Itec; and
7.8.1.10. any operating system, package software, application, platforms and/or server or terminal device that is developed by a vendor outside of Itec's supplier of the Equipment and/or Software and which is designed to be used for a wider variety of applications than those developed by such supplier of Itec, for example Microsoft Windows and/or Linux servers, or the use of Equipment in conjunction with third-party equipment and/or software which is proven to be defective or does not meet Itec's specifications for compatibility with the Equipment and/or Software as specified by Itec.

7.9. Subject to clause 7.1, the Customer will be liable to Itec for any repairs, services and/or parts (as the case may be) excluded from these Terms and Conditions, at Itec's then prescribed rate.

7.10. Notwithstanding anything herein contained, Itec will not be responsible for any direct or indirect loss or damages of any nature whatsoever or howsoever arising as a result of any acts and/or omissions of Itec and/or its representatives.

7.11. Further and in the event of the Equipment containing data storage devices, Itec will bear no liability in the event of any loss of and/or damage to data stored, and/or intended to be stored, thereon or thereby.

8. ACCEPTABLE USE POLICY

8.1. Itec's Acceptable Use Policy (AUP) can be accessed and viewed by visiting our website. The AUP is published at https://itecgroup.co.za/ - Legal Stuff.

9. FAIR USE POLICY

9.1. Itec's Fair Use Policy (FUP) can be accessed and viewed by visiting our website. The FUP is published at https://itecgroup.co.za/ - Legal Stuff.

10. BREACH

10.1. In the event that the Customer –
10.1.1. commits a breach of any of the terms, conditions, payment obligations, undertakings or representations contained in these Terms and Conditions or the Cybersecurity Services Agreement (all of which terms are deemed material), and should such breach be incapable of being remedied; or
10.1.2. capable of being remedied, and the Customer fails to remedy such breach within 30 (thirty) days after receipt of a written notice to that effect from Itec requiring the breach to be remedied;
10.1.3. terminates the Cybersecurity Services Agreement for any reason whatsoever before the end of the Initial Period;
10.1.4. becomes subject to any insolvency proceeding, inter alia, a final or provisional order of liquidation or sequestration, a compromise with any of its creditors, being or in the process of being wound up, being under judicial management, or any business rescue being proposed or has commenced in terms of the Companies Act 71 of 2008;
10.1.5. failing to satisfy or failing to make application for the rescission of any judgement that has been granted against it for more than 60 (sixty) days after becoming aware of such judgment;
10.1.6. makes false statements in connection with these Terms and Conditions or the Cybersecurity Services Agreement;
10.1.7. commits any fraudulent act or makes any misrepresentation in relation to these Terms and Conditions or the Cybersecurity Services Agreement;
10.1.8. repudiates these Terms and Conditions or the Cybersecurity Services Agreement or any of the obligations set out herein; or
10.1.9. does anything to prejudice Itec's right under these Terms and Conditions or the Cybersecurity Services Agreement,
Itec will be entitled, without prejudice to any other rights it may have in terms of these Terms and Conditions or in law, to cancel all of

the Cybersecurity Services Agreements and/or claim all amounts which are in arrears at the date of cancellation, including interest, and all payment that would have been paid by the Customer from the date of the aforesaid cancellation until the next earliest possible date upon which the Cybersecurity Services Agreements could have terminated on notice as pre-estimated liquidated damages.

10.2. Should Itec instruct an attorney to collect any amounts in terms of breach of these Terms and Conditions, or take any other action under these Terms and Conditions for the enforcement of its rights hereunder, the Customer will be liable to pay all fees and other legal charges on the scale as between attorney and own client, whether Court proceedings have been instituted or not.

10.3. In the event that Itec –

10.3.1. commits a material breach of any of the terms, conditions, payment obligations, undertakings or representations contained in these Terms and Conditions or the Cybersecurity Services Agreement, and should such breach be –

10.3.1.1. incapable of being remedied; or

10.3.1.2. capable of being remedied, and Itec fails to remedy such breach within 30 (thirty) days after receipt of a written notice to that effect from the Customer requiring the breach to be remedied,

10.3.2. then the Customer will be entitled, without prejudice to any other rights which it may have in terms of these Terms and Conditions or at law, either, to claim specific performance by Itec, or to immediately terminate the Cybersecurity Services Agreement. The Customer's remedies in the event of a breach by Itec will be limited to a claim for the repayment of the Charges for the relevant period in question as contained in the applicable Cybersecurity Services Agreement.

11. INTELLECTUAL PROPERTY RIGHTS

11.1. All right, title and interest in and to the "Itec" name and logos and/or any other trademarks, brand names and/or logos used by Itec, or its Affiliates and/or which relate to the Equipment, Services and the Software ("Trademarks") vest in Itec (or its supplier and/or licensee, as the case may be), and the Customer has no claim of any nature thereto. Similarly, all rights in and to the intellectual property associated with and/or relating to the Software, Services and the Equipment irrevocably vests in Itec (or its suppliers or licensees, as the case may be), and all Software provided remains the exclusive property of Itec (or its suppliers or licensees, as the case may be).

11.2. The intellectual property rights attaching to the Software may be held by the third-party owner thereof. Accordingly, to the extent permitted by such third-party, Itec hereby grants to the Customer and/or the User a non-exclusive license to use the Software for the purpose for which it was supplied for the duration of these Terms and Conditions.

11.3. Before Itec supplies any Software to the Customer, the Customer shall enter into the applicable software license agreement pertaining to the Software to protect the intellectual property rights of Itec and its suppliers or licensees in and to the Software. If the Customer breaches any of the terms of any such software license agreement, Itec shall be entitled to terminate such software license agreement or cause any such software license agreement to be terminated with immediate effect, without prejudice and in addition to any and all other rights and remedies of Itec in such circumstances. The Customer hereby consents to Itec inspecting an installation at the Site for the purpose of verifying whether a programme configuration of Software supplied to the Customer conforms to the Customer's information as registered with Itec and/or as specified in the applicable software license agreement, and in the event of the Customer's system being discovered to contain an installation or configuration of the Software not in conformity with the Customer's information as registered with Itec and/or as specified in the applicable software license agreement, Itec shall be entitled to terminate the Customer's unauthorised use of the Software.

11.4. The Customer undertakes to keep confidential (as per clause 14) all operating manuals and other documentation supplied by Itec in terms of these Terms and Conditions and shall disclose same to its employees, agents or contractors on a need-to-know basis.

11.5. The Customer shall not nor permit anyone else to, without the prior written consent of Itec, to copy, reverse engineer, decompile, modify, tamper with, vary, enhance, copy, sell, lease, licence, sub-licence or otherwise deal with the Software, the operating manuals or other documentation, or any part, variation, modification, release or enhancement thereof or have any software or program written or developed based on it;

11.6. The Customer shall not, by means of the Services, infringe the intellectual property rights of any third-party by means of, inter alia, the using, publishing, submitting, copying, uploading, downloading, posting, transmitting, reproducing or distributing Software, video or audio content or any other material owned by any third-party and protected in terms of any intellectual property rights, trademark law or other proprietary rights.

11.7. The Customer hereby indemnifies Itec against any direct and indirect costs, claims, damages and/or expenses which may be incurred by Itec as a result of any claim brought by any third-party arising out of the breach of the provisions of this clause 12 (whether by the Customer, the User or any other party engaged by the Customer and/or the User), including all and any legal costs incurred on an attorney and own client scale.

12. DATA PROTECTION

12.1. **INTERPRETATION**

12.1.1. "**Data Protection Legislation**" means any and all laws relating to the protection of data or of Personal Information relevant to a Party, including POPI, the GDPR (to the extent applicable) and the protection of Personal Information principles agreed to in these Terms and Conditions;

12.1.2. "**Data Protection Legislation**" means any and all laws relating to the protection of data or of Personal Information relevant to a Party, including POPI, the GDPR (to the extent applicable) and the protection of Personal Information principles agreed to in these Terms and Conditions;

12.1.3. "**GDPR**" means the General Data Protection Regulation 2016/679, as amended from time to time;

12.1.4. "**Personal Information**" shall have the meaning ascribed thereto in applicable Data Protection Legislation;

12.1.5. "**POPI**" means the Protection of Personal Information 4 of 2013; and

12.1.6. "**Process**" shall have the meaning ascribed thereto in applicable Data Protection Legislation.

12.2. **PROCESSING OF PERSONAL INFORMATION**

12.2.1. Each Party warrants to and in favour of the other that it shall at all times during the term of these Terms and Conditions comply with Data Protection Legislation.

12.2.2. The Customer acknowledges that Itec may be required to Process the Personal Information of the Customer and other relevant data subjects (including the Customer's customers) ("Customer Personal Information") in connection with and for the purposes of providing its Services to the Customer and for fulfilling its obligations in terms of these Terms and Conditions.

12.2.3. Itec shall —

12.2.3.1. only Process the Customer Personal Information for the purpose(s) connected with the provision of the Services and to the extent strictly necessary to provide the Services, except to the extent specifically requested to do otherwise by the

Customer in writing or required by Data Protection Legislation or other Applicable Laws;

12.2.3.2. comply with all reasonable, lawful directions and instructions which may be given by the Customer regarding the Processing of the Customer Personal Information;

12.2.3.3. only Process the Customer Personal Information strictly in compliance with Data Protection Legislation and Itec's Privacy Policy, published at https://itecgroup.co.za/ - Legal Stuff, and

12.2.3.3.1. secure the integrity and confidentiality of the Customer Personal Information in its possession or under its control by taking appropriate, reasonable technical and unauthorized measures to prevent –

12.2.3.3.1.1. loss of, damage to, or unauthorized destruction of the Customer Personal Information; and/or

12.2.3.3.1.2. unlawful access to or unlawful Processing of the Customer Personal Information.

12.2.3.4. Where the Customer provides Itec with Personal Information relating to a third-party data subject (including but not limited to the Customer's staff, suppliers, customers, directors, shareholders, and affiliates), the Customer warrants that it has obtained all necessary approvals and/or consents, as applicable, from such third-party data subjects and to the extent required by Applicable Law, for the Customer to share such Personal Information with Itec (unless otherwise unauthorized to share their Personal Information in terms of another lawful basis).

12.2.4. The Customer shall be liable to Itec for its failure to comply with any of its obligations under this clause 13 and shall indemnify Itec against all claims, damages, costs, or administrative fines arising therefrom, except to the extent caused by Itec's breach of its obligations. The indemnification provisions in this clause 13.2.1.6 are in addition to, and do not in any way derogate from, any statutory or common law remedy Itec may have for breach of these Terms and Conditions, including breach of any representation or warranty.

13. CONFIDENTIALITY

13.1. Subject to clause 12.2, each Party undertakes to the other Parties that it will treat as confidential the terms of these Terms and Conditions and Cybersecurity Services Agreement together with all information whether of a commercial, financial, personal or technical nature or otherwise relating in any manner to its business or affairs of the other Party as may be communicated to it hereunder or otherwise in connection with these Terms and Conditions and Cybersecurity Services Agreement and will not disclose such information to any person, firm or company (other than to its auditors and other professional advisers) or to the media, and will not use such information other than for the purposes of these Terms and Conditions and Cybersecurity Services Agreement, subject always to any prior specific authorisation in writing by the Parties concerned to such disclosure or use.

13.2. The provisions of clause 12.2 shall not apply to any information which –

13.2.1. is in the public domain other than by default of the recipient Party;

13.2.2. is obtained by the recipient Party from a bona fide third-party having the right to disseminate such information;

13.2.3. is or has already been independently generated by the recipient Party;

13.2.4. is required to be disclosed by law or the valid order of a court or governmental or other regulatory authority or agency, in which event the disclosing Party shall notify the other Party as promptly as practicable (and if possible prior to making any disclosure) and shall use its reasonable endeavours to seek confidential treatment of such information;

13.2.5. is required to be disclosed pursuant to any rules of any recognised stock exchange.

13.3. The obligations contained in this clause 14 shall endure beyond the termination of these Terms and Conditions and Cybersecurity Services Agreement without limit in time except until any confidential information enters the public domain otherwise than through default of the recipient Party.

14. NON-CIRCUMVENTION

14.1. Neither party to this Agreement shall, without the written consent of the other party, which consent shall not be unreasonably delayed or withheld, directly, indirectly or in any capacity as agent, contractor or otherwise, at any time while this Agreement is in force and for a period of 2 (two) years after termination of this Agreement for whatever reason, approach, encourage, entice, induce, solicit, or cause a third party to employ any person employed by the other party.

14.2. In the event of either of the parties ("Soliciting Party") employing the employee of the other party contrary to the provisions of 11.1, the Soliciting Party shall be obliged to effect payment of an amount equal to the total annual cost to company of the employee to the employer within 30 (thirty) days of the date of appointment of the employee by the Soliciting Party as pre-liquidated damages without prejudice to any other rights the employer may have in law vis-à-vis the Soliciting Party.

14.3. At any time prior to the expiration of this Agreement and for a period of 2 (two) years thereafter, it is expressly agreed that the identities of any individual or entity and any other third parties (including, without limitation, suppliers, customers, financial sources, manufacturers and consultants) discussed and made available by the disclosing party shall constitute Confidential Information and the receiving party or any of its affiliates or associated entity or individual shall not (without the prior written consent of, or having entered into a commission agreement with, the disclosing party):

14.4. directly or indirectly initiate, solicit, negotiate, contract or enter into any business transactions, agreements or undertakings with any such third party identified or introduced by the disclosing party; or

14.5. seek to by-pass, compete, avoid or circumvent the disclosing party from any business opportunity that relates to the Agreement by utilising any Confidential Information or by otherwise exploiting or deriving any benefit from the Confidential Information.

14.6. The receiving party covenants that any financial gain made by it, or any associated party, from a breach of this clause 11 shall be held on trust for the benefit of the disclosing party and then be transferred to a nominated account of the disclosing party, until which time such outstanding amount shall incur interest at the rate of prime plus 4% per annum. Such interest shall accrue on a daily basis from the due date until actual payment of the overdue amount, whether before or after judgment and the receiving party shall pay the interest together with the overdue amount.

14.7. Clause 14.4 does not affect the disclosing party's ability to also sue for damages should the covenants in clause 11 be violated in any way.

15. DISPUTE RESOLUTION

15.1. Any dispute, claim or disagreement arising from or relating to this Agreement shall be finally settled by arbitration in accordance with the rules for commercial arbitration of the Arbitration Foundation of Southern Africa by one arbitrator appointed in accordance with the rules.

15.2. The decision of the arbitrator may be made an order of court and nothing shall preclude either Party from access to a competent court for interim relief in the form of an interdict or order for specific performance pending the outcome of arbitration or in respect of such

arbitration. For these purposes the Parties submit to the non-exclusive jurisdiction of the South Gauteng High Court.

15.3. This Agreement shall in all respects be governed by the law of South Africa.

16. DOMICILIUM AND NOTICES

16.1. The Parties choose domicilium citandi et executandi ("domicilium") for all purposes of the giving of any notice, the payment of any sum, the serving of any process and for any other purpose arising from these Terms and Conditions the physical address, fax number or e-mail address as set out in the Cybersecurity Services Agreement.

16.2. Each Party shall be entitled from time to time, by written notice to the other/s, to vary its domicilium to any other physical address within South Africa, fax number or e-mail address.

16.3. Any notice given, and any payment made by a Party to another Party which is delivered by hand during the normal business hours of the addressee at the addressee's domicilium shall be rebuttably presumed to have been received by the addressee at the time of delivery.

16.4. Any notice given by a Party to another Party by fax or e-mail shall be rebuttably presumed to have been received by the addressee on the date of successful transmission thereof.

16.5. Notwithstanding anything to the contrary in this clause 16, a written notice or other communication actually received by a party shall be adequate notice to it notwithstanding that the notice was not delivered to its given domicilium or in the manner contemplated by the foregoing provisions of this clause 16.

17. INDEPENDENT ADVICE AND RELIANCE

17.1. Each of the Parties hereby acknowledge and agrees that –

17.1.1. It has been free to secure independent legal and other advice as to the nature and effect of all the provisions of these Terms and Conditions and Cybersecurity Services Agreement and that it has either taken such independent legal and other advice or dispensed with the necessity of doing so;

17.1.2. all of the provisions of these Terms and Conditions and Cybersecurity Services Agreement and the restrictions herein contained are fair and reasonable in all the circumstances and are part of the overall intention of the Parties in connection with these Terms and Conditions and Cybersecurity Services Agreement; and

17.1.3. it has not placed any reliance upon the advice, views and/or opinions expressed by the other of them or the other Party's independent legal, tax and other advisors in the preparation, negotiating, executing, and implementing of these Terms and Conditions and Cybersecurity Services Agreement.

18. LIMITATION OF LIABILITY

18.1. Unless otherwise provided in this Agreement, neither Party shall be liable to the other for any indirect or consequential damages.

18.2. **Nothing in this Agreement shall restrict either Party's liability for:**

18.2.1. fraud; or

18.2.2. death or personal injury caused by its negligence or intentional or wilful act; or

18.2.3. damage to real or tangible personal property caused by its gross negligence or intentional or wilful misconduct; or

18.2.4. any breach of its obligations under this Agreement in respect of confidentiality and intellectual property; or

18.2.5. any breach of a provision in terms of which it indemnifies the other Party; or

18.2.6. any other liability that cannot be excluded by law.

18.3. If a Party is in breach of any obligations under this Agreement (or any part of it) to the other Party or if any liability arises (including for negligence and breach of statutory duty) then such Party's liability to the other Party shall be limited to total charges paid in the 12 (twelve) month period prior to the date on which a claim arose, for clarity on date of occurrence of the breach.

18.4. The limitation of liability contained in this clause 18 shall apply to the fullest extent permissible in law and shall be for the benefit of the Parties and their directors, employees, its agents or any other persons for whom it may be liable in law.

18.5. Itec shall not be held liable for any damages, losses, business interruption, data exposure, unauthorized access, breach, or security incident caused by hardware failure, vendor defects, third-party delays, RMA processing times, or the temporary unavailability of the firewall or associated security services. This limitation applies irrespective of whether the failure occurs during normal operation or during RMA-related activities.

18.6. To the maximum extent permitted by South African law:

18.6.1. Itec shall not be liable for any consequential, indirect, special, or punitive damages.

18.6.2. Cybersecurity services do not guarantee the absolute prevention of breaches.

18.7. Itec is not liable for breaches caused by:

18.7.1. customer non-compliance, weak internal practices, or misconfigurations outside Itec's control;

18.7.2. third-party vendor failures, cloud attacks, or compromised Customer credentials; and

18.7.3. employee negligence, phishing, or insider threats

19. APPLICABLE LAW

19.1. All matters arising from or in connection with these Terms and Conditions, its validity, existence or termination shall be determined in accordance with any Applicable Laws and the laws for the time being of South Africa.

20. GENERAL

20.1. This document constitutes the sole record of the agreement between the Parties in relation to its subject matter and supersedes all other agreements or understandings relating to the subject matter hereof.

20.2. No Party shall be bound by any representation, warranty, promise or the like not recorded in this document.

20.3. Itec reserves the right to amend, add, vary, or novate these Terms and Conditions by notice to the Customers, which notice may be published on Itec's Online Portal in accordance with clause 1.5.

20.4. No suspension of a right to enforce any term of these Terms and Conditions and no pactum de non petendo shall be of any force or effect unless in writing and duly signed by or on behalf of the Parties.

20.5. No indulgence which a Party may grant to another party shall constitute a waiver of any of the rights of the grantor unless in writing signed by both Parties.

20.6. The Parties hereby consent in terms of section 45 of the Magistrates Courts Act 32 of 1944 to the jurisdiction of the Magistrates' Court for purposes of any proceedings in terms of or incidental to these Terms and Conditions, provided that the Parties shall have the right to institute proceedings in any division of the High Court of South Africa having jurisdiction, whereby costs shall be determined in terms of the High Court tariffs.

20.7. A certificate signed by any director or manager of Itec, whose appointment and designation need not be proved, will be prima facie proof of the Customer's indebtedness to Itec, the rate of interest payable thereon and the date from which such interest is calculated.

20.8. All costs, charges and expenses of any nature whatsoever which may be incurred by a Party in enforcing its rights in terms of these Terms and Conditions and the Cybersecurity Services Agreement, including legal costs on the scale of attorney and own client and collection commission, irrespective of whether any action has been instituted, shall be recoverable on demand from the Party against which such rights are successfully enforced and shall be payable on demand.

20.9. The Customer indemnifies and keeps indemnified Itec and its personnel against all loss, claims of whatsoever nature, damage, liability, penalty, costs (including legal costs on attorney and own client scale) and expenses suffered or incurred by Itec under contract, delict, breach of duties (statutory or otherwise) or any other basis and howsoever arising as a result of:

20.9.1. a negligent, fraudulent or wrongful act or omission by the Customer (or its personnel) and/or the User under or in relation to these Terms and Conditions or any Cybersecurity Services Agreement;

20.9.2. the Customer (or its personnel) and/or the User breaching or failing to comply (or Itec being held liable or deemed to have breached or failed to comply as a direct result of a breach or failure by the Customer) with any law;

20.9.3. any breach by the Customer and/or the User of any of the terms, conditions, representations or warranties contained in these Terms and Conditions; and/or

20.9.4. any act or omission of any third-party appointed by the Customer engaged by the Customer and/or the User.

20.10. Itec is entitled to cede and/or assign its rights and/or obligations under these Terms and Conditions without prior notice to, and/or without the prior consent of, the Customer. The Customer may not cede and/or assign any of its rights and/or obligations under these Terms and Conditions without the prior written consent thereto of Itec, which consent will not be withheld unreasonably.

20.11. The provisions of these Terms and Conditions shall be binding upon the successors-in-title and the permitted assigns of the Parties.

20.12. The Customer will not, without the written consent of Itec, directly or indirectly or in any capacity as agent, contractor or otherwise, at any time while these Terms and Conditions is in force and for a period of 2 (two) years after termination of these Terms and Conditions for whatever reason, approach, encourage, entice, induce, solicit, or cause a third-party to employ any person employed by Itec.

20.13. At any time prior to the expiration of these Terms and Conditions and for a period of 2 (two) years thereafter, it is expressly agreed that the identities of any individual or entity and any other third parties (including, without limitation, suppliers, customers, financial sources, manufacturers and consultants) discussed and made available by the disclosing Party in respect of the these Terms and Conditions, the Services and any related business opportunity shall constitute Confidential Information and the recipient Party or any of its affiliates or associated entity or individual shall not (without the prior written consent of, or having entered into a commission agreement with, the disclosing Party):

20.13.1. directly or indirectly initiate, solicit, negotiate, contract or enter into any business transactions, agreements or undertakings with any such third-party identified or introduced by the disclosing Party; or

20.13.2. or seek to bypass, compete, avoid or circumvent the disclosing Party from any business opportunity by utilising any Confidential Information or by otherwise exploiting or deriving any benefit from the Confidential Information.

20.13.3. The recipient Party covenants that any financial gain made by it, or any associated party, from a breach of clause 18.13 shall be held on trust for the benefit of the disclosing Party and then be transferred to a nominated account of the disclosing Party, until which time such outstanding amount shall incur interest at the rate of Prime plus 4% per annum. Such interest shall accrue on a daily basis from the due date until actual payment of the overdue amount, whether before or after judgment and the recipient Party shall pay the interest together with the overdue amount.

20.14. The Customer hereby confirms and warrants that, as at the date of these Terms and Conditions, its annual turnover or asset value is equal to or exceeds R 2 000 000.00 (two million Rand). Furthermore, the Customer undertakes immediately to notify Itec in writing in the event of its annual turnover or asset value dropping be-low R 2 000 000.00 (two million Rand) at any stage throughout the duration of these Terms and Conditions, failing which it will be deemed that the Customer's annual turnover or as-set value has remained above R 2 000 000.00 (two million Rand) throughout the duration of these Terms and Conditions.

20.15. The Customer hereby agrees that Itec is entitled at any time to communicate with any person to obtain and provide any information relating to the Customer's payment behaviour, credit worthiness or defaults.

20.16. These Terms and Conditions do not create a partnership, joint venture, employment or agency between the Parties and neither Party shall be liable for the debts of the other Party howsoever incurred.

20.17. All provisions in these Terms and Conditions are, notwithstanding the manner in which they have been put together or linked grammatically, severable from each other. Any provision of these Terms and Conditions which is or becomes unenforceable in any jurisdiction, whether due to voidness, invalidity, illegality, unlawfulness or for any other reason whatsoever, shall, in such jurisdiction only and only to the extent that it is so unenforceable, be treated as pro non scripto and the remaining provisions of these Terms and Conditions shall be of full force and effect. The Parties declare that it is their intention that these Terms and Conditions would be executed without such unenforceable provisions if they were aware of such unenforceability at the time of its execution.

20.18. No remedy conferred by these Terms and Conditions is intended, unless specifically stated, to be exclusive of any other remedy which is otherwise available at law, by statute or otherwise. The election of any one or more remedy by a Party shall not constitute a waiver by such Party of the right to pursue any other remedy available at law.

SCHEDULE 1: RESPONSE AND FAULT PROCEDURES

RESPONSE TIMES AND FAULT REPORTING PROCEDURES

The procedure below must be followed by the Customer when reporting a fault, incident or change request in respect of any Equipment or Service. Adherence to these procedures will ensure the best possible response and timeous resolution of any incidents or faults.

1. DEFINITIONS:

1.1. "**Resolution Time**" means the maximum time permitted to restore the Service or to provide a temporary workaround that returns the Service to operational levels, to the extent such restoration or workaround is within Itec's reasonable control. Resolution Time excludes any delays resulting from Customer-owned or unsupported equipment, Customer-caused actions, restricted access to the Site, third-party carrier or upstream network failures, cyber-security incidents, scheduled maintenance, non-redundant or single-path infrastructure, environmental or power-related issues at the Site, Customer-driven delays, or any force majeure events.

1.2. "**Response Time**" means the time from when Itec receives a fault or request to when Itec formally acknowledges it via email, ticketing system and provides a ticket reference number.

2. TERMS OF SERVICE:

2.1. The Customer's nominated Service Manager/s shall be the primary contact responsible for contacting Itec in the event of a fault, incident or change request and to receive proactive Itec outage notifications.

2.1.1. In the event of any fault, incident or change request, the customer must contact the Help Desk –

2.1.2. by email to **helpdesk@itecsupport.co.za**;

2.1.3. by telephone on 086 101 4832 (during business hours); or

2.1.4. by telephone on 010 492 7000 (Priority 1 only, after business hours).

2.2. The Customer is required to provide sufficient, accurate information when contacting the Help Desk to enable it to identify the location of the fault, the contact person on Site, the nature of the fault or incident and the Equipment or Service that is affected. All change requests must be confirmed in writing via email to **helpdesk@itecsupport.co.za**;

2.3. Once the fault, incident or change request has been logged, the Customer will receive a Service Ticket reference number from the Help Desk which must be used by the Customer when enquiring on the status of the fault, incident or change request. No fault, incident or change request will be attended to unless a call has been logged and a reference number provided.

2.4. Itec will contact the Customer to attempt to rectify the problem over the telephone or via Itec's remote assistance systems. The Customer is required to cooperate with Itec to ensure that the fault, incident or change request is repaired immediately or, alternatively, that a technician with the necessary background knowledge of the fault and the spare parts is dispatched to the Site to rectify the problem. In some instances, it may be required for photographic evidence to be provided in support of incident troubleshooting and resolution, please provide this information as and when requested.

2.5. Itec will provide feedback to the Customer on the cause of the fault, incident or change request and the resolution thereof as well as any applicable recommendations.

2.6. The various "Response Times" outlined in this Schedule are measured from the moment the Customer logs a Service Ticket with the Help Desk and receives a ticket reference number and confirmation email, up until Itec begins addressing the service request, whether remotely or onsite.

2.7. Unless otherwise provided for in a specific Cybersecurity Services Agreement and associated Schedule hereto, the Help Desk provides telephonic and remote support during business hours. However, any Service Tickets logged after 15:00 will be deemed as logged at 08:00 on the following business day. All Service Tickets logged with the Help Desk will be measured against the criteria set out in this Schedule unless the Customer agrees to after-hours support charges which will be quoted by the Help Desk on request of the Customer.

2.8. In the event that a Service Ticket falls outside the scope of Itec's services to the Customer as part of one or more Cybersecurity Services Agreements, the Service Ticket will be referred back to the customer for action/resolution and where practical, Itec will provide information to enable the Customer to action resolution with its external provider.

2.9. Service Tickets will be dealt with based on the Priority Type of the fault, incident or change request in terms of the Priority Matrix below and multiple Service Tickets of the same priority, will be dealt with on a first come first served basis.

2.10. Onsite support will be arranged at the discretion of Itec, subject to all telephonic and/or remote support efforts having been exhausted, and if applicable, the Customers acceptance of billable charges by an official purchase order and/or signed acceptance of quote prior to commencement of the support services.

3. ONSITE RESPONSE TIMES

3.1. Response times apply during business days within a 50km radius of an Itec direct service centre.

Priority Type	Radius	Response Times
Priority 1	Within 50km	Same Business Day (where possible)
	Beyond 50km	Next Business Day (incl. travel time) *
Priority 2	Within 50km	Next Business Day
	Beyond 50km	Two Business Days (incl. travel time) *
Priority 3	Within 50km	Within Two Business Days
	Beyond 50km	Three Business Days (incl. travel time) *
Priority 4	Within 50km	Within Three Business Days
	Beyond 50km	Four Business Days (incl. travel time) *

* An additional travelling charge per kilometre (based on the standard AA rate) is applicable for every kilometre outside of a 50km radius.

3.2. To expedite high priority Service Tickets, any Priority 1 Service Ticket reported via e-mail must also be followed up with a phone call from the Customer to the Help Desk as soon as the Service Ticket is logged.

3.3. The Response Times will not apply to any of the following Service Tickets logged –

3.3.1. any system additions, moves, changes and/or deletions;

3.3.2. any environmental faults not directly related to the equipment or system installed by Itec;

3.3.3. original equipment manufacturer Software maintenance subscription and/or assurance;

3.3.4. any upgrades not directly related to a system fault; or

3.3.5. total disaster recovery where all or a large portion of the Equipment is damaged. In the event of a Site disaster, Itec will assist on a Best Effort basis to restore essential services, upon the Customer's acceptance of billable charges by an official purchase order and/or signed acceptance of quote prior to commencement of the support services, as soon as is reasonably possible under the circumstances.

3.4. Notwithstanding the undertakings by Itec regarding Response Times, should the work, including travel time, extend outside of normal business hours, the Customer will be offered the option of paying an overtime surcharge and allowing work to continue to completion, or postponing the fault, incident or change request until 08:00 on the following business day. Itec will not be held liable to the Customer for any losses or damages should the Customer choose to postpone the fault, incident or change request.

4. PRIORITY MATRIX

4.1. The time referred to in the Priority Matrix in Table 1.1 below refers only to business hours.

Table 1.1 Priority matrix

Priority Type	Definition		
Priority 1	Nature of Fault	Conditions exist that cannot be prevented or avoided by a workaround or fix. The Service is severely degraded or not functioning	
	Business Operations	Critical. The Customer is completely down – all users affected	
	Response Definition	Help Desk agents respond immediately, assess the situation, escalate internally with senior resources or externally with service provider (whichever is applicable)	
	Response Time (engagement with Customer)	From time Service Ticket is logged until engagement of a Help Desk agent with the Customer	45 Minutes
	Resolution Time	The time resolution has been reached, or time has run out for specific support level before escalating to the next support level	4 Hours
	Direct Escalation Path to follow after 4 Hours	Level 3	3@iteccomms.co.za
Priority Type	**Definition**		
Priority 2	Nature of Fault	Condition exists that causes the Services to be partially inoperative. Some major functions are not working. The Services are being limited or hindered, resulting in limited functionality	
	Business Operations	Significant. High volumes of users or senior level users are affected	
	Response Definition	Help Desk agents respond using standard procedures and operating within normal supervisory management	
	Response Time (engagement with Customer)	From time Service Ticket is logged until engagement of a Help Desk agent with the customer	2 Hours
	Resolution Time	The time resolution has been reached, or time has run out for specific support level before escalating to the next support level	6 Hours
	Direct Escalation Path to follow after 4 Hours	Level 1 Level 2 Level 3	1@iteccomms.co.za 2@iteccomms.co.za 3@iteccomms.co.za
Priority Type	**Definition**		
Priority 3	Nature of Fault	Conditions exist that allow services to be used with limited functionality, users/systems are able to perform basic functions	
	Business Operations	Not Severe. Low volume and or some regular level users are affected	
	Response Definition	Help Desk agents respond using standard procedures as time allows	
	Response Time (engagement with Customer)	From time Service Ticket is logged until engagement of a Help Desk agent with the customer	4 Hours
	Resolution Time	The time resolution has been reached, or time has run out for specific support level before escalating to the next support level	12 Hours
	Direct Escalation Path to follow after 4 Hours	Level 1 Level 2 Level 3	1@iteccomms.co.za 2@iteccomms.co.za 3@iteccomms.co.za
Priority Type	**Definition**		
Priority 4	Nature of Fault	Configuration changes or less than 10% of services not functioning	
	Business Operations	Low Severity. Adds, moves, changes, scheduled maintenance	
	Response Definition	Help Desk agents respond using standard procedures as time allows	
	Response Time (engagement with Customer)	From time Service Ticket is logged until engagement of a Help Desk agent with the customer	6 Hours
	Resolution Time	The time resolution has been reached, or time has run out for specific support level before escalating to the next support level	24 Hours
	Direct Escalation Path to follow after 4 Hours	Level 1 Level 2 Level 3	1@iteccomms.co.za 2@iteccomms.co.za 3@iteccomms.co.za

SCHEDULE 2: MAINTENANCE AND WARRANTY

1. EQUIPMENT WARRANTY

1.1. The standard original manufacturer's / supplier's ("Supplier") warranty of a minimum of 12 (twelve) months will apply to the Equipment from the Delivery Date ("Warranty Period"). The warranties only apply to Equipment supplied by Itec.
1.2. The standard terms and conditions of the Supplier's warranty will apply hereto as if specifically set forth herein and is available on request.
1.3. The warranty will be void and lapse immediately if the Customer, the User and/or any unauthorized third-party performs any work on the Equipment and/or should any unauthorized and untested equipment be connected to the Equipment.
1.4. The warranty will not cover, inter alia, defects or damage resulting from accident, misuse, abuse, neglect, unusual physical, electrical or electromechanical stress, or modification of any part of the Equipment including antenna or cosmetic damage; installation, maintenance and service of the Equipment by a third-party; Equipment that has been altered or modified without proper authorization by Itec; Equipment rendered inoperative by fire, flood, lightening, or any Force Majeure event; or Equipment not run on a dedicated and grounded electrical outlet with a surge protector and/or damaged from power surges.
1.5. The Customer must log a service request with the Help Desk in terms of the Response and Fault Procedures.
1.6. In the event of Equipment failure during the Warranty Period, the Customer may either deliver the Equipment to Itec at their own cost or request Itec to collect it from the Site. Where collection is requested, standard call out, collection and travel charges will apply. Itec will then facilitate the warranty process with the supplier for the Equipment repair or replacement thereof, at Itec or the Supplier's sole discretion.
1.7. The Equipment must be in a suitable container accompanied by the Customer's sales receipt or comparable substitute proof of sale showing the date of purchase, the serial number of the Equipment and Itec's name and address.
1.8. The Supplier may, at its sole option, use refurbished or new parts or components when repairing any Equipment or replacing the Equipment. The Warranty Period on all repaired/replaced Equipment will be for a period equal to the remainder of the Warranty Period on the original Equipment.
1.9. The Customer must pay all parts, shipping, and labour charges for the repair or return of any Equipment not covered by the warranty as determined by the Supplier in its sole discretion.
1.10. Except as stipulated in the warranties herein, the Customer takes the Equipment "as is." Itec makes no representation or warranty with respect to the Equipment except those stated herein and there are no conditions, express or implied, statutory or otherwise, of any kind whatsoever with respect to the Equipment. No instruction manual shall be construed to create an express warranty of any kind whatsoever with respect to the Equipment. All implied warranties and conditions that may arise by operation of law, including, if applicable, the implied warranties of merchantability and fitness for a particular purpose; any implied warranties arising from statue, trade usage, course of dealing or course of performance warranties of title or non-infringement; design, condition, quality or performance of the product; the workmanship of the product or the components contained therein; compliance of the product with the requirements of any law, rule, specification or contract pertaining thereto, are hereby expressly excluded unless specifically contained in the warranty terms and conditions, and Itec disclaims all such warranties.
1.11. Itec shall not be liable for any damages of any kind, including incidental, special or consequential damages, loss of profits or benefits or for any and all damages resulting from the Customer's, use, or misuse of, or inability to use the Equipment or arising directly or indirectly from the use or loss of use of the Equipment or from the breach of the express warranty, or for any breach of contract or for any claim brought against the Customer by any other party. Itec makes no warranties or representations and there are no conditions, express or implied, statutory or otherwise, as to the quality, capabilities, operations, performance or suitability of any third-party software or equipment that is included with the Equipment supplied by Itec or otherwise, including the ability to integrate any such software or equipment with the Equipment.
1.12. Unless otherwise specifically covered under a specific Service Level Agreement plan, Itec will provide the Customer with a quotation for the replacement or repair of all Equipment that falls outside of the Warranty Period together with applicable call-out, travel and labour fees at Itec's then prescribed rate. Itec will supply the Equipment and applicable services on acceptance by the Customer of Itec's quotation.

2. MAINTENANCE OF EQUIPMENT AND CHARGES

2.1. Itec will provide the Customer with maintenance for Cybersecurity Equipment and/or Software supplied by Itec as per the selected Service Level Agreement type associated to the solution, and unless otherwise stated on the selected Service Level Agreement, does not include call outs, travel outside of a 50km radius and onsite labour. The Service Level Agreement will be charged on a monthly basis for the for the Initial Period and thereafter on a month-to-month basis until either party gives 90 (ninety) days' written notice of cancellation.
2.2. Should the Customer refuse to proceed with a Service Level Agreement type, the Customer acknowledges that any maintenance of Cybersecurity Equipment and/or Software is subject to the availability of Itec support and product availability and will be charged at Itec's then prescribed rates.
2.3. In circumstances where no Service Level Agreement ("SLA") is in effect, the Customer shall be liable for the Charges at Itec's the prescribed rates for any system additions, relocations, modifications, or deletions requested following the completion and acceptance of the initial scope of work. Where an SLA is in effect, such Charges shall become applicable in respect of any work, service, or request that falls outside the scope, entitlements, or response parameters defined in that SLA. All such Charges are subject to amendment from time to time at Itec's sole discretion.
2.4. Maintenance services are subject to the Customer's account with Itec being in good standing.
2.5. The maintenance Charges exclude callouts, travel beyond a 50 km radius from the nearest Itec Service Centre, onsite labour, and the replacement or supply of any Equipment. Notwithstanding the provisioning Cybersecurity Equipment and/or Software and any, where Equipment failure is not covered under the Supplier's warranty, or where the Equipment is deemed beyond economic repair, the cost of replacement Equipment shall be borne solely by the Customer. Itec shall not be liable for the replacement of any Equipment outside the applicable warranty or Service Level Agreement parameters.
2.6. Itec's maintenance charges are exclusive of VAT and are subject to change at Itec's sole discretion without prior notice.

SCHEDULE 3: MANAGED END POINT SERVICES

1. PPTA-ORG-001 — Organisation Exposure Assessment

1.1. **Service Description**: Itec shall conduct a baseline assessment of the Customer's external attack surface for the purpose of identifying exposed services, domain-level posture weaknesses, misconfigurations, and outdated technologies.
1.2. **Service Deliverables:**
1.2.1. External exposure assessment of publicly accessible systems;
1.2.2. Identification of observed vulnerabilities or misconfigurations; and
1.2.3. A risk-ranked exposure report suitable for executive consumption.
1.3. **Service Exclusions,** the following are expressly excluded for the Service in this Agreement:
1.3.1. penetration testing;
1.3.2. exploitation activities; and
1.3.3. internal network assessments.

2. PPTA-CHL-002 — CyberHeal Endpoint Automation Service

2.1. **Service Description:** Itec shall provide an endpoint-based automation service designed to identify outdated or end-of-life applications and initiate available update workflows to reduce endpoint-level exposure.
2.2. **Service Deliverables:**
2.2.1. Endpoint application inventory and versioning;
2.2.2. Automated detection of outdated, vulnerable, or unsupported software;
2.2.3. Automated initiation of supported update workflows; and
2.2.4. Periodic endpoint compliance reporting.
2.3. **Service Exclusions,** the following are expressly excluded for the Service in this Agreement:
2.3.1. manual patch deployment;
2.3.2. operating system upgrades; and
2.3.3. procurement or licensing of third-party software.

3. PPTA-DWK-003 — Dark Web Threat & Leakage Scan

3.1. **Service Description:** Itec shall conduct ongoing reconnaissance of dark web and related underground sources to identify possible exposure of the Customer's organisational data or credentials.
3.2. **Service Deliverables:**
3.2.1. Automated scanning of dark web sources against Customer authorised domains or identifiers;
3.2.2. Summary reporting of any identified exposed credentials, data, or impersonation risks; and
3.2.3. Recommendations regarding mitigation measures.
3.3. **Service Exclusions**: the following are expressly excluded for the Service in this Agreement:
3.3.1. the removal of data from third party websites or marketplaces;
3.3.2. active engagement with threat actors; and
3.3.3. incident response or remediation activities.

SCHEDULE 4: FIREWALL CONFIGURATION AND IMPLEMENTATION

1. Initial Configuration

1.1. Itec and/or its Supplier shall perform the initial configuration of the firewall to establish connectivity within the Customer's network environment.
1.2. Security Zone Definition: Itec and/or its Supplier shall define and configure all required security zones, including but not limited to internal, external, DMZ, and any additional zones specified by the Customer. Appropriate access control rules shall be applied in accordance with the approved design.
1.3. Feature Enablement: Itec and/or its Supplier shall configure VPN services, Network Address Translation (NAT), and any other required firewall features in alignment with the Customer's documented security requirements.
1.4. Logging and Monitoring: Where required, Itec and/or its Supplier shall enable system logging and monitoring capabilities to support continuous traffic analysis, incident investigation, and operational reporting.
1.5. Rule Validation: Itec and/or its Supplier shall validate all firewall rules and policies to ensure required traffic flows are permitted and all unauthorized or non-compliant traffic is denied.
1.6. Policy and VPN Verification: Itec and/or its Supplier shall verify the correct operation of all deployed security policies and any associated VPN services to ensure secure connectivity and compliance with the design.

2. Deployment and Integration Services

2.1. Firewall and CPE Integration: As part of the deployment phase, the ITEC shall integrate all firewall appliances and Customer Premises Equipment (CPE) into the Customer's environment, ensuring alignment with the approved network and security architecture.
2.2. Firewall & CPE Configuration: Itec and/or its Supplier shall configure all devices in accordance with the agreed-upon design specifications, applying optimal security settings and ensuring functional readiness of each component.
2.3. System Testing: Itec shall conduct comprehensive testing of the deployed network security architecture, including but not limited to:
  2.3.1. Firewall rule efficacy;
  2.3.2. High-availability and failover capability;
  2.3.3. End-to-end connectivity; and
  2.3.4. Security incident detection and response behavior.
2.4. Performance Tuning: Upon completion of testing, Itec and/or its Supplier shall optimize Firewall and related system configurations to ensure minimal performance degradation while maintaining maximum security posture.

3. Ongoing Support and Maintenance

3.1. Software and Firmware Updates: Itec and/or its Supplier shall apply regular software and firmware updates, including security patches, to the Firewall and associated security devices, subject to maintenance windows and approved change control and subject to Clause 6 of the Cybersecurity Agreement.
3.2. Periodic Security Audits: Itec and/or its Supplier shall conduct periodic security audits to assess the effectiveness of the firewall configuration and overall network security posture. Audit outcomes shall be documented and shared with the Customer, together with any recommended corrective actions.
3.3. General Support Services: Itec and/or its Supplier shall provide ongoing operational support for the firewall environment in accordance with the selected SLA agreed to by the Customer on the Cybersecurity Services Agreement and in line with the Cybersecurity Terms and conditions associated with this agreed SLA.