logo5.png

Supplementary Terms for the Supply of Security as a Service

NexGen Cyber shall provide Security as a Service to the Client on the terms and conditions set out in NexGen Cyber’s General Terms and Conditions and the terms and conditions of this Supplement. All definitions set out in the General Terms and Conditions shall, unless otherwise specified below, have the same meaning when used in this Supplement.

# SUPPLEMENTARY DEFINITIONS

‘Cloud-Based Utilities’ means the collection of ancillary third-party provided services, including backup, anti-Malware, and monitoring services which will be used by NexGen Cyber in support of Security as a Service.

‘Configuration’ means the configuration of the IT Equipment or component thereof, including hardware, installed software and all associated settings and / or parameters.

‘Data Centre’ means the relevant NexGen Cyber facility built to securely house IT computing systems such as servers, storage systems and network devices.

‘Data Security Event’ means a breach of the security of the Client’s infrastructure resulting in loss or damage, including loss of user-names, passwords, Personal Data; crypto-locking or other Malware-related damage.

‘Device’ means an item of IT Equipment including servers, workstations, laptop computers, tablets, mobile telephones, routers and firewalls.

‘Emergency Maintenance’ means any period of maintenance for which, due to reasons beyond its reasonable control, NexGen Cyber is unable to provide prior notice of.

‘Endpoint’ means an item of IT Equipment including workstations, laptop computers, tablets and mobile telephones.

‘End User’ means a user of the IT Equipment.

‘Hours of Cover’ means the times that the Support Desk is available to respond to Incidents, and is set out in the Service Schedule.

‘IT Equipment’ means the Devices listed on the Order and is to be covered under the terms of this Agreement.

‘IT Infrastructure’ means the IT Equipment, Local Area Network and their respective configuration.

‘Monitoring Agent’ means Software which is installed on the IT Equipment by NexGen Cyber which enables security monitoring and reporting.

‘Monitoring Services’ means NexGen Cyber’s services which enable the delivery of elements of Security as a Service.

‘Penetration Test’ means an automatic or manual check of the Client's systems configuration pertaining to cyber security which is performed by NexGen Cyber.

‘Security as a Service’ means the security services described in the Service Schedule.

‘Security Update’ means security updates provided by third-party software and hardware vendors.

‘Software’ means the software which is installed on the IT Equipment by NexGen Cyber to enable the Security as a Service.

‘Support Desk’ means NexGen Cyber’s dedicated team of qualified support specialists.

# TERM

This Agreement will come into effect on acceptance of the Client’s Order by NexGen Cyber and shall run until the RFS Date (the ‘Run-Up Period’) and following the RFS Date for the Minimum Term as set out in the Order.

This Agreement shall continue to run after the expiry of the Minimum Term (or subsequent Additional Term) for an Additional Term. The duration of the Additional Term shall be one year.

NexGen Cyber shall, not less than ninety days prior to the end of the Minimum Term or any Additional Term thereafter, notify the Client of changes to Charges and any other changes to the terms of this Agreement. In the event that:

The Client serves notice to terminate this Agreement in accordance with clause 11 of the General Terms and Conditions or clause 9 hereof, this Agreement shall terminate at the end of the Minimum Term or Additional Term thereafter;

The Client notifies NexGen Cyber of acceptance of changes, the Agreement shall continue in force for an Additional Term;

The Client fails to notify NexGen Cyber of acceptance of changes and fails to serve notice to terminate, such failure to notify NexGen Cyber shall imply that the changes have been accepted and the Agreement shall continue in force for an Additional Term.

# PROVISION OF SERVICES

Security as a Service is provided to merely mitigate the cyber vulnerability of the IT Equipment.

The Service Components to be provided under the terms of this Agreement are set out on the Order and described in the Service Schedule.

Security as a Service will be provided by NexGen Cyber remotely.

For the avoidance of doubt, Security as a Service does not include IT systems support, hardware maintenance or local area network support.

NexGen Cyber shall use reasonable endeavours to provide the Security as a Service during the Hours of Cover described in the Service Schedule.

During the term of this Agreement, NexGen Cyber shall be entitled to make alterations to the Configuration of the IT Equipment. Such alterations may result in temporary disruption to the availability of the IT Equipment and NexGen Cyber will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

NexGen Cyber does not make any representations as to the accuracy, comprehensiveness, completeness, quality, currency, error-free nature, compatibility, security or fitness for the Client’s purpose of the Cloud-Based Utilities.

During the term of this Agreement, NexGen Cyber shall be entitled to make alterations to the Configuration of the Cloud-Based Utilities. Such alterations may result in temporary disruption to the availability of the Cloud-Based Utilities and NexGen Cyber will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

NexGen Cyber cannot guarantee and does not warrant that the Security as a Service shall result in the IT Equipment operating free from interruptions or will be free from the risk of Malware infection or other Data Security Event.

A number of the Security as a Service include Monitoring Services; and

NexGen Cyber shall use reasonable endeavours to provide the Monitoring Services 24 x 7 x 365;

NexGen Cyber cannot guarantee and does not warrant that the Monitoring Services will be free from interruptions, including:

Interruption of the Monitoring Services for operational reasons and temporary degradation of the quality of the Monitoring Services;

Interruption of the connection of the Monitoring Services to other network services provided either by NexGen Cyber or a third party; and

Any such interruption of the Monitoring Services referred to in this sub-clause shall not constitute a breach of this Agreement.

# ACCEPTABLE USE

The Client agrees to use the IT Equipment in accordance with the provisions of this Agreement, any relevant service literature and all other reasonable instructions issued by NexGen Cyber from time to time.

The Client agrees to ensure that the IT Equipment is not used by its End Users to:

Post, download, upload or otherwise transmit materials or data which is abusive, defamatory, obscene, indecent, menacing or disruptive;

Post, download, upload or otherwise transmit materials or data uploads or make other communications in breach of the rights of third parties, including but not limited to those of quiet enjoyment, privacy and copyright;

Carry out any fraudulent, criminal or otherwise illegal activity;

Act in any manner which brings NexGen Cyber’s name into disrepute;

Knowingly make available or upload file that contain Malware or otherwise corrupt data;

Falsify true ownership of software or data contained in a file that the Client or End User makes available via IT Equipment;

Falsify user information or forge addresses;

Act in any way which threatens the security or integrity of the IT Equipment, including the download, intentionally or negligently, of Malware;

Violate general standards of internet use, including denial of service attacks, web page defacement and port or number scanning;

Connect to the IT Equipment insecure equipment or services able to be exploited by others to carry out actions which constitute a breach of this Agreement including the transmission of unsolicited bulk mail or email containing infected attachments or attempts to disrupt websites and/or connectivity or any other attempts to compromise the security of other users of our network or any other third-party system.

The Client acknowledges that it responsible for all data and/or traffic originating from the IT Equipment.

The Client agrees, subject to the provisions of sub-clause 10.13 of the General Terms and Conditions, to indemnify NexGen Cyber against all costs, damages, expenses or other liabilities arising from any third-party claim which arises from the Client’s breach of this clause 4.

# CLIENT’S OBLIGATIONS

During the term of this Agreement, the Client shall:

Pay all agreed additional Charges levied by NexGen Cyber.

Ensure that user-names, passwords and personal identification numbers are kept secure.

Accept that is the Client’s sole responsibility to take all reasonable steps to prevent the introduction of Malware into the IT Equipment.

Be solely responsible for ensuring compliance with the terms of licence of any Software that is a component of the IT Equipment that has been provided by the Client.

Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the Security as a Service.

Be responsible for implementing (or requesting that NexGen Cyber implements) NexGen Cyber’s recommendations and acknowledges if that such recommendations are not implemented, it may be impossible for NexGen Cyber to provide the Service, and failure to implement NexGen Cyber’s recommendations will be deemed a material breach of this Agreement.

Warrant that information provided to NexGen Cyber during any discovery or audits shall be provided honestly and accurately by person(s) who are authorised and qualified to provide the requested information.

Within ten Working Days of any request for an appointment made by NexGen Cyber for the purpose carrying out Penetration Tests, agree an appointment date.

Notify NexGen Cyber immediately and in any event with not less than one Working Day beforehand if the Client wishes to cancel a previously made appointment.

Prior to the agreed date for any Penetration Test, provide to NexGen Cyber the necessary administration credentials to allow it to carry out the test.

Use by the Client of certain Cloud-Based Utilities is subject to third-party vendor’s terms and conditions and the Client hereby agrees to be bound by such terms and conditions.

# NEXGEN CYBER’S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Client of its obligations hereunder, NexGen Cyber shall:

Provide the Security as a Service set out in the Order and described in the attached Service Schedule, subject to any service limitations set out on the Order and herein.

During the Hours of Cover, make available a Support Desk that shall provide support and guidance in the use of the Services and manage the resolution of any Incidents that arise in the Security as a Service.

Be responsible for the licensing and installation of Monitoring Agents and all Software that NexGen Cyber installs on the IT Equipment.

# Clause Intentionally Unused

# GENERAL

The installation of Security Updates may limit the availability of the IT Equipment. NexGen Cyber will use reasonable endeavours to schedule Security Updates to minimise disruption to the Client; and

The Client shall test its IT Equipment once the Security Update has been applied to ensure it has not impacted their functionality. If a Security Update has an adverse effect on the operation of the Software, NexGen Cyber will where possible remove the Security Update, in agreement with the Client;

NexGen Cyber may be unable to provide prior notice of Emergency Maintenance to the Cloud-Based Utilities, but will endeavour to minimise the impact of any such maintenance on the Client.

If NexGen Cyber carries out work in response to an Incident reported by the Client and NexGen Cyber subsequently determines that such Incident was not in the Security as a Service or caused by any act or omission by NexGen Cyber, it shall be entitled to charge the Client at its prevailing rate.

In the event of persistent breach of clause 4.2.8, NexGen Cyber shall be entitled to:

Charge the Client at its prevailing rate for the removal of Malware;

Terminate this Agreement.

If the Client suffers a Data Security Event and subsequently requests assistance from NexGen Cyber, it is the Client’s sole responsibility to ensure that such request for assistance will not breach the terms of any cyber-insurance policy that the Client has in place, prior to requesting assistance from NexGen Cyber.

If the Client is contacted by NexGen Cyber and requested to make a change to the Configuration of the IT Equipment, it is the Client’s sole responsibility to verify the identity of the requestor prior to carrying out the requested change.

The Client is responsible for the licensing of all other software, including Windows operating systems, Microsoft Office and line of business applications which have not been supplied by NexGen Cyber under the terms of any other agreement between NexGen Cyber and the Client.

# TERMINATION

In addition to the provisions of clause 11 of the General Terms and Conditions, this Agreement may also be terminated:

By either party by giving the other not less than ninety days’ notice in writing to terminate at the end of the Minimum Term or at any time thereafter.

By the Client by giving thirty days’ notice in writing if NexGen Cyber makes changes to the Services which are materially adversely affect the Client (for the avoidance of doubt, not including changes to Charges) PROVIDED THAT such notice is given within twenty eight days of the effective date of the change(s).

By NexGen Cyber at any time if it can no longer provide the Services;

By the Client by reason of NexGen Cyber’s un-remedied or repeated breach of the terms of this Agreement.

# CHARGES AND PAYMENT

Invoices for periodic Charges shall be raised in advance of the relevant period. The invoicing period is set out on the Order.

The periodic Charges will be based on the number Devices set out on the Order and as amended from time to time.

In addition to Charges contemplated in sub-clause 10.2, NexGen Cyber shall be entitled to charge the Client for:

The ad hoc supply of any Services that are requested by the Client but not set out on the Order;

Reasonable expenses;

Onsite visits that extend beyond the end of the Working Day;

NexGen Cyber shall commence charging for the Security as a Service from the RFS Date, regardless of the date on which the Client commences use of the Security as a Service. If the RFS Date does not correspond with NexGen Cyber’s invoicing period as set out in the Order, NexGen Cyber shall charge the Client at a pro-rata rate for the first invoicing period.

On-boarding and usage-based Charges, including Charges made for use of Services in excess of any pre-paid amounts, will be invoiced in arrears.

The Client acknowledges that the Charges for the Minimum Term are calculated by NexGen Cyber in consideration inter alia of the setup costs to be incurred by NexGen Cyber and the length of the Minimum Term offered.

If, during the term of this Agreement the Client requires additional Devices to be added to the schedule of IT Equipment, the Client shall raise a supplementary Order to cover the additional equipment and NexGen Cyber shall promptly provide a quotation for the additional Services.

The Client agrees that it shall be liable for termination Charges in the event that this Agreement is terminated by:

The Client terminating this Agreement for convenience prior to the end of the Minimum Term or any Additional Term whereupon the Client shall be liable for the fixed periodic Charges payable for the remainder of the current term and any outstanding installation Charges;

The Client terminating this Agreement for convenience during the Run-Up Period, whereupon the Client shall be liable for all set-up costs and cancellation costs incurred by NexGen Cyber up to the date that NexGen Cyber received notice of the Client’s intention to terminate;

NexGen Cyber terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Client’s un-remedied breach of the terms of this Agreement, whereupon the Client shall be liable for the fixed periodic Charges payable for the remainder of the current term and any outstanding installation Charges.

The Client shall not be liable for termination Charges if a right of termination arises under the provisions of sub-clauses 9.1.2 to 9.1.4.

# LIMITATIONS AND EXCLUSIONS

The following are not included under the terms of this Agreement:

IT policy and template design;

Compliance Incidents;

IT Equipment support or maintenance;

Changes to the Configuration of the IT Equipment other than those covered by the Security as a Service;

On-Site support;

Remediation, Malware removal or data restoration following a Malware attack.

NexGen Cyber, if requested, may provide any of the excluded services listed above, and will charge for so doing at its prevailing rate.

# EXCLUSION OF LIABILITY

The Client acknowledges and agrees that:

Any recommendations or advice provided by NexGen Cyber is intended to merely mitigate the Client’s cyber vulnerability and is provided without any warranty that that on implementing such recommendations or advice, the Client will be free from cyber security vulnerabilities or their attendant risks;

NexGen Cyber shall not be liable for any liabilities, losses, damages, costs, fines or expenses that result directly or indirectly from recommendations or advice provided by NexGen Cyber unless such recommendation or advice was either given negligently or was negligently withheld.

The Client agrees that NexGen Cyber shall not be liable for any actions, losses damages, judgements, legal fees, costs, fines, claims or expenses incurred by the Client or legal proceedings which are brought or threatened against the Client by a third party in the event of:

Any breaches by the Client of any Data Protection Legislation;

Any security breach of or vulnerability in the Client’s systems and processes.

All Security as a Service are provided on an ‘as is’ basis, without warranty, guarantee of fitness for purpose or suitability for the Client’s purpose; and

NexGen Cyber shall not be liable for any damages or costs arising from a failure of any component of the Security as a Service, including failure to detect Malware, Data Security Events or the requirement for Security Updates unless such failure is caused by the negligence of NexGen Cyber.

Security Updates are supplied by NexGen Cyber-authorised software vendors and not NexGen Cyber. NexGen Cyber will use reasonable endeavours to prevent a Security Update causing an adverse reaction with any particular IT Equipment configuration, but NexGen Cyber shall not be liable for any disruption resulting from the installation of Security Updates. In such circumstances, NexGen Cyber’s sole responsibility will be to de-install the Security Update or roll back to an appropriate restore point to resolve the Incident.

The Client acknowledges and agrees that:

There is a small risk that Penetration Tests carried out by NexGen Cyber may cause problems in the Client’s IT systems, including routers and / or firewalls ceasing to function correctly and database and storage access Incidents;

The testing of the Client’s IT systems for correct functioning after NexGen Cyber’s Penetration Tests and any necessary reconfiguration, and any associated costs shall be the Client’s sole responsibility;

Whilst NexGen Cyber warrants that it shall use reasonable care during the execution of Penetration Tests, NexGen Cyber shall not be liable for any losses or damage which arise either directly or indirectly from its access to the Client’s IT Infrastructure.

The provisions of sub-clauses 12.1, 12.2 and 12.3 shall survive the termination of this Agreement in perpetuity.

Service Schedule

This paragraph summarises all of the Service Components that NexGen Cyber provides under Security as a Service. The individual Service Components to be provided to the Client under the terms of this Agreement are set out on the Order.

# Basic Security Awareness Training

Basic Security Awareness Training is based on an initial online questionnaire, which identifies individual End User’s security vulnerabilities and then provides individual tailored training programs. The service also provides:

* Customised simulated phishing campaigns which can be run quarterly
* Dark web monitoring, which checks for email addresses which include the Client’s top level domain name
* Policy management, providing customisable templates for a variety of policy areas and the management of their distribution, End User acknowledgement and periodic refresh

# Password Manager

NexGen Cyber’s Password Manager provides the following functionality:

* Cloud based for maximum flexibility
* Encrypted vault
* Password generator
* Multi-platform support
* Auto-fill
* Browser extensions
* Administration tools
* Multi factor authentication

# Endpoint Security Service

NexGen Cyber’s Managed Next Generation Anti-Malware Service provides full Security Operations Centre (‘SOC’) supported Endpoint monitoring and threat detection to identify active threats and remediate attacks. Using advanced artificial intelligence and machine learning, NexGen Cyber rapidly identifies and halts the most sophisticated attacks, minimising harm and reducing risk to the Client’s Endpoints. In more extreme cases such as ransomware, the SOC will roll back to restore system and data access.

The service includes containment and remediation elements, thus the Client should ensure that this service does not conflict with the provisions of any cyber-insurance policy that is held by the Client prior to subscribing to this service.

This service is provided under the terms of this Agreement and additionally under the terms of business of SentinelOne.

# Email Protection Service

The Email Protection Service provides cloud-based protection at the Client’s email perimeter and inside the Client’s network and organisation. The Email Protection Service includes:

* Malware scanning
* Spam filtering
* Content filtering
* Outbound filtering
* Imposter (business email compromise) protection
* Credential theft protection
* URL defence (sandboxing)
* Social media account protection

# Security Monitoring and Management

NexGen Cyber will install its Monitoring Agents on the Devices set out on the Order to enable pro-active monitoring for Security Threats. The Monitoring Agents will alert NexGen Cyber to any Security Threats or potential Security Threats as they arise. The Monitoring Agents will monitor Devices and automatically resolve potential Security Threats whenever possible. NexGen Cyber shall respond to any alerts that cannot be automatically resolved during Support Desk Hours of Cover in a manner that is appropriate to the severity of the threat, whilst aiming to minimise disruption to the availability of the IT Equipment. NexGen Cyber shall:

* Automatically detect missing updates and deploy security patches to Endpoints and Servers
* Manage software and updates distribution
* Provide remote support
* Receive alerts, run reports on available updates, processes, and configurations
* Perform maintenance on the IT Equipment, even when the End User is unavailable
* Run commands, PowerShell scripts, reboot computers, and restart services remotely as required

# Backup Service for Microsoft 365 and Azure

NexGen Cyber’s Backup Service for Microsoft 365 and Azure protects the Client against loss of data that is held within Microsoft’s cloud infrastructure. Unexpected data loss can typically be due to user error or occur if an End User subscription expires, and NexGen Cyber’s service, in addition to providing the Client with additional control over its data, mitigates the risk of such data loss.

NexGen Cyber provides a number of backup and recovery options. The options selected are set out on the Order. Options include:

* Cloud backup at NexGen Cyber’s Data Centre
* Backup to a resilient backup appliance which is located at the Client’s Site, which can be provided by NexGen Cyber or the Client.
* Backup to the Client’s nominated Data Centre

Backups can be made at image (server, virtual server or endpoint) or file / folder level.

Backups are encrypted at rest and during transmission.

NexGen Cyber will back-up the Client’s Microsoft 365 data based on the number of End Users and storage capacity set out on the Order; backup data is stored NexGen Cyber’s Data Centre.

Microsoft 365 backups include:

* OneDrive file and folder data backups (documents), per End User
* Exchange data, including emails, email attachments, notes, deleted items, contacts (excluding photographs), tasks and calendar events (including attendees, recurrence, attachments and notes)
* SharePoint primary, custom, group and team site collections; folders, document libraries and sets; site assets, templates and pages
* Groups (including conversations, plans, files, sites and calendar)
* Teams (including wiki and chat)
* Contacts, tasks and calendars

Backup frequency and retention periods are set out on the Order.

The Backup and Recovery Service is fully managed by NexGen Cyber.

The backup system will automatically notify NexGen Cyber of backup success or failure.

Data restoration:

* Data restores will only be initiated by NexGen Cyber when requested by an authorised representative of the Client
* NexGen Cyber will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level) requested by the Client
* NexGen Cyber will use reasonable endeavours to restore data to the location that is specified by the Client
* Restores can be made at file, mailbox, Sharepoint Site or virtual server level.

Whilst NexGen Cyber shall execute automatic backups and monitor the performance of the backup service 24 x 7 x 365, NexGen Cyber will carry out the following activities during the Hours of Cover:

* Respond to Client requests for data restores
* Respond to and investigate any Incidents that arise in the service which cannot be remediated automatically, whether raised by the Client or by NexGen Cyber’s Monitoring Agents

Test Data Restore

In response to requests from the Client, NexGen Cyber will perform occasional test restores of backed-up data to ensure that backups are functioning correctly. This will be implemented by NexGen Cyber contacting the Client to agree a test target (for example a mailbox or SharePoint Site) and carrying out the test restore at an agreed time. NexGen Cyber will charge for providing Test Data Restores at its prevailing rate.

# Mobile Device Management

Mobile device operating system support and management is provided via a NexGen Cyber-supplied Microsoft InTune subscriptions or other NexGen Cyber-supplied MDM software subscription. Mobile Device Management includes:

* Enrolment of devices and End Users
* Publishing security settings, certificates and profiles to devices
* Resource access control
* Monitoring and management, including measuring and reporting device compliance and app inventory
* Publishing mobile apps to devices
* Configuration of email applications
* Securing and removal of corporate data

Mobile Device Management does not include the publishing or management of anti-Malware software or hardware support for physical devices.

# Advanced Security Awareness Training

NexGen Cyber’s Advanced Security Awareness Training includes a number of services which are targeted at increasing staff awareness of cyber security threats and how to mitigate them. Advanced Security Awareness Training is a recurring service under which NexGen Cyber will provide:

* Access to a wide range of cyber training materials for all staff
* Monthly random staff phishing simulations
* Regular IT security review and reports
* Access to staff security awareness assessments
* Reporting of learner assessments, scorecards, etc
* Additionally chargeable, tailored ‘spear-phishing’ simulations can be provided at the Client’s request

# Advanced Password Manager

NexGen Cyber’s Advanced Password Manager provides the following functionality:

* Cloud based for maximum flexibility
* Encrypted vault
* Password generator
* Multi-platform support
* Auto-fill
* Browser extensions
* Administration tools
* Multi factor authentication
* Single sign on support for a wide range of applications

# Advanced Email Protection Service

The Advanced Email Protection Service provides cloud-based protection at the Client’s email perimeter and inside the Client’s network and organisation. The Email Protection Service includes:

* Malware scanning
* Spam filtering
* Content filtering
* Outbound filtering
* Imposter (business email compromise) protection
* Data loss prevention
* URL defence (sandboxing)
* Attachment defence (reputation-based)
* Attachment defence (sandboxing)
* Email Encryption
* Social media account protection
* Emergency inbox (30 days)
* Email spooling
* Instant replay
* Tamper-proof offsite archive
* Search and discovery
* Unlimited storage (10 year archive)

# Mobile Security

NexGen IT’s Mobile Security service gives the Client direct insight into the threats that can affect its employees’ mobile devices. The service protects both Android and iOS devices and the cloud-based dashboard that provides immediate visibility and analysis of mobile-borne threats. The service works either in standalone mode or layered on a Mobile Device Management service. The service provides a privacy-friendly, lightweight security app for iOS and Android that helps to block mobile threats before they can harm the Client’s business.

Features of the service include:

* Quick and easy set up with zero-touch deployment and one-touch enrolment for MDM-managed devices.
* App and device threats that are monitored (Android) include:
  + Malware
  + Screen recording
  + Leaky apps
  + Camera/Microphone access
  + App permission abuse
  + OS exploits
  + Vulnerable configuration
* Network threats that are monitored (Android & iOS) include∷
  + Man-in-the-Middle at tacks
  + Phishing
  + Malicious proxies
  + Malicious web scripts
  + Unsecured Wi-fi
  + Weak Wi-fi security

# Security Assessment and Vulnerability Management

Nexgen Cyber’s Security and Vulnerability Management service provides a number of services:

* Asset Discovery

Asset discovery uses several protocols to discover and probe network assets, and by leveraging several sources of ongoing vulnerability information, helps to detect vulnerabilities in the Client’s Devices.

* Active Directory Assessment

Active Directory assessments help to identify mis-configurations, weak policies and privileged user access.

* External IP Scans

External IP scans help detect open ports, protocols, and named vulnerabilities in public-facing network equipment such as web servers and firewalls.

* Compliance Scanning

Compliance scanning verifies compliance of the Client’s IT Infrastructure with a wide range of common cyber-security compliance standards that make up the foundation of a strong cyber-security strategy.

* Application Patching

Application Patching remediates the vulnerability associated with un-patched software by patching third-party Windows applications. This reduces risk exposure and helps safeguard the Client’s IT Infrastructure.

* Application Baseline

Application baseline scans the Client’s IT Infrastructure to detect inconsistencies between the installed base and the documented baseline and provides a report.

# Mobile Device Management and Conditional Access

Mobile device operating system support and management is provided via a NexGen Cyber-supplied Microsoft InTune subscriptions or other NexGen Cyber-supplied MDM software subscription. Mobile Device Management includes:

* Enrolment of devices and End Users
* Publishing security settings, certificates and profiles to devices
* Resource access control
* Monitoring and management, including measuring and reporting device compliance and app inventory
* Publishing mobile apps to devices
* Configuration of email applications
* Securing and removal of corporate data
* Conditional Access for Exchange, Microsoft 365 and Microsoft 365 apps on mobile device

Mobile Device Management does not include the publishing or management of anti-Malware software or hardware support for physical devices.

# Zero Trust Protection

NexGen Cyber’s Zero Trust Protection provides a suite of services that are designed to mitigate risk of cyber attack to the Client’s IT Infrastructure.

By defining how applications can interact with each other, and by controlling what resources applications can access, such as networks, files, and registries, Zero Trust Protection helps to prevent file-less Malware and software exploits, including:

* Protecting data from malicious behaviour
* Preventing file-less Malware and limit damage from application exploits
* Defining how applications integrate with other applications
* Preventing applications from interacting with other applications, network resources, registry keys, and files
* Preventing applications from interacting with built-in tools such as PowerShell, Command Prompt and RunDLL
* Preventing built-in tools from accessing file shares

Whitelisting has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, whitelisting provides control over which software, scripts, executables, and libraries can run on the Client’s IT Infrastructure. This approach not only stops malicious software, but it also stops other unpermitted applications from running and therefore mitigates cyber threats.

Zero Trust Protection provides an advanced storage control solution that protects information by enabling the Client to control the flow and access of data. The Client can choose what data can be accessed, or copied, and the applications, users, and Devices that can access the data. Storage control allows the Client to:

* Choose how data is accessed
* Visualise a full audit of all file access on USB, Network, and Local Hard Drives
* Restrict or deny access to external storage, including USB drives, network shares, or other devices
* Approve for a limited amount of time or permanently
* Restrict access to specific file types
* Limit access to a Device or file share based on the application
* Enforce or audit the encryption status of USB hard drives and other external storage

Elevation control enables End Users to run selected applications as a local admin and remove local admin permissions without stopping productivity. Elevation control provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their End Users, whilst allowing them to run individual applications as an administrator. Key Capabilities of Elevation control include:

* Providing complete visibility of administrative rights
* Providing the ability to approve or deny an End User’s administrator access to specific applications within an organization even if the End User is not a local administrator
* End Users can request permission to elevate applications and add notes to support their requests
* Allows setting durations for how long End Users are allowed access to specific applications by granting either temporary or permanent access
* Ensuring that once applications are elevated, End Users cannot jump to infiltrate connected applications within the network

Network access control provides cloud-managed Endpoint and server firewall functionality with dynamic access control lists to block unwanted network traffic. Network access control allows total control of inbound traffic to the Client’s protected Devices. Key capabilities of network access control include:

* The ability to configure network access to Endpoints using global and granular policies
* A centralized view of Endpoint policies across the Client’s IT Infrastructure

# Penetration Testing

NexGen Cyber’s Penetration Testing service provides a simulated internal and external cyber attack against the Client’s IT Infrastructure, which tests for exploitable vulnerabilities, including cross-site scripting and SQL injection. Each test is customised to attempt to breach the IT Infrastructure and a sample of the Client’s applications. At the conclusion of the test, the results will be analysed by NexGen Cyber and reported to the Client, along with recommendations for addressing any discovered vulnerabilities. The Penetration Testing service does not include the remediation of any vulnerability that is discovered.

# Support Desk

The Support Desk provides a means of contact with NexGen Cyber, for the reporting Incidents within the Services provided under this Agreement.

The Client shall report Incidents by one of the following methods:

* By email to NexGen Cyber’s Support Desk: technical@nexgencyber.co.uk
* By telephone to NexGen Cyber’s Support Desk: 0204 566 6000

The Support Desk is available between the hours of 9am to 5pm Monday to Friday, excluding bank and public holidays. The Client may however send emails at any time.

NexGen Cyber’s Support Desk does not provide:

* “How to” advice
* Remediation of any security-related Incidents that are identified by the Services and are not remediated as per the relevant Service Component that is set out on the Order
* Onsite Support
* Any excluded services listed in sub-clause 11.1

# Complaint Handling

If dissatisfied with any Services-related matter, the Client should make a complaint using the following escalation path. If the complaint remains unresolved, the Client should escalate to the next level in the escalation path.

| Escalation Level | Role | Contact Details |
| --- | --- | --- |
| 1 | Chief Technology Officer | mhardcastle@nexgencyber.co.uk |
| 2 | Chief Executive Officer | srosemeyer@nexgencyber.co.uk |

Formal complaints will be responded to within three Working Days.