Acceptable Use Policy

This Acceptable use policy identifies activities that you are prohibited from engaging in when using MaTK IT Solutions Services ("Services" or in the case of an individual service, "Service"), which includes any Service that links to this Acceptable use policy.

1. Purpose and Status of this Policy

1.1 This Acceptable Use Policy ("AUP") establishes the requirements for lawful, responsible and secure use of the services supplied by ManTK IT Solutions (ManTK) ("ManTK", "we", "us" or "our").

1.2 The AUP is intended to protect customers, end users, third parties, ManTK infrastructure and the broader internet ecosystem against misuse, unlawful conduct, security threats and service disruption.

1.3 This AUP supports ManTK's obligations as a member of the Internet Service Providers' Association of South Africa ("ISPA") and must be read with the applicable customer agreement, service schedule, privacy policy and any specific security, hosting or support terms.

1.4 Nothing in this AUP permits conduct that is unlawful under South African law or any other law applicable to the customer's use of the services.

2. Scope and Application

2.1 This AUP applies to every customer, customer administrator, employee, contractor, agent, end user or other person who accesses, uses, administers or benefits from a ManTK service through a customer account or customer-controlled environment.

2.2 Customers are responsible for ensuring that their authorised users comply with this AUP and for promptly addressing any misuse arising from systems, domains, mailboxes, websites, hardware or endpoints under their control.

2.3 The AUP applies to the following ManTK services, where contracted or supplied:

Service Area	Services Covered by this AUP
Hosting / Cloud Services	Email hosting; website hosting on ManTK-hosted infrastructure; server hosting where the customer's hardware is hosted on the ManTK network or at a ManTK-controlled facility.
Security Services	Firewall-related services; content filtering; endpoint security; and general security consulting.

3. Agreement to and Responsibility for Compliance

3.1 By ordering, accessing, using or continuing to use a ManTK service, the customer agrees to comply with this AUP and to ensure compliance by all users and systems operating through or in connection with the service.

3.2 The customer remains responsible for all activity undertaken through its services, accounts, hosted environments, hosted hardware, email domains, websites, endpoint agents or credentials, unless the customer promptly reports unauthorised access and cooperates with reasonable investigation and containment measures.

3.3 A breach of this a may result in investigation, restriction, suspension or termination of the affected service in accordance with this AUP and the applicable customer agreement.

4. General Acceptable Use Requirements

4.1 Customers may use the services only for lawful business or personal purposes that are consistent with the service description, the applicable agreement and this AUP.

4.2 Customers must take reasonable steps to keep their accounts, systems, websites, mailboxes, servers and endpoints secure, including using appropriate access controls, maintaining supported configurations and notifying ManTK of security incidents that may affect services supplied by ManTK.

4.3 Customers must not use, attempt to use, or permit the use of the services in any manner that:

4.3.1 commits, facilitates, promotes or assists any criminal, illegal, unlawful, fraudulent or deceptive act;

4.3.2 infringes or misappropriates any intellectual property, privacy, confidentiality, contractual or other rights of another person;

4.3.3 interferes with, disrupts, damages, disables, overloads or degrades any ManTK service, network, system, equipment, security control or any third-party system;

4.3.4 circumvents, disables or defeats access controls, security mechanisms, monitoring controls or technical restrictions without proper authority;

4.3.5 exposes ManTK, its customers or any third party to material security, legal, regulatory or reputational risk; or

4.3.6 breaches any service agreement, service-specific terms or lawful instruction issued in relation to a service.

5. Prohibited Content and Unlawful Material

5.1 Customers must not use the services to host, store, transmit, publish, display, link to or distribute content where doing so is unlawful or where the customer lacks the necessary rights or authority.

5.2 Prohibited content includes content or material that:

5.2.1 infringes copyright, trade marks, patents, trade secrets or other intellectual property rights;

5.2.2 constitutes unlawful harassment, intimidation, threats, defamation, fraud, impersonation or deceptive conduct;

5.2.3 is unlawfully discriminatory, hateful or incites violence or criminal conduct;

5.2.4 contains or facilitates unlawful access to personal information, confidential information, authentication credentials or payment information;

5.2.5 constitutes unlawful sexual abuse material or any other unlawful content involving children; or

5.2.6 is the subject of a lawful take-down notice, court order, regulatory direction or other binding instruction requiring restriction or removal.

5.3 Where ManTK receives a valid take-down notice or lawful direction affecting hosted or transmitted content, ManTK may restrict access to, remove or disable the affected material in accordance with applicable legal and ISPA processes.

6. Email Hosting, Messaging and Spam

6.1 Email hosting services must be used in a manner that protects recipients, mail infrastructure and domain reputation from abuse.

6.2 Customers must not send, cause to be sent, or assist in sending unsolicited bulk email, spam, unlawful direct marketing communications, phishing messages, malicious attachments, deceptive messages or messages that unlawfully conceal or falsify sender identity.

6.3 Where direct marketing email is lawfully permitted, the customer must ensure that communications comply with applicable legal requirements, accurately identify the sender, provide a functional opt-out or unsubscribe mechanism where required, and promptly honour valid opt-out requests.

6.4 Customers must not operate open mail relays, use compromised mailboxes, deliberately bypass mail filtering, forge headers, spoof sender information without lawful authority, or use the email service to distribute malware or collect credentials.

6.5 Customers must implement reasonable mailbox security controls appropriate to their environment, including strong authentication practices, protection of administrative accounts and prompt reporting of suspected mailbox compromise.

6.6 ManTK may apply technical controls to protect email services and recipients, including filtering, rate-limiting, temporary blocking, quarantining suspected malicious email or suspending compromised mailboxes, where reasonably required to mitigate abuse or security risk.

7. Website Hosting and Server Hosting

7.1 Customers using website hosting or hosting customer-owned servers on the ManTK network are responsible for the lawfulness, security and administration of their hosted content, applications, devices, operating systems, software, user accounts and data, except to the extent expressly assumed by ManTK in a written service agreement.

7.2 Customers must not use hosted websites or servers to:

7.2.1 host or distribute unlawful material, malicious code, phishing pages, fraudulent payment pages, credential-harvesting pages or deceptive websites;

7.2.2 operate command-and-control infrastructure, botnets, malicious redirectors, exploit delivery infrastructure, unauthorised cryptocurrency mining or other harmful computational activity;

7.2.3 conduct unauthorised vulnerability scanning, intrusion attempts, denial-of-service attacks, password attacks, exploitation or interference against ManTK or third-party networks or systems;

7.2.4 provide anonymous or uncontrolled services that materially increase abuse risk, including open proxies, open resolvers or open relays, unless specifically authorised and appropriately secured; or

7.2.5 consume excessive network, compute, storage, power or operational resources in a manner that materially impairs service availability or other customers' legitimate use.

7.3 For customer-owned hardware hosted on a ManTK network or facility, the customer must ensure that the hardware is safely configured, properly maintained, legally operated and used only for contracted purposes. Physical access, equipment changes and removal of equipment remain subject to applicable service and facility controls.

7.4 Where a hosted website or server is compromised or creates a security or operational threat, ManTK may require remediation, isolate the system, restrict network access, block malicious traffic or suspend the affected service to limit harm.

8. Firewall, Content Filtering and Endpoint Security Services

8.1 ManTK may provide security services intended to assist customers in reducing risk, managing exposure or enforcing approved security policies. The customer remains responsible for determining its security requirements, permitted business use, user communications and legal or regulatory obligations, unless otherwise agreed in writing.

8.2 Customers must not use security services to perform unlawful surveillance, unlawfully intercept communications, unlawfully monitor individuals, improperly restrict lawful rights, or access data without a legitimate purpose and appropriate authority.

8.3 For firewall-related services, customers must provide accurate authorised requirements and must not request firewall configurations intended to facilitate unlawful activity, bypass controls without authority or deliberately expose systems to abuse.

8.4 For content filtering services, customers are responsible for configuring or approving filtering categories and rules appropriate to their organisation and for using filtering capabilities in a transparent and lawful manner. Filtering reduces risk but cannot guarantee that all harmful or inappropriate content will be blocked.

8.5 For endpoint security services, customers must not remove, disable, tamper with, bypass or interfere with security agents, detection rules, telemetry collection or remediation actions without authority and coordination with ManTK where the service is managed by ManTK.

8.6 Customers must promptly notify ManTK where a security control supplied or monitored by ManTK is suspected to be compromised, disabled, misconfigured or generating material false positives or service disruption.

9. General Security Consulting and Authorised Testing

9.1 Security consulting services, including assessments, configuration reviews, vulnerability assessments, penetration testing or security validation activities, may only be performed against systems, applications, domains, networks or data for which appropriate written authorisation has been granted.

9.2 Customers must provide accurate scope, ownership and authorisation information before requesting testing or technical security activities. A customer may not request testing of a third party's assets without documented authority from the lawful owner or authorised controller.

9.3 Security deliverables, test results, vulnerability details, exploit evidence, credentials and sensitive technical information must be treated as confidential and used only for authorised risk management, remediation and governance purposes.

9.4 Customers must not use information, tools or outcomes provided through security consulting services to unlawfully access, disrupt, damage or compromise any system or person.

10. Network and Security Abuse

10.1 Unless expressly authorised in writing as part of a legitimate ManTK service, customers must not use the services for activity that seeks to compromise, probe, evade, disrupt or harm a network, service, system, application, account or device.

10.2 Prohibited network and security abuse includes:

10.2.1 distribution, hosting or execution of malware, ransomware, spyware, malicious scripts, destructive code or harmful payloads;

10.2.2 phishing, impersonation, credential harvesting, fraudulent social engineering or unauthorised collection of access information;

10.2.3 denial-of-service or distributed denial-of-service activity, traffic amplification, flooding or deliberate service degradation;

10.2.4 unauthorised port scanning, vulnerability scanning, enumeration, exploitation, intrusion attempts, credential attacks or lateral movement;

10.2.5 interception, monitoring, alteration or redirection of data or communications without lawful authority; and

10.2.6 deliberate concealment of abusive activity, including falsification of addressing, logs, identity or traffic origin.

11. Privacy, Confidentiality and Personal Information

11.1 Customers must use the services in a manner that respects privacy, confidentiality and the lawful processing of personal information.

11.2 Customers must not use the services to obtain, store, process, publish, sell, transmit or disclose personal information, confidential information or electronic communications unlawfully or without appropriate authority.

11.3 Where services involve customer content, communications, security telemetry or other information, the processing and protection of that information is also subject to the applicable privacy policy, customer agreement and any written data processing provisions.

12. Intellectual Property and Third-Party Rights

12.1 Customers must respect the intellectual property rights and lawful interests of ManTK and third parties.

12.2 Customers must not use hosted websites, servers, email services or any other ManTK service to copy, distribute, make available, sell, license or otherwise exploit protected material without permission or another lawful basis.

12.3 ManTK may act upon credible infringement complaints or lawful directions affecting services used by a customer and may require the customer to provide evidence of lawful authority to use disputed material.

13. Customer Security Obligations

13.1 Customers must take reasonable measures to prevent unauthorised access to or misuse of services under their control.

13.2 Without limiting clause 13.1, customers should, where relevant to the subscribed service:

13.2.1 protect usernames, passwords, administrator credentials, API keys, certificates and other authentication material from disclosure or misuse;

13.2.2 restrict privileged access to authorised persons and remove access when no longer required;

13.2.3 maintain supported, appropriately patched and securely configured customer-managed systems and applications;

13.2.4 retain appropriate backups and recovery arrangements for customer-managed data and systems; and

13.2.5 report suspected compromise, abuse or unauthorised access affecting a ManTK service without undue delay.

13.3 ManTK security or hosting services do not relieve customers of responsibility for their own lawful governance, risk management, access management, data protection and business continuity requirements.

14. Reporting Abuse and Unacceptable Use

14.1 Suspected contraventions of this AUP involving ManTK services should be reported to:

Abuse Reports	abuse@mantkitsolutions.co.za
Spam Complaints	abuse@mantkitsolutions.co.za
General Queries	info@mantkitsolutions.co.za

14.2 An abuse report should, where available, identify the affected service, domain, IP address, email address, URL or endpoint; describe the suspected abuse; include relevant dates and times; and provide supporting evidence such as message headers, logs, screenshots or other information that can assist investigation.

14.3 ManTK may investigate reports in good faith, request additional information, take proportionate steps to protect customers and networks, and refer matters to ISPA, affected providers, law enforcement or regulatory authorities where appropriate or legally required.

14.4 Complaints or take-down requests relating to unlawful content may also be submitted through the applicable ISPA processes available on ISPA's website.

15. Monitoring, Investigation and Cooperation

15.1 ManTK may use reasonable technical and administrative measures necessary to operate services, protect infrastructure, detect or prevent abuse, investigate incidents, meet legal obligations and enforce this AUP, subject to applicable law and contractual obligations.

15.2 Customers must reasonably cooperate with investigations and remediation actions concerning suspected misuse, service compromise, malicious traffic, security incidents, unlawful content or complaints relating to services used by the customer.

15.3 ManTK is not required to proactively monitor all customer content or activity and does not assume responsibility for customer content merely because it provides hosting, email or security services.

16. Enforcement, Suspension and Termination

16.1 Where ManTK reasonably believes that a service is being used in breach of this AUP, presents a material security or operational risk, or is subject to a lawful instruction, ManTK may take proportionate action.

16.2 Action may include:

16.2.1 issuing a notice requiring the customer to stop the conduct or remediate the affected system;

16.2.2 filtering, blocking, quarantining or removing malicious, unlawful or abusive traffic, email or content;

16.2.3 restricting, isolating or suspending an affected account, mailbox, domain, hosted server, website, endpoint security service or related connectivity;

16.2.4 terminating the affected service in accordance with the applicable agreement where the breach is serious, persistent or incapable of appropriate remediation; and

16.2.5 reporting the matter to relevant authorities, rights holders, ISPA or other affected parties where lawful and appropriate.

16.3 Where reasonably practicable and consistent with security and legal requirements, ManTK will seek to notify the customer before suspension or restriction. Immediate action may be taken without prior notice where required to prevent harm, respond to an urgent threat, comply with law or protect service availability.

16.4 The customer remains liable for charges properly due under the applicable agreement during a suspension attributable to the customer's breach, unless the agreement expressly provides otherwise.

17. Limitations and No Guarantee of Security

17.1 Hosting and security services are intended to manage or reduce risk but cannot guarantee complete prevention of spam, malicious content, compromise, data loss, unauthorised access, service interruption or other security events.

17.2 The customer's use of security services must form part of an appropriate broader security and governance programme, including customer-controlled access management, patching, configuration management, backups, staff awareness and incident response arrangements.

18. Changes to this Policy

18.1 ManTK may amend this AUP from time to time to address changes to services, security threats, legal or regulatory obligations, industry codes or operational requirements.

18.2 Where a change materially affects customers, ManTK will publish an updated version on its website and, where reasonably appropriate, provide notice through the relevant customer communication channel.

18.3 The updated AUP will apply from the effective date displayed in the published policy, subject to any rights or notice periods stated in an applicable agreement or required by law.

19. ISPA Membership and Related Information

19.1 ManTK is a member of the Internet Service Providers' Association of South Africa (ISPA) and is committed to compliance with the applicable ISPA Code of Conduct.

19.2 Information regarding the ISPA Code of Conduct, complaints process and take-down procedures is available through the ISPA website: https://ispa.org.za/

19.3 Nothing in this AUP limits any rights available to a complainant under applicable law, the ISPA Code of Conduct or an applicable customer agreement.

20. Contact Details

20.1 Queries regarding this AUP, reports of abuse, spam complaints or suspected misuse of ManTK services should be directed to the following designated contact details:

Registered Company Name	ManTK IT Solutions
Website	https://www.mantkitsolutions.co.za/
Abuse Email Address	abuse@mantkitsolutions.co.za
General Enquiries Email Address	info@mantkitsolutions.co.za
Telephone Number	+27 (0) 35 340 1061 / +27 (0) 66 123 7824
Physical Address	52 Pearson Avenue, Eshowe KwaZulu Natal, 3815