D H D
Information Security

TERMS AND CONDITIONS

DHD Information Security (Pty) Ltd

1. Definitions

In these Terms and Conditions, the following terms have the meanings set out below:

- **"DHD Information Security" or "we" or "us":** DHD Information Security (Pty) Ltd, Registration No. 2026/209612/07, a company registered in South Africa.
- **"Client" or "you":** The business or individual that has accepted these Terms by electronic means, including via checkbox on a quote or invoice.
- **"Services":** The cybersecurity monitoring, alerting, and reporting services described in clause 3, delivered using the Huntress platform.
- **"Huntress":** Huntress Labs Inc., a third-party managed detection and response platform used to deliver the Services. Use of the Services is subject to Huntress's own terms of service and privacy policy, available at huntress.com.
- **"Monitoring Agent":** The Huntress software agent installed on Client endpoint devices to enable the Services.
- **"Alert":** A notification generated by the Huntress platform indicating suspicious or potentially malicious activity detected on a monitored endpoint.
- **"Work Product":** Monitoring reports, alert summaries, investigation findings, and any other output generated by DHD Information Security in the course of delivering the Services.
- **"Xero":** Xero Ltd, a cloud-based accounting and invoicing platform used by DHD Information Security for client quoting, invoicing, and financial record-keeping.
- **"Cloudflare":** Cloudflare Inc., a third-party provider of DNS, content delivery, security, and bot-detection services for the DHD Information Security website.
- **"Absolute Hosting":** Absolute Hosting (Pty) Ltd, a South African hosting provider that hosts the DHD Information Security website and website database at Digital Parks Africa's Samrand facility in Gauteng.
- **"Microsoft Exchange Online":** A hosted business email platform operated by Microsoft Ireland Operations Ltd, used by DHD Information Security for all inbound and outbound business email communications. Data is processed within the European Union under Microsoft's Data Processing Agreement.
- **"Proton Drive":** A secure cloud document storage and sharing platform operated by Proton AG, headquartered in Geneva, Switzerland. Used by DHD Information Security for the storage and sharing of internal business records and, where applicable, client-facing documentation. Data is stored in Switzerland and Iceland under the Swiss Federal Act on Data Protection (FADP), using zero-access encryption.
- **"Business Hours":** 07:00–17:00 South African Standard Time (SAST), Monday to Friday, excluding South African public holidays.
- **"Effective Date":** The date on which the Client accepts these Terms electronically.
- **"AFSA":** The Arbitration Foundation of Southern Africa, an independent body providing arbitration and mediation services under South African law. See arbitration.co.za.
- **"ECTA":** The Electronic Communications and Transactions Act 25 of 2002.
- **"POPIA":** The Protection of Personal Information Act 4 of 2013.
- **"CPA":** The Consumer Protection Act 68 of 2008.

2. Acceptance and Electronic Agreement

These Terms govern the use of all Services provided by DHD Information Security to the Client. By accepting these Terms electronically — including by checking a box on a quote, invoice, or order form — the Client confirms that they have read, understood, and agree to be bound by these Terms and our Privacy Policy.

In accordance with ECTA, electronic acceptance constitutes a valid and binding agreement equivalent to a handwritten signature. No physical signature is required.

If you are accepting on behalf of a business, you confirm that you have authority to bind that business to these Terms.

The following rules of interpretation apply to these Terms:

- The contra proferentem rule — the rule that ambiguous terms are construed against the party who drafted them — shall not apply to these Terms.
- No alteration, cancellation, variation, or addition to these Terms shall be of force and effect unless reduced to writing and agreed to by both parties. No verbal agreement or exchange of correspondence shall constitute a variation of these Terms.
- If any provision of these Terms is found to be invalid, unlawful, or unenforceable, that provision shall be severed and the remaining provisions shall continue in full force and effect.
- The expiry or termination of these Terms shall not affect clauses that by their nature must survive, including clauses 7 (Disclaimer of Warranties and Guarantees), 10 (Limitation of Liability), 14 (Confidentiality), 15 (Intellectual Property), 18 (Coverage Gaps, Suspended Services, and Forensic Findings), and 21 (Dispute Resolution and Governing Law).

3. Scope of Services

DHD Information Security provides cybersecurity monitoring, alerting, and reporting services using the Huntress managed detection and response platform. The Services are designed to assist the Client in identifying potentially suspicious activity on supported endpoint devices.

The Services include:

- Installation or removal of approved Monitoring Agents on Client endpoints.
- Monitoring endpoint activity and suspicious behaviour indicators.
- Reviewing and validating Alerts before notifying the Client to reduce false positives.
- Review and notification of Alerts relating to potentially suspicious activity during Business Hours.
- Monthly reporting on monitored activity.
- Communication with the Client or their designated IT provider.

Services are observational and advisory in nature. DHD Information Security does not provide:

- Managed IT services or general IT support.
- Security administration or configuration management.
- Incident response, containment, or active remediation (unless separately agreed in writing).
- Backup management, disaster recovery, or data recovery.
- Security guarantees or compliance certification.
- 24/7 monitoring — Alerts are actioned during Business Hours as defined above.

Huntress is a third-party platform. Use of the Services is therefore also subject to Huntress's own terms and conditions and privacy policy, available at huntress.com.

4. Pilot Programme

The pilot programme is optional. Clients who wish to proceed directly to a paid subscription without a pilot may do so by accepting these Terms on a quote, in which case the subscription commences immediately and billing applies from the 1st of the following calendar month as set out in clause 16.

For clients who wish to evaluate the Services before committing, DHD Information Security offers a structured pilot at no charge, operating as follows:

- Maximum endpoints: 5 devices during the pilot period. The Client may select which devices to include, subject to the 5-device cap. The pilot covers the agreed number of devices from the date of first installation regardless of whether all selected devices have been installed. Devices not installed due to Client-side delays in providing access do not extend the pilot period or create any obligation on DHD Information Security.
- Duration: the pilot commences on the date the first Monitoring Agent is successfully installed on a Client endpoint, and runs until the last day of that calendar month. DHD Information Security recommends commencing a pilot on or before the 14th of the month to ensure a minimum 14-day evaluation window. Pilots commencing after the 14th will run until month end regardless of duration. No extension into a following month is provided.
- Post-pilot onboarding gap: following the end of the pilot, a reasonable onboarding period of up to 14 calendar days is recognised during which the Client may review findings, request a quote, and accept a subscription. Pilot agents may remain installed during this period at DHD Information Security's discretion and at no charge, but no active monitoring obligation or service obligation applies during this gap. This period does not constitute active service delivery.
- Conversion and billing: the Client may convert to a paid subscription at any point during or after the pilot. Regardless of when in a calendar month the Client accepts a paid subscription, the first invoice is issued on the 1st of the following calendar month at the full monthly rate for all contracted devices. No charge is raised for any portion of the pilot period. Where acceptance occurs early in a month, DHD Information Security may activate monitoring on all contracted devices immediately and carry the partial month at no charge pending the 1st invoice date. Early conversion is encouraged and will be accommodated without delay.
- Non-conversion: if the Client does not convert within 14 calendar days of pilot end, Monitoring Agents will be removed from all pilot endpoints and access to the Huntress portal will be withdrawn. No charge will be raised.
- The cost of the pilot is absorbed by DHD Information Security as a customer acquisition expense, capped at 5 devices regardless of the Client's intended subscription size.
- Pilot Services are provided subject to all disclaimers and limitations in these Terms, including clauses 7, 8, and 10.
- Abuse of the pilot offering, including creating multiple pilot accounts, misrepresenting business information, or repeatedly requesting pilots without genuine conversion intent, entitles DHD Information Security to terminate the pilot immediately and restrict future access to the programme.

The pilot does not constitute a commitment by either party to enter into an ongoing subscription. No billing obligations arise until the Client accepts a paid subscription by accepting these Terms on a quote or invoice.

5. Client Responsibilities

The Client is solely responsible for:

- Their overall IT environment, including security configuration, antivirus, patch management, and backups.
- Ensuring that all software, operating systems, and applications installed on monitored endpoints are fully and properly licensed. The Client warrants at the time of onboarding and on an ongoing basis that no unlicensed, cracked, or counterfeit software is in use on any

endpoint covered by the Services. DHD Information Security accepts no liability for security vulnerabilities, service disruptions, audit findings, or legal consequences arising from unlicensed software on Client systems, and reserves the right to suspend the Services if unlicensed software is identified on covered endpoints.

- Business continuity planning and disaster recovery procedures.
- User awareness, phishing training, and identity and access management.
- Maintaining the Monitoring Agent on all contracted endpoints. DHD Information Security cannot be responsible for gaps in coverage resulting from agent removal, blocking, or infrastructure changes made by the Client or their IT provider.
- Notifying DHD Information Security promptly of any changes to their network, firewall, VPN configuration, proxy settings, or other infrastructure that could affect the Monitoring Agent's connectivity or reporting capability. Failure to notify may result in undetected coverage gaps for which DHD Information Security accepts no liability.
- Notifying DHD Information Security of any changes to the number of monitored endpoints. Additional devices added to the monitored environment must be reported and will be billed from the date of addition. Devices permanently removed from the monitored environment must be reported so that the Monitoring Agent can be properly decommissioned. DHD Information Security accepts no liability for coverage gaps on unreported devices.
- Providing timely access to all contracted endpoints for Monitoring Agent installation. The subscription is device-based: it covers the number of devices listed on the accepted quote from the first invoice date, regardless of whether installation has been completed on all devices. This is consistent with standard software subscription billing — the invoice reflects contracted entitlement, not installation status. No credit, adjustment, or refund is provided for devices not yet installed due to Client-side delays in providing access. Coverage gaps arising from delayed installation are the Client's responsibility, and the Client is responsible for coordinating timely access with their IT provider or staff following subscription acceptance.
- Responding promptly to Alerts and escalating to their IT provider or other appropriate party.
- Maintaining a valid, monitored email address on record with DHD Information Security for the receipt of invoices, alerts, and enforcement notices. The Client is responsible for notifying DHD Information Security promptly of any change to their billing or primary contact email address. DHD Information Security's automated enforcement process relies on email communication and cannot be held responsible for missed notices resulting from an invalid, unmonitored, or changed email address.
- Maintaining relationships with external or third-party IT providers who are responsible for any remediation actions.

The Client is solely responsible for the operation, maintenance, backup, and recovery of its systems and business processes. Where suspicious activity is identified, remediation and recovery actions remain the responsibility of the Client or their designated IT provider.

---

6. Alert Notifications and Response

DHD Information Security will use reasonable endeavours to review and notify the Client of critical Alerts during Business Hours. Alerts are reviewed and validated before being passed to the Client to reduce false positives.

The Client acknowledges that:

- Alert notification does not constitute incident response or remediation.
- Response times may vary depending on alert volume and complexity.
- Alerts occurring outside Business Hours will be reviewed on the next available business day unless a separate out-of-hours arrangement has been agreed in writing.

---

7. Disclaimer of Warranties and Guarantees

Cybersecurity monitoring may help identify suspicious activity earlier, but no solution can eliminate all threats. Cybercriminals continuously evolve their methods, and ongoing monitoring may assist in identifying suspicious activity but cannot eliminate risk.

⚠ IMPORTANT – PLEASE READ CAREFULLY BEFORE ACCEPTING

DHD Information Security provides the Services on an "as is" and "as available" basis. No warranty, representation, or guarantee is made regarding uninterrupted availability, completeness, accuracy, or fitness for a particular purpose.

DHD Information Security does not guarantee that all malicious activity, compromise attempts, phishing attacks, malware, ransomware, or unauthorised access attempts will be detected, prevented, contained, or reported.

The use of the Services does not guarantee that the Client will not experience security incidents, data loss, system compromise, operational disruption, financial loss, fraud, or business interruption.

8. Third-Party Platforms and Software

The Services and DHD Information Security's business operations rely on several third-party platforms, software providers, and infrastructure partners. DHD Information Security is not responsible for:

- Failures or outages of third-party services, including Huntress.
- Detection limitations within third-party products.
- Delays in third-party alerting or reporting.
- Software defects, compatibility issues, or licensing interruptions.
- Internet or infrastructure failures outside our control.
- Incomplete, delayed, inaccurate, false positive, or false negative results originating from third-party platforms.

The principal third-party platforms used in delivering the Services and operating the business are:

- **Huntress Labs Inc.** — managed detection and response platform through which all endpoint monitoring services are delivered.
- **Xero Ltd** — used for client quoting, invoicing, and financial records. Client billing contact information is stored in Xero's cloud infrastructure in Australia.
- **Absolute Hosting** — hosts the DHD Information Security website and website database, physically located at Digital Parks Africa's Samrand facility in Gauteng, which holds ISO 27001:2022, ISO 9001:2015, and Uptime Tier III Design certification. Primary hosting infrastructure is located within South Africa.
- **Cloudflare Inc.** — provides security, DNS, and content delivery for the DHD Information Security website, including bot detection via Cloudflare Turnstile.
- **Microsoft Exchange Online** (Microsoft Ireland Operations Ltd) — hosted business email platform used for all inbound and outbound business communications, including client correspondence and alert notifications. Email data is processed within the European Union under Microsoft's Data Processing Agreement, with encryption at rest and in transit. Microsoft holds ISO 27001 and SOC 2 Type II certifications.
- **Proton AG** (Proton Drive) — secure document storage and sharing platform used for internal business records and, where applicable, client-facing documentation. Data is stored in Switzerland and Iceland under Swiss Federal law (FADP). Proton employs zero-access encryption, meaning documents are encrypted client-side and Proton cannot access their contents.

DHD Information Security makes no representations or warranties about any third-party provider's capabilities, uptime, security posture, or fitness for purpose beyond what each provider warrants in its own published terms. Clients are encouraged to review each provider's terms and legal documentation directly. Certain provider security and data handling details are described in our Privacy Policy at https://dhdinfosec.com/privacy, which forms part of these Terms.

9. DHD Information Security Operational Standards

DHD Information Security aims to maintain the following operational standards in the delivery of the Services:

- Multi-factor authentication (MFA) is enforced on all accounts with access to the Huntress management portal and Client-related data.
- Access to Client information is restricted to authorised personnel only, on a need-to-know basis.
- DHD Information Security endeavours to ensure that communications involving Client data are conducted over encrypted channels where reasonably practicable.
- Account credentials are reviewed regularly and revoked promptly upon any change in access requirements.
- The Huntress portal and related tooling are accessed only from secured, up-to-date devices.
- DHD Information Security does not maintain independent local telemetry databases; endpoint telemetry is primarily processed and stored within Huntress's cloud infrastructure subject to Huntress's security programme.

DHD Information Security does not claim formal certification (such as ISO 27001 or SOC 2) at this stage. The standards above represent the operational commitments made to Clients and reflect the operational standards currently implemented by DHD Information Security. Should certification be obtained in future, these Terms will be updated accordingly.

10. Limitation of Liability

⚠ IMPORTANT – PLEASE READ CAREFULLY BEFORE ACCEPTING

This clause limits DHD Information Security's liability. Please read it carefully. To the extent permitted by applicable law, including the Consumer Protection Act 68 of 2008, DHD Information Security's total cumulative liability to the Client for any and all claims arising from or related to the Services shall not exceed the total fees paid by the Client in the six (6) months preceding the event giving rise to the claim.

DHD Information Security shall not be liable for any direct, indirect, special, incidental, or consequential losses, including but not limited to: business interruption, loss of revenue or profits, data loss, recovery costs, ransom payments, reputational damage, operational downtime, or losses arising from phishing, BEC, malware, ransomware, or unauthorised access.

The Client acknowledges that cybersecurity monitoring reduces uncertainty but does not eliminate risk, and that the pricing of the Services reflects this allocation of risk.

Nothing in these Terms excludes or limits liability arising from gross negligence, fraud, or intentional misconduct where such limitation is prohibited by applicable law.

11. Recovery and Remediation

DHD Information Security is not responsible for, and does not provide as part of the Services:

- Restoring systems, data, or applications following a security incident.
- Reinstalling operating systems or recovering encrypted or deleted information.
- Business continuity operations, manual operational workarounds, or recovery coordination.
- Legal or regulatory reporting obligations arising from a security incident.
- Forensic investigations.

These responsibilities remain with the Client or their appointed service providers. DHD Information Security can provide referrals to appropriate incident response providers on request.

12. Data Processing and Privacy

In delivering the Services and operating the business, DHD Information Security processes personal information through several platforms. In terms of POPIA:

- **The Client** is the responsible party for personal information processed on their own systems.
- **DHD Information Security** acts as operator in respect of endpoint telemetry, processing data only on the Client's instruction and for the purpose of delivering the Services.
- **Huntress** acts as sub-operator for endpoint telemetry processed through the Huntress platform, with data hosted in the United States.
- **Xero** processes Client billing contact information (name, company, email, address) as a separate data processor for invoicing and accounting purposes, processed using Xero's cloud infrastructure which may include international hosting locations including Australia.
- **Absolute Hosting** processes website visitor data and contact form submissions as infrastructure provider for the DHD Information Security website, with all data physically located in South Africa.
- **Microsoft Exchange Online** (Microsoft Ireland Operations Ltd) processes business email data, including client communications and alert notifications, within the European Union under Microsoft's Data Processing Agreement and EU–UK GDPR-equivalent protections.
- **Proton AG** processes business records and client-facing documentation stored in Proton Drive, with data located in Switzerland and Iceland under Swiss Federal law (FADP). Zero-access encryption ensures Proton cannot access the contents of stored files.
- **Cloudflare** processes technical website visitor data including IP addresses and browser information globally as part of providing security, DNS, and content delivery services for dhdinfosec.com.

Full details of how we collect, use, store, and protect personal information — including the role of each third-party provider — are set out in our Privacy Policy, available at **https://dhdinfosec.com/privacy**, which forms part of these Terms and is incorporated by reference. By accepting these Terms, the Client also accepts the Privacy Policy.

13. Website Use

Users of https://dhdinfosec.com may not attempt to disrupt or compromise the website, submit malicious or fraudulent information, or use the website for unlawful purposes. DHD Information Security reserves the right to restrict access where misuse is suspected. Unauthorised use of this website may give rise to a claim for damages and/or a criminal offence.

14. Confidentiality

Alert data, investigation findings, monitoring reports, and any other information generated by DHD Information Security in the course of delivering the Services ("Service Information") is confidential to the Client and is provided solely for the Client's internal use.

The Client agrees not to:

- Publish, distribute, or share Service Information publicly or with third parties without the prior written consent of DHD Information Security, except where reasonably required for legal, insurance, regulatory, audit, or incident remediation purposes.
- Use Service Information in a way that misrepresents the nature, scope, or capabilities of the Services.
- Make representations to their own clients, staff, or third parties about the Services that exceed or contradict the limitations set out in these Terms.

The Client indemnifies DHD Information Security against any claim, loss, or liability arising from the Client's misrepresentation of the Services to any third party, including the Client's own staff, customers, or advisors.

15. Intellectual Property

All monitoring reports, alert summaries, investigation findings, and other work product generated by DHD Information Security in the course of delivering the Services ("Work Product") remain the intellectual property of DHD Information Security. The Client is granted a non-exclusive, non-transferable licence to use Work Product solely for their own internal business purposes.

The Client may not reproduce, publish, on-sell, or otherwise distribute Work Product to third parties without the prior written consent of DHD Information Security.

The Huntress name, logo, and related marks are the intellectual property of Huntress Labs Inc. Where DHD Information Security references Huntress in client-facing materials, this is done under licence from Huntress and does not imply ownership of or exclusive agency for the Huntress platform. The Services are "Powered by Huntress" within the meaning of Huntress's partner programme.

Nothing in these Terms transfers ownership of any pre-existing intellectual property of either party to the other.

16. Payment, Billing, and Service Continuity

16.1 Subscription Start and Invoicing

All subscriptions commence on the 1st of the calendar month following the date on which the Client accepts a quote or these Terms, regardless of whether the subscription follows a pilot or is a direct sign-up. DHD Information Security will activate monitoring as soon as practicable following acceptance. Any monitoring activated prior to the first invoice date is provided solely as a courtesy onboarding period and does not alter the subscription commencement date or first billing date. No pro-rata adjustment applies to the period between activation and the first invoice date.

Invoices are issued on or before the 1st of each calendar month for that month's Services and are payable by the 7th of that month. All fees are exclusive of VAT where applicable. The subscription is device-based and covers the number of devices listed on the accepted quote from the first invoice date, regardless of installation status on individual devices.

Payment may be made by EFT or through any payment method made available via DHD Information Security's invoicing platform. Payment shall not be deemed received until funds have cleared into DHD Information Security's account. The Client shall not be entitled to withhold or set off payment where Services have been rendered, including where a dispute is pending.

16.2 Automated Enforcement Policy

DHD Information Security operates a policy-driven, automated payment enforcement process applied consistently to all clients regardless of account size or tenure. Enforcement actions are not discretionary and are not subject to individual negotiation. The following lifecycle applies to unpaid invoices:

- Day 8 (one day after payment due date): automated payment reminder issued to the Client's registered email address.
- Day 15: final written notice issued advising that service suspension is imminent.
- Day 17: Services suspended and removal or deactivation of Monitoring Agents from Client endpoints initiated without further notice. The Client acknowledges that suspension on this date is consistently applied.

The Client acknowledges that enforcement actions are automated, consistently applied, and necessary for the operational and financial sustainability of the Services. The period from agent deactivation to reinstatement constitutes a Coverage Gap Period as defined in clause 18.

16.3 Reinstatement

Reinstatement of suspended Services requires full payment of all outstanding amounts plus a service restoration fee starting from R500, increasing based on device count and redeployment complexity. Reinstatement is subject to scheduling availability and may require advance payment of the first month's fees.

16.4 Annual Price Adjustments

Fees will be reviewed annually and may be adjusted with effect from 1 March each year, capped at the Consumer Price Index (CPI) as published by Statistics South Africa for the preceding 12 months. At least 30 calendar days' written notice will be given. Continued use of the Services after the adjustment date constitutes acceptance.

16.5 Service Continuation and Other Suspension Grounds

The Services continue on a rolling 30-day basis. DHD Information Security may also suspend or terminate Services for evidence of misuse, a security incident requiring isolation, or operational or legal requirements outside its reasonable control.

17. Termination

Either party may terminate the Services by providing 30 calendar days' written notice to the other party. The Services continue on a rolling 30-day basis and there is no minimum contract period unless otherwise agreed in writing on the applicable quote.

Upon termination:

- Monitoring Agents will be removed from Client endpoints.
- Access to related dashboards or portals will be withdrawn.
- The Client remains liable for all fees incurred up to and including the effective date of termination.

DHD Information Security may terminate immediately and without notice in the event of material breach by the Client, persistent non-payment, or where continued service would present a legal or security risk.

Clauses that by their nature survive termination — including clauses 7, 10, 14, 15, 18, and 21 — shall remain in full force and effect after termination or expiry of these Terms.

18. Coverage Gaps, Suspended Services, and Forensic Findings

⚠ IMPORTANT – PLEASE READ CAREFULLY BEFORE ACCEPTING

This clause is important. Please read it carefully.

No monitoring, alerting, or detection service is provided during any period in which the Services are suspended or terminated, or in which the Monitoring Agent is not operational on a covered endpoint, for any reason including non-payment by the Client, agent removal, or Client-side infrastructure changes.

DHD Information Security accepts no liability to the fullest extent permitted by applicable law for any security incident, breach, data loss, or damage that occurs, originates, or propagates during a Coverage Gap Period. A "Coverage Gap Period" means any period during which the Services were not active on the affected endpoint(s) for any reason.

Retrospective forensic findings: Where a Digital Forensic and Incident Response (DFIR) investigation or similar analysis determines that an initial compromise, intrusion, or malicious activity may have begun during a period when the Services were active, this finding alone does not constitute evidence of negligence by DHD Information Security. The Client acknowledges that:

- Cyber threats are designed to evade detection, and no monitoring service guarantees detection of all threats (see clause 7).
- The existence of a breach during a covered period does not imply that DHD Information Security failed to meet its obligations under these Terms.
- Any claim arising from such findings remains subject to the limitation of liability in clause 10, including the 6-month fee cap.
- No claim may be brought in respect of events that occurred wholly or partly during a Coverage Gap Period, regardless of when those events were discovered.

The Client is responsible for maintaining records of any periods during which the Monitoring Agent was disabled, removed, or non-functional on their endpoints, and for notifying DHD Information Security promptly of any such changes.

19. Force Majeure

DHD Information Security shall not be liable for any failure or delay in performing its obligations under these Terms where such failure or delay results from circumstances beyond its reasonable control, including but not limited to:

- Acts of God, natural disasters, flood, fire, or extreme weather events.
- National power grid failures, load shedding beyond scheduled outages, or utility infrastructure disruptions.
- Internet backbone or undersea cable failures, or failures of telecommunications infrastructure not operated by DHD Information Security.
- Failures, outages, or disruptions of third-party platforms including Huntress, cloud hosting providers, or DNS services.
- Acts of government, regulatory action, civil unrest, pandemic, or national emergency.

- Cyber attacks directed at DHD Information Security's own infrastructure that are beyond its reasonable ability to prevent.

In the event of a force majeure event, DHD Information Security will notify the Client as soon as reasonably practicable and will use reasonable endeavours to resume Services at the earliest opportunity. The Client's payment obligations are suspended for the duration of a verified force majeure event affecting service delivery. Neither party may claim damages from the other for losses arising solely from a force majeure event.

20. Changes to Services or Terms

DHD Information Security may modify operational procedures or these Terms from time to time. Pricing changes are governed by the annual CPI adjustment mechanism in clause 16.4. Material changes to these Terms will be communicated to the Client at least 14 calendar days in advance via email to the address provided at the time of acceptance.

Continued use of the Services after the effective date of any change constitutes acceptance of the updated Terms. Updated Terms will be published at https://dhdinfosec.com/terms.

21. Dispute Resolution and Governing Law

These Terms and Conditions are governed by the laws of the Republic of South Africa.

In the event of any dispute arising from or in connection with these Terms, the parties agree to attempt resolution in the following sequence:

- Informal resolution: either party may give written notice of the dispute, following which the parties will use reasonable endeavours to resolve it directly within 14 calendar days.
- Mediation: if informal resolution fails, either party may refer the dispute to mediation under the rules of the Arbitration Foundation of Southern Africa (AFSA) or such other mediator as the parties may agree. Each party bears its own costs of mediation.
- Arbitration: if mediation fails or either party declines mediation, the dispute shall be finally resolved by binding arbitration in accordance with the rules of AFSA, conducted in English in Middelburg or such other venue as the parties may agree. The arbitrator's award shall be final and binding.
- Small claims: where the amount in dispute does not exceed the jurisdiction of the Magistrates' Court, either party may elect to refer the matter directly to the Magistrates' Court as an alternative to arbitration.
- Court proceedings: nothing in this clause prevents either party from seeking urgent interim relief from a court of competent jurisdiction where necessary to prevent irreparable harm.

These Terms do not limit any rights the Client may have under the Consumer Protection Act 68 of 2008 or any other applicable South African legislation that cannot be excluded by agreement.

22. Contact and Complaints

For any questions, concerns, or complaints regarding the Services or these Terms, please contact us:

DHD Information Security (Pty) Ltd
Registration No: 2026/209612/07
5 Dolorite Crescent, Middelburg, 1050, South Africa
Email: admin@dhdinfosec.com
Tel: (+27) 13 880 2252
Mobile: (+27) 67 948 1571
Website: https://dhdinfosec.com

Effective Date: 1 May 2026

We will acknowledge your complaint within 2 business days, provide a reference and estimated resolution timeline, and deliver a substantive response within 30 calendar days. If you are not satisfied with our response, you may escalate the matter in accordance with the dispute resolution process set out in clause 21.

⚠ IMPORTANT – PLEASE READ CAREFULLY BEFORE ACCEPTING

IMPORTANT — CLIENT ACCEPTANCE

By accepting these Terms electronically (including by checking a box on a quote or invoice), the Client confirms that they have read, understood, and agree to be bound by all clauses in this document, including in particular:

- Clause 7: Disclaimer of Warranties and Guarantees — no guarantee of detection or prevention.
- Clause 8: Third-Party Platform limitations including Huntress.
- Clause 9: DHD Information Security operational standards.
- Clause 10: Limitation of Liability — total liability capped at 6 months' fees.
- Clause 14: Confidentiality and no misrepresentation of the Services.
- Clause 15: Intellectual Property — Work Product ownership.
- Clause 16: Payment, billing, enforcement, and reinstatement fees.
- Clause 18: Coverage Gaps and the effect of suspended or terminated services.
- Clause 19: Force Majeure.

The Client further confirms:

- They accept the Privacy Policy at https://dhdinfosec.com/privacy-policy, incorporated into these Terms by reference.
- They have the authority to bind the business named on the quote or invoice.
- Electronic acceptance constitutes a valid and binding agreement under the Electronic Communications and Transactions Act 25 of 2002.

Questions before accepting? Contact us at **admin@dhdinfosec.com** or (+27) 13 880 2252.