PRIVACY POLICY

DHD Information Security (Pty) Ltd

1. Introduction

Effective Date: 1 May 2026

DHD Information Security (Pty) Ltd ("we", "us", or "our") respects your privacy and is committed to protecting personal information in accordance with the Protection of Personal Information Act 4 of 2013 ("POPIA") and all applicable South African law.

This Privacy Policy explains what personal information we collect, why we collect it, how we use and protect it, and what rights you have in relation to it. It applies to:

- Visitors to and users of https://dhdinfosec.com.
- Individuals and businesses who submit enquiries or pilot requests through our website.
- Clients who have entered into a service agreement with DHD Information Security for the delivery of managed cybersecurity monitoring services using the Huntress platform.

This Privacy Policy forms part of our Terms and Conditions, available at https://dhdinfosec.com/terms, which are incorporated by reference. Where you are a client, both documents apply to your relationship with us.

2. Who We Are and Our Role Under POPIA

DHD Information Security (Pty) Ltd is the responsible party in respect of personal information collected through this website and in connection with service enquiries.

Where DHD Information Security delivers managed monitoring services to a client, the data processing roles are as follows:

- **The Client** is the responsible party for personal information held on their own systems and endpoints.
- **DHD Information Security** acts as operator, processing endpoint telemetry and related data solely on the Client's instruction and for the purpose of delivering the contracted Services.
- **Huntress Labs Inc.** acts as a sub-operator in respect of data processed through the Huntress managed detection and response platform. Huntress's own privacy policy and legal documentation are available at huntress.com.

DHD Information Security does not process client endpoint data for any purpose other than delivering the Services, and does not share, sell, or use such data for marketing or analytics.

3. Information We Collect

3.1 Website and Enquiry Data

When you visit our website or submit an enquiry or pilot request form, we may collect:

- Name and surname.
- Business email address and telephone number.
- Company name and number of devices or systems discussed.
- Information voluntarily submitted through contact forms, including your message content.

- Technical website information such as browser type, IP address, and pages visited, collected automatically for security and analytics purposes.

3.2 Service Delivery Data

Where you are an active client, the Huntress Monitoring Agent installed on your endpoints processes endpoint telemetry in order to deliver the Services. Routine data collection is limited to system metadata and does not include the content of user documents, emails, or business files. Specifically:

- Process activity, network connection data, and behavioural indicators used to detect suspicious activity.
- Device identifiers, operating system details, software inventory, registry entries, and scheduled tasks.
- Alert data, investigation findings, and monitoring reports generated during the service period.
- File hashes (cryptographic fingerprints) may be checked against threat intelligence databases such as VirusTotal. This is a hash lookup only — the file itself is not transmitted in this process and document content does not leave the endpoint.
- In limited circumstances where a file exhibits behaviour strongly indicative of malware, Huntress may collect a copy of that file for security analysis in accordance with Huntress's own detection logic and Data Processing Addendum. This applies only to files exhibiting active malicious behaviour indicators, not to ordinary business documents, spreadsheets, emails, or other user data.

We do not use service delivery data for any purpose other than delivering and improving the contracted Services. We do not collect, view, or process the content of personal communications, documents, or financial records on your endpoints.

3.3 Client End-User Disclosure Obligation

Where the Client is an organisation, the Client (as responsible party under POPIA) bears the obligation to inform their own staff, end users, and where applicable their own customers, about the nature of endpoint monitoring and the data processed through the Services. DHD Information Security and Huntress are not responsible for disclosures that the Client is required to make to their own personnel or third parties under applicable data protection law. Clients should refer to Huntress's Privacy Policy and Data Processing Addendum, available at huntress.com, for further detail on data handling at the sub-operator level.

---

4. Lawful Basis for Processing

We process personal information only where we have a lawful basis to do so under POPIA section 11. The applicable bases for each category of processing are:

- **Website and enquiry data:** Consent, given when you submit a contact or pilot request form and confirm acceptance of this Privacy Policy.
- **Service delivery data:** Contractual necessity — processing is required to perform our obligations under the Terms and Conditions accepted by the Client.
- **Billing and financial records:** Contractual and legal necessity — processing of billing contact information in Xero is required to raise quotes and invoices, maintain financial records, and comply with applicable tax and accounting obligations.
- **Legal and regulatory obligations:** Where we are required to retain or disclose information to comply with applicable law, court order, or regulatory requirement.

You may withdraw consent for enquiry data processing at any time by contacting us. Withdrawal of consent does not affect processing already carried out on a lawful basis, and does not apply to service delivery data where processing is required to fulfil a contractual obligation.

---

5. How We Use Personal Information

We use the information we collect to:

- Respond to enquiries and arrange consultations or pilot deployments.
- Communicate with you regarding the Services you have requested or engaged.
- Assess your business requirements and provide appropriate recommendations.
- Deliver and manage the contracted cybersecurity monitoring Services.

- Generate monitoring reports and alert notifications for active clients.
- Improve website functionality, security, and user experience.
- Maintain records of communications and service delivery as required by law or contract.
- Comply with legal and regulatory obligations.

We do not sell personal information to third parties. We do not use personal information for unsolicited marketing without your explicit consent. If you have provided consent to receive marketing communications, you may opt out at any time by contacting us at admin@dhdinfosec.com. Opting out of marketing does not affect transactional or service-related communications, which we will continue to send as required to deliver the Services.

6. Third-Party Service Providers

We may share limited personal information with trusted third-party providers who assist us in operating our business and delivering our Services. All third-party providers are engaged subject to appropriate contractual safeguards and are required to process information only for the purpose for which it was shared.

Current third-party providers include:

- **Huntress Labs Inc.** (huntress.com) — managed detection and response platform used to deliver client monitoring Services. Huntress processes endpoint telemetry as sub-operator on our behalf. Data is hosted in the United States and may be processed outside South Africa subject to Huntress's contractual and technical safeguards, including their Data Processing Addendum. Huntress may also use anonymised, de-identified system data (containing no personal data or client-identifying information) for threat research, product improvement, and industry reporting. Huntress's Privacy Policy and Data Processing Addendum are available at huntress.com.

- **Xero Ltd** (xero.com) — cloud-based accounting, quotation, and invoicing platform. When we raise a quote or invoice, client contact details including name, company name, email address, and billing address are stored in Xero. Xero is a New Zealand company with infrastructure in Australia and other jurisdictions. Data processed by Xero is subject to Xero's Privacy Policy, available at xero.com/za/legal/privacy.

- **Cloudflare Inc.** (cloudflare.com) — provides DNS, content delivery, DDoS protection, and security services for our website. Cloudflare processes technical visitor data including IP addresses, browser type, and request metadata to protect the website against malicious traffic. Our website also uses Cloudflare Turnstile, a privacy-preserving bot-detection tool. Cloudflare's Privacy Policy is available at cloudflare.com/privacypolicy.

- **Absolute Hosting** (absolutehosting.co.za) — South Africa-based hosting provider that hosts our website and website database. Infrastructure is 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.

- **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 and is subject to the EU–UK GDPR-equivalent protections. Microsoft's privacy documentation is available at microsoft.com/en-us/trust-center.

- **Proton AG** (proton.me) — Proton Drive is used for secure document storage and sharing, including internal business records and where applicable client-facing documentation. Proton AG is headquartered in Geneva, Switzerland, and data is stored on servers located in Switzerland and Iceland. Processing is subject to the Swiss Federal Act on Data Protection (FADP) and Proton's zero-access encryption architecture, under which documents are encrypted client-side and Proton cannot access their contents. Proton's Privacy Policy is available at proton.me/legal/privacy.

Where any provider processes personal information outside South Africa, we take reasonable steps to ensure that appropriate safeguards are in place consistent with POPIA's cross-border transfer requirements.

7. Data Retention

We retain personal information only for as long as is reasonably necessary for the purpose for which it was collected, or as required by law.

Specific retention periods:

- **Enquiry and contact form data:** Retained for the duration of any resulting business relationship, or for up to 3 years from last contact where no relationship is formed, after which it is securely deleted or anonymised.
- **Service delivery data:** Retained for the duration of the active service agreement and for up to 12 months after termination to support any post-termination queries, disputes, or forensic requirements. Endpoint telemetry processed by Huntress is subject to Huntress's own retention policy.
- **Business email (Microsoft Exchange Online):** Email communications are retained for the duration of the active business relationship and for up to 3 years thereafter, consistent with applicable legal and contractual record-keeping obligations.
- **Documents stored in Proton Drive:** Business records and client-facing documentation are retained for as long as required by the underlying business relationship or applicable legal obligation, and are securely deleted when no longer required.
- **Legal and compliance records:** Retained for as long as required by applicable law or regulatory obligation, which may exceed the periods above.

Information no longer required is securely deleted or anonymised where technically practicable.

8. Website Analytics and Security

Our website may use cookies, security services, and analytics tools to improve functionality, detect abuse, and help safeguard the site against malicious activity. Technical information including IP addresses and browser information may be processed for security monitoring and fraud prevention purposes.

Where cookies are used, non-essential cookies will only be set with your consent. You may adjust your cookie preferences at any time through your browser settings. Essential security and functionality cookies may be set without consent as they are necessary for the website to operate correctly.

9. Security Measures

We implement reasonable technical and organisational measures to protect personal information against unauthorised access, disclosure, misuse, loss, and destruction. Our own operational security measures include:

- Multi-factor authentication (MFA) on all accounts with access to client data or 3rd party management portals.
- Strong access controls limiting access to client information to authorised personnel only.
- Encrypted communications for all data in transit.
- Regular review of access credentials and prompt revocation upon any change in access requirements.

Our key infrastructure and service providers maintain the following security standards:

- **Xero Ltd —** ISO/IEC 27001:2022 certified and independently audited to SOC 2. Xero uses MFA, encrypts data at rest and in transit, and replicates data across multiple locations.
- **Huntress Labs Inc. —** maintains a comprehensive security programme including logical data segregation, role-based access controls, encryption at rest and in transit, audit logging, vulnerability management, incident response procedures, and business continuity planning.

- **Absolute Hosting —** infrastructure is physically housed at Digital Parks Africa's Samrand facility in Gauteng, which holds ISO 27001:2022 and ISO 9001:2015 certifications and carries Uptime Tier III Design certification.
- **Cloudflare Inc. —** operates a global network with enterprise-grade DDoS mitigation, web application firewall (WAF), and bot protection. Cloudflare holds ISO 27001, SOC 2 Type II, and PCI DSS certifications.
- **Microsoft Exchange Online —** hosted within Microsoft's EU datacentre region under Microsoft Ireland Operations Ltd. Microsoft holds ISO 27001, ISO 27018, SOC 1 and SOC 2 Type II certifications, and complies with the EU–UK GDPR Data Processing Agreement. Data is encrypted at rest and in transit.
- **Proton AG —** employs zero-access end-to-end encryption for Proton Drive, meaning documents are encrypted client-side before upload and Proton cannot access their contents. Proton's infrastructure is located in Switzerland and Iceland under Swiss Federal law.

However, no internet-based system can be guaranteed completely secure. In the event of a data breach that is likely to result in harm to affected data subjects, we will notify affected parties and the Information Regulator as required by POPIA section 22.

10. Your Rights Under POPIA

Your rights as a data subject	
Access	Request confirmation of whether we hold personal information about you, and obtain a copy.
Correction	Request correction of inaccurate, incomplete, or outdated personal information.
Deletion	Request deletion of personal information we are no longer lawfully entitled to hold.
Objection	Object to the processing of your personal information on grounds relating to your particular situation.
Withdrawal of consent	Where processing is based on consent, withdraw that consent at any time.
To exercise any of these rights, contact us at admin@dhdinfosec.com. We will endeavour to respond within 30 calendar days of receiving your request. Identity verification may be required before requests can be processed.	

If you are not satisfied with our response, or believe we have processed your personal information unlawfully, you have the right to lodge a complaint with the South African Information Regulator:

Information Regulator (South Africa)
Website: https://inforegulator.org.za
General enquiries: enquiries@inforegulator.org.za
POPIA complaints: POPIAComplaints@inforegulator.org.za
Tel: 0800 017 160
Address: Woodmead North Office Park, 54 Maxwell Dr, Sandton, 2191, South Africa

11. Cross-Border Transfers of Personal Information

Some of our third-party service providers operate infrastructure outside South Africa. Specifically:

- **Huntress** processes endpoint telemetry data in the United States, subject to their Data Processing Addendum.
- **Xero** processes billing contact information in Australia and other jurisdictions, subject to their Privacy Policy and applicable data transfer safeguards.
- **Cloudflare** processes technical visitor data globally through their distributed network infrastructure.
- **Microsoft Exchange Online** processes business email data within the European Union under Microsoft Ireland Operations Ltd, subject to Microsoft's Data Processing Agreement and EU–UK GDPR-equivalent protections.
- **Proton** Drive stores documents in Switzerland and Iceland under Swiss Federal law (FADP), with zero-access encryption ensuring Proton cannot access the contents of stored files.

Where personal information is transferred to a foreign country, we take reasonable steps to ensure that the recipient is subject to a law, binding corporate rules, or a binding agreement that provides a comparable level of protection to POPIA. By using our website or Services, you acknowledge that your information may be processed in jurisdictions outside South Africa, subject to these safeguards.

12. Children's Personal Information

Our Services are intended exclusively for businesses and professional users. We do not knowingly collect personal information from individuals under the age of 18. If you believe we have inadvertently collected such information, please contact us immediately and we will take steps to delete it.

13. Policy Updates

This Privacy Policy may be updated periodically to reflect operational, legal, or technical changes. The latest version will always be published at https://dhdinfosec.com/privacy.

Where changes are material — meaning they affect how we process your personal information in a way that could impact your rights — we will notify active clients by email at least 14 calendar days before the changes take effect. Non-material updates (such as clarifications of existing practices) may be made without prior notice.

14. Contact Us and Complaints

For any questions, requests, or concerns regarding this Privacy Policy or the processing of your personal information, 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
Information Officer: Damian Pfister (admin@dhdinfosec.com)
Effective Date: 1 May 2026

Our complaints commitment to you:

- We will acknowledge your complaint within 2 business days and provide a reference number.
- We will inform you of estimated timelines and next steps.
- We will provide a substantive response within 30 calendar days.
- If we are unable to resolve your complaint to your satisfaction, we will explain the reason for our decision and advise you of further options.

If you remain dissatisfied after engaging with us directly, you may refer the matter to the South African Information Regulator using the contact details in clause 10 above.