Security at Tacklit

V2.0

Last updated October 2026

TACKLIT



Introduction

At Tacklit, we believe technology can help mental health providers deliver care that is more efficient, more personal and more effective. Our purpose is to help millions of people access proactive, personalised, outcome-driven mental health care. To do that, we capture and organise the information our customers need through modern digital touch points.

Moving care records, assessments and conversations online means the information we hold is among the most sensitive there is. It demands high security standards in every part of our business.

This whitepaper sets out the steps and practices we use to protect privacy and safeguard your data.

Executive Summary

- We treat security as a first-class concern. All data, including client records, file attachments and images, is encrypted by default: in transit using TLS 1.2 or higher, and at rest using industry-standard AES-256 encryption.
- Personally identifiable information carries an additional layer of application-level encryption, so neither database administrators nor our infrastructure providers can read it.
- Your data is stored in your region: London for UK customers and Sydney for Australian customers. It is backed up every 2 hours, weekly and monthly, and we test our ability to restore it every year.
- Our staff are trained to handle your data with the utmost care. No one at Tacklit has routine access to customer data: engineers receive time-limited, just-in-time access for a specific task, under the principle of least privilege.
- Monitoring and audit logging are enabled at every critical point in our infrastructure, databases and application, and logs are retained for 12 months.
- Our security is independently assured. Tacklit is Cyber Essentials certified, is penetration tested every year by an independent specialist, and is a signatory to the NHS Cyber Security Charter for Suppliers.
- We comply with UK GDPR and the Data Protection Act 2018, the Australian Privacy Act 1988 and the New Zealand Privacy Act 2020.

Cyber Essentials Certification

CERTIFICATE OF ASSURANCE

Tacklit UK Ltd complies with the requirements of the Cyber Essentials scheme

SCOPE	Whole organisation
DATE OF CERTIFICATION	10 August 2026
RECERTIFICATION DUE	10 August 2027
REQUIREMENTS VERSION	3.3 (Danzell)
CERTIFICATE NUMBER	15f132b3-788f-412e-af56-a3d3bc35d5c8
CYBER ESSENTIALS PARTNER	IASME

Tacklit holds Cyber Essentials certification, renewed in August 2026 for the whole organisation.

Cyber Essentials is a UK government-backed scheme, run with the National Cyber Security Centre, that independently checks an organisation has the core technical controls in place to defend against the most common cyber attacks:

- Firewalls and secure internet gateways
- Secure configuration of devices and software
- User access control
- Malware protection
- Security update management

Cyber Essentials certification is required for UK central government contracts that involve handling sensitive and personal information. Certification is renewed every year.

in association with National Cyber Security Centre

Cyber Essentials

View our certificate
https://resources.tacklit.com/information/Cyber-Essentials-2026.pdf

Contents

2 **ORGANISATIONAL SECURITY**

How we manage our people and processes

3 **APPLICATION SECURITY**

How we build and test our software

4 **OPERATIONS SECURITY**

How we run our infrastructure

5 **KEY POLICIES**

Legislation, data residency, transfers and retention

6 **THIRD-PARTY PROCESSORS**

Our key partners and service providers

7 **ASSURANCE AND CLINICAL SAFETY** NEW

Certifications, independent testing and clinical risk management



2. Organisational Security

2.1 Employee training

Tacklit employees complete security, privacy and compliance training every quarter, followed by questionnaires that check their understanding. Keeping user data safe is everyone's responsibility at Tacklit, so this training covers every role and every level of the organisation.

Our management team brings over 50 years of combined experience operating large-scale technology companies, and that experience shapes how we recruit, train and manage our staff.

2.2 Access control to data

Tacklit staff have no standing access to customer data. When an engineer needs production access to resolve a support request or engineering task, it is granted just in time for that specific task and removed when the task is complete. A small number of named executives hold standing production access as a controlled exception.

All access follows the principle of least privilege and is provisioned through centralised account management, so we can revoke it immediately if an account is ever compromised. Every access to production infrastructure and databases is logged.

2.3 Multi-factor authentication and strong passwords

Tacklit maintains a strict password policy for every internal and external service we use, including production systems and tooling. Everyone at Tacklit must use a strong, complex password on a 60-day rotation cycle, and multi-factor authentication is mandatory as a second login check.

2.4 Incident and security response plan

Our Incident Response Plan sets out how we identify, triage, contain, eradicate and recover from a security incident, and how we notify and review afterwards. The plan is reviewed every year and rehearsed through tabletop exercises.

As your data processor, if we become aware of a personal data breach affecting your data we will notify you without undue delay, and within 24 hours. We will give you the information you need to meet your own obligations as data controller, including notifying the regulator (in the UK, the ICO within 72 hours) and affected individuals, and we will cooperate fully with your response.

After every incident we carry out a post-incident review and put corrective and preventive measures in place so it does not happen again.

2.5 Secure endpoints

Tacklit has a strict policy for the laptops and mobile devices used to access our tooling and services. Staff devices are protected with strong passwords, lock automatically when unattended and have encrypted disks by default. If a device is lost or stolen, encryption stops anyone reading its data, and we can locate the device and erase it remotely.



3. Application Security

3.1 Data encryption

In transit

Tacklit is built on a client (your web browser or our mobile apps) and server architecture. All traffic between your device and our servers is encrypted using TLS 1.2 or higher with strong ciphers, including AES-256. This secure connection stops anyone listening in, tampering with or forging your communications anywhere between your device and our system.

At rest

All information stored in the Tacklit database, together with uploaded files and backups, is encrypted using AES-256. Highly sensitive data such as patient identifiable information (PII) has an additional layer of application-level encryption, so neither database administrators nor third-party infrastructure staff can read it.

3.2 File storage

Uploaded documents and attachments are encrypted at rest using AES-256 and protected by access control at the API level, which logically separates each file from other Tacklit users. Every file request is checked against the user's access token to confirm they are entitled to it.

3.3 Authentication and access

Tacklit enforces a strong password policy when you or your clients create an account. Passwords are never stored in readable form: our identity platform, Auth0, salts and hashes them using bcrypt, a one-way algorithm designed to resist brute-force attacks.

Our application also detects brute-force activity such as repeated failed logins, locks high-risk accounts and automatically emails the affected user about the suspicious activity.

- **Multi-factor authentication** is available on every login and can be required for your whole team.
- **Single sign-on** lets your staff log in with your existing identity provider, including Microsoft Entra ID, using OpenID Connect or SAML.
- **Automatic logout** ends idle sessions after 90 minutes. The window is set so an extended telehealth consultation is not interrupted mid-session.
- **Role-based access** means every user holds a role, and custom roles and fine-grained permissions can restrict access down to named clients or episodes of care.

3.4 Software development process and practices

We aim to catch security vulnerabilities during development and testing, so our first principle is to design the application with security in mind.

Every change is peer reviewed against the industry-standard guidance of the Open Worldwide Application Security Project (OWASP), checking for issues such as insecure endpoints or exposed access tokens. Private endpoints are only accessible with a valid access token and only return data that belongs to the requester.

https://owasp.org/www-project-top-ten/

We use Snyk, an industry-leading security and vulnerability scanning tool, throughout our development workflow for static code analysis and dependency scanning. Dependency and vulnerability scanning is built into our continuous delivery pipeline, so every build is checked.

Development, staging and production environments are isolated from each other. Every release passes quality assurance checks and nightly automated regression tests in staging before it reaches production. We also run a bug bounty programme that supports responsible disclosure of vulnerabilities by ethical security researchers, and hold in-depth security reviews and workshops with our development teams every quarter.

3.5 Penetration testing and vulnerability management

An independent security specialist penetration tests the Tacklit platform every year. Testing is grey-box, across multiple user roles, and aligned to the OWASP Top 10, the OWASP Application Security Verification Standard and the OWASP API Security Top 10. Our most recent test, in June 2026, found no critical or high severity issues. All findings were remediated and retested. A summary report is available on request.

Vulnerabilities found through scanning, provider security advisories, penetration testing or our bug bounty programme are rated by severity and fixed to these targets:

Severity	Remediation target
Critical	Within 48 hours
High	Within 7 days
Medium	Within 30 days
Low	Next release cycle

NHS High Severity Alerts and equivalent vendor advisories are assessed on receipt and treated as critical where the affected component is in use. A Software Bill of Materials (SBOM) is available under NDA on request.

3.6 Audit trail

Every time a user creates, views, edits or exports a client record, Tacklit writes an entry to an append-only audit log recording who, what and when. Clinical notes are tamper-evident: amendments are added and the original is preserved. Consent records and custom data fields keep a full version history. No customer role can edit or delete the audit log, which is available in the platform and retained for a minimum of 12 months.



4. Operations Security

4.1 Data centres

The Tacklit application runs on Google Cloud, and our database runs on MongoDB Atlas, hosted on Amazon Web Services (AWS) in the same region. Both Google Cloud and AWS hold ISO 27001 and SOC 2 certification, and we follow their recommended practices to secure access, data and production environments.

Their data centres are protected by multi-layered physical security, including 24/7 surveillance and tiered controlled access to hardware, and services are spread across multiple availability zones. Operating systems, databases and services are kept up to date with the latest security patches.

4.2 Network security

Tacklit isolates testing and development environments from production to protect sensitive data. Engineers work in the testing and development environments; access to production is restricted and granted just in time (see 2.2).

Inbound traffic arrives through the Google Cloud global load balancer, which absorbs large-scale denial of service traffic at the network edge. Firewall policies then allow only known IP addresses and essential network ports. Every application service accepts calls only from known sources with validated access tokens, and API rate limiting and input validation protect the application layer. System calls are logged and monitored, and alert policies are in place to detect potential intrusion.

4.3 Auditing and monitoring

Auditing lets us investigate who did what, and when, in the event of an intrusion. It is critical to understanding the scope of a data breach or security incident, closing the vulnerability quickly and preventing it happening again.

Auditing is enabled across all production infrastructure and databases, logging database access, IP addresses, times and actions taken. Logs are held centrally in Google Cloud Logging, within the same region as your data, and retained for 12 months to support any later investigation.

Monitoring helps us stop threats before they cause harm. Tacklit runs multiple alerting systems across our application and network that notify our technical team when something needs attention, and give them the context to troubleshoot and resolve it quickly. We prioritise investigating these alerts to resolve technical issues and prevent malicious activity.

To protect user accounts, every Tacklit login is logged so we can detect unusual traffic or patterns such as repeated failed logins. Too many failed attempts block the account to prevent password brute-force attacks, and our technical team is notified so they can check whether it is a genuine login problem and help the user regain access.

4.4 Disaster recovery and business continuity

Tacklit uses several mechanisms to keep the platform available and resilient. Our services run in Google Cloud in each region we serve: London for the UK and Sydney for Australia. Our infrastructure is self-healing, replacing degraded servers with new instances automatically, and servers are load-balanced across multiple instances and availability zones.

Customer data is held in a database cluster that is replicated across servers and availability zones, so we can patch and maintain it without downtime. If a server fails, the database automatically fails over to healthy servers and our services continue without interruption. Our Business Continuity and Disaster Recovery Plan sets a recovery time objective of under 1 minute and a recovery point objective of 1 hour for core production services.

We treat data integrity and availability as just as important. To protect against failure or corruption, your data is backed up every 2 hours, weekly and monthly. Backups are encrypted, stay in your region, and are stored separately from the infrastructure the database runs on.

We test recovery every year in each production region. In our most recent UK test, in June 2026, we restored a full production backup to an isolated environment in 33 minutes and verified it with no discrepancies.

4.5 Data ownership

You are the data controller and Tacklit is your data processor. Your data is yours. We process it only on your documented instructions and only to deliver our service. We do not scan it for marketing or advertising, and we never sell it to third parties.

In line with our Terms of Use and Data Processing Agreement, we may create anonymised, aggregated information that cannot be used to identify any individual, and use it to improve our products and services. Organisations that need to restrict this can do so in their agreement with us.

If you choose to move to another system, we will help you export a complete copy of your data securely. On termination, we provide your data as a structured export and then delete it, and we can provide a certificate of destruction on request.

If you ask us to erase data, we make it unavailable immediately and delete it in accordance with our Data Processing Agreement and privacy policy.

https://www.tacklit.com/policies/privacy-policy

4.6 Key management

Encryption keys are generated and held in our cloud providers' managed key services, never in application code or on developer machines. Application keys are managed in Google Cloud Key Management Service and Secret Manager, and database encryption at rest uses keys managed through MongoDB Atlas and cloud key management. Access to keys is restricted by role, every key operation is logged, and keys are rotated and retired under policy.



5. Key Policies

5.1 Adherence to required legislation

Tacklit complies with the rules that apply in each country where we operate, for how we collect, use and protect personal and health information.

- **United Kingdom:** UK GDPR and the Data Protection Act 2018. Tacklit UK Ltd is registered with the Information Commissioner's Office (registration C2051947).
- **Australia:** the Privacy Act 1988 and the Australian Privacy Principles, together with state health records legislation where it applies.
- **New Zealand:** the Privacy Act 2020 and the Health Information Privacy Code 2020.

The detail is set out in our Terms of Use, End User Licence Agreement, Data Processing Agreement and privacy policy for each region.

5.2 Data residency

Tacklit stores customer data in the country where your account is held. For UK customers, data, backups and disaster recovery copies are held only in London (Google Cloud europe-west2 and MongoDB Atlas on AWS eu-west-2). For Australian customers, data is held in Sydney.

Some features rely on third-party processors that may process data in other countries. Most of these are optional and only process your data if you switch the related feature on. Section 6 lists our processors.

5.3 International access and transfers

Our support and engineering teams work from the UK and Australia. Where Australian-based staff access UK customer data to provide support, that access is covered by an International Data Transfer Agreement between Tacklit UK Ltd and Tacklit Group Pty Ltd, using the ICO's mandatory clauses and supported by a transfer risk assessment. Third-party processors outside your region are engaged under appropriate transfer safeguards.

To date, no government or law enforcement body has asked Tacklit to provide customer data. If we ever receive such a request, we will tell you unless the law prohibits it.

5.4 Data retention

Retention periods are configured for each workspace and record type, so your records are kept for as long as the rules that apply to you require, such as the NHS Records Management Code of Practice or Australian state health records legislation. Closed episodes of care become read-only, records cannot be deleted before the configured period ends, and destruction at the end of that period is logged.

6. Third-Party Processors

To provide the very best service, Tacklit works with leading technology partners to deliver some of our platform capabilities. We assess the security, compliance and privacy practices of every provider before we engage them, and bind them to data processing and security terms. Under our Data Processing Agreement, we notify customers of changes to this list and you have the right to object.

Provider	Services they support for Tacklit	Security information
CORE PLATFORM		
Google Cloud Platform	Cloud infrastructure, application hosting, logging, key management and AI services	https://cloud.google.com/security
MongoDB Atlas	Managed database	https://www.mongodb.com/products/platform/trust
Amazon Web Services	Database hosting (through MongoDB Atlas) and session transcription (Amazon Transcribe)	https://aws.amazon.com/security/
Auth0 (Okta)	Identity, login, multi-factor authentication and single sign-on	https://auth0.com/security
Twilio SendGrid	Transactional email	https://sendgrid.com/policies/security/
Retool	Internal admin console for account and workspace configuration (no client clinical data)	https://docs.retool.com/page/security

Provider	Services they support for Tacklit	Security information
OPTIONAL FEATURES (ONLY USED IF YOU SWITCH THE FEATURE ON)		
Twilio	SMS, telehealth video and calls	https://www.twilio.com/legal/security-overview
TNZ	New Zealand SMS	https://www.tnz.co.nz/Docs/Downloads/Security%20Features.pdf
Stripe	Payment processing	https://stripe.com/docs/security/stripe
Airwallex	Payment processing and reconciliation	https://www.airwallex.com/security
Paperform	Dynamic form library	https://trust.paperform.app
Intercom	In-app customer support	https://www.intercom.com/help/en/articles/264-security-at-intercom
Cronofy	External calendar connections	https://www.cronofy.com/compliance-center
Apideck	External accounting connections	https://compliance.apideck.com/security
Healthlink	Secure clinical messaging (Australia and New Zealand)	https://www.healthlink.net
Parchment Health	Australian eScript provision	https://www.parchment.health
GoFax	eFax services	https://support.gofax.com.au/en/fax-security

Provider	Services they support for Tacklit	Security information
INTERNAL AND CUSTOMER COMMUNICATION TOOLS		
Google Workspace	Internal communications and documentation	https://workspace.google.com/intl/en_au/security/
Slack	Internal communications	https://slack.com/intl/en-au/trust/security
Appsmith	Internal data visualisation	https://docs.appsmith.com/product/security
Learnworlds	Customer training and learning content	https://www.learnworlds.com/data-security/
Loops	User email and newsletter	https://loops.so/privacy

7. Assurance and Clinical Safety

7.1 Certifications and independent assurance

Cyber Essentials	Certified, whole organisation. Renewed 10 August 2026, recertification due August 2027.
Penetration testing	Annual independent test aligned to OWASP standards. June 2026: no critical or high severity findings.
NHS Cyber Security Charter for Suppliers	Signatory.
NHS Data Security and Protection Toolkit	Tacklit UK Ltd is registered (ODS code C7P3L) and is completing its first assessment, with publication at Standards Met targeted by 31 December 2026.
Information security management	Aligned to ISO 27001. Our hosting providers (Google Cloud, AWS and MongoDB Atlas) and identity provider (Auth0) hold ISO 27001 and SOC 2.
Data protection registration	Tacklit UK Ltd, ICO registration C2051947.

7.2 Clinical safety

Tacklit manages clinical risk in line with the NHS clinical risk management standard DCB0129. We maintain a Clinical Risk Management System, a Clinical Safety Case Report and a Hazard Log, overseen by a named Clinical Safety Officer who is a registered psychologist with more than 20 years of experience leading mental health service delivery.

7.3 Artificial intelligence

Tacklit's AI features help clinicians with documentation and administration, such as drafting notes and letters, summarising the record and extracting detail from referrals. A clinician reviews every output and makes every clinical decision. AI features are optional and are switched on for each workspace.

7.4 Supporting documents

The following documents are available from the Tacklit Trust Centre or on request:

- Data Processing Agreement (UK and Australia)
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan, and latest data restore test record
- Penetration test summary
- Data Protection Impact Assessment support pack
- Clinical safety documentation (DCB0129)
- Software Bill of Materials (under NDA)

Contact us

Security and information governance: security@tacklit.com
General enquiries and support: support@tacklit.com

Tacklit UK Ltd
128 City Road, London EC1V 2NX
Company number 12700473

Tacklit Australia
2/29 Carlisle Street
St Kilda VIC 3182