Security at Tacklit

V1.3

Last updated August 2021

tacklit

Introduction

At Tacklit, we believe the power of technology can help mental health providers innovate and elevate the efficiency and quality of their care delivery. To deliver on our purpose to help millions of people access proactive, personalised, outcome-driven mental health care we use modern digital touch points to capture and organise relevant information to support our customers.

The digitisation of traditional data collection and engagement requires high-security standards in all areas to protect and secure all user data.

In this whitepaper, we outlined all the appropriate steps and practices we implemented to safeguard privacy and user data.

Executive Summary

- We treat security as a first-class concern at Tacklit. All data (customer records, file attachments, images) that are in transit and at rest are encrypted by default using industry-standard AES 256bit encryption.

- Personally identifiable information is treated with additional encryption to protect this information from our third-party service providers.

- Your data is backed up hourly, weekly, and monthly to ensure we can recover your data in the event of server or database failures.

- Our employees are trained to handle your customer data with utmost care. Access to production environments is restricted to only senior staff with the “least privilege” principle.

- Monitoring and audit logs are enabled in all critical points (infrastructure and databases). This enables us to take appropriate actions to prevent, or mitigate, any potential security issues.

- We adhere to leading health information standards in accordance with HIPAA, GDPR, the UK Data Protection Act and the Australian Privacy Act.

Contents

2. Organisational Security

2.1 Employee training

Tacklit employees undergo quarterly security, privacy and compliance training and are required to complete questionnaires to assess their understanding. The safety and security of our user data is the responsibility of everyone in Tacklit, therefore the security training spans across every role and level of our organisation.

Our management team bring over 50 years combined experience in operating large scale, leading technology companies that informs our recruitment, training and operational procedures for staff.

2.2 Access control to data

Access to the production environment and data is limited to senior management to reduce the risk of login exposure.

Access (least privileged) is provisioned from centralised account management for Tacklit to quickly respond to any compromised accounts. Any additional access granted to our tech team for production support is strictly a need-to-know basis and removed when not needed.

2.3 Two Factor Authentication and Strong Password

Tacklit maintains a strict password policy for logins to all internal or external services including production systems and tooling that Tacklit uses. It is mandatory for everyone in Tacklit to create a strong and complex password with a 60 days rotation cycle and multi-factor authentication as a secondary login validation.

2.4 Incident and security response plan

Our focus at Tacklit is to apply best security practices to safeguard our user data. In the event of any security incident, we have put in place a response plan to triage and resolve the problem as quickly as possible. If any data breach is detected, it is our responsibility to notify all affected users to help limit any further damage. Tacklit strives to ensure similar incidents would not repeat by conducting post-incident reviews and implementing proper corrective and preventive steps.

2.5 Secure endpoints

Tacklit has a stringent policy for the devices such as laptops and mobile devices used to access our tooling and services, we take appropriate precautions to keep them secure. Staff computers are locked with strong passwords, automatically locked when away and disks are encrypted by default. In the event of theft, an encrypted disk prevents anyone from reading the data and Tacklit also enables remote location tracking and the capability to remotely erase data contained within those devices.

3. Application Security

3.1 Data encryption

In Transit

Tacklit is built based on client (your web browser) and server architecture. When using Tacklit, web traffic between your web browser and servers are encrypted by using industry-standard TLS 1.2 protocols and AES256 encryption by default. This secure connection prevents malicious actors from listening to your communications, tampering or forgery anywhere in between your computer and our system.

At Rest

All information that is stored in the Tacklit database is secured by AES 256-bit encryption. For highly sensitive data like patient identifiable information (PII), additional encryption is added to obscure the data. As a result, neither the database administrator nor third party infrastructure staff can read the information.

3.2 File storage

Files such as any documents or attachments that were uploaded are encrypted using AES256 at rest and protected by access control (API level), which logically separates the file access from other Tacklit users. Every file retrieval action is verified against the user's token to validate if it belongs to the owner.

3.3 Authentication - password policy

Tacklit enforces a strong password policy when you or your client create an account. User passwords are then one-way hashed using AES256 to provide extra protection. A combination of hash and strong passwords will make it harder for brute-force attacks, such as using computational methods to guess the password. To combat this, our application detects any potential brute force activity such as too many failed login attempts and locks any high-risk accounts. Our system will automatically notify the affected users via email regarding the suspicious activity.

3.4 Software development process and practices

At Tacklit, we aim to catch security vulnerabilities in our development process and testing phase therefore our primary focus is to design our application with security in mind.

We incorporated security best practices in our development process via peer code review based OWASP leading industry-standard guidelines and methodologies for eg. checking on potential insecure endpoints or exposed access tokens. Private endpoints should only be accessible with valid access tokens and only return data that belongs to the owner.

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

We also use Synk (an industry-leading security and vulnerability scanning solution) as part of our development toolkit. Synk integrates directly into our development workflow allowing static code analysis, dependency scanning and more throughout our development process.

We have integrated dependencies and vulnerabilities scanning into our continuous delivery and build pipeline on third-party libraries. All development cycles go through our quality assurance checks and nightly automated regression tests in a staging environment before any deployment to production systems.

As part of an ongoing effort to stay up to date with cybersecurity trends, we conduct in-depth security reviews and workshops quarterly with our development teams.

4. Operations Security

4.1 Data Centres

The Tacklit platform runs on top of Google Cloud utilising its world-class infrastructure and security. Tacklit employs stringent security practices as per Google Cloud's recommendations to secure the access, data and production environments. Google Cloud's data centres are also protected by multi-layered physical security such as 24-7 surveillance, multi-tiered controlled access to physical hardware and service availability are supported by multi availability zones. Operating systems, databases and services are regularly updated with the latest patches to remove any potential security vulnerabilities.

4.2 Network security

Tacklit isolates testing and development environments from production systems to protect sensitive data. While engineers have access to testing and development environments, access to production systems is restricted to reduce compromised account-related risk.

Network security is a core part of the overall security especially towards detecting network intrusion. Tacklit integrates firewall policies into our network for eg. only whitelisting known IPs, only allows essential network ports. All of our application services only allow system calls from known sources and with validated access tokens. Application system calls are logged and monitored. Alert policies are in place to detect potential intrusion.

4.3 Auditing and monitoring

Central to our security practices, auditing allows us to investigate who, when and what happened in the event of an intrusion. This is critical for our team to examine the scope of a data breach or security-related incidents which help quickly take measures to close any security vulnerabilities and prevent similar events in the future.

Auditing is enabled for all of our production infrastructure and databases by logging database access, IP addresses, time and actions taken. These logs are stored securely for 30 days for analysis and to aid any backdated investigations if needed.

Monitoring prevents potential threats from happening by alerting our tech team to take appropriate steps to respond to malicious actors. Tacklit deploys multiple alerting systems around our application and network to reduce downtime and provides our tech team with the context to troubleshoot and resolve any technical issues.

All application system calls are recorded and alert policies are set up to notify our technical team when incidents are raised. We actively prioritise our investigation into these alerts to resolve any technical issues and prevent any malicious activities.

To safeguard our user's account, all Tacklit logins events are logged to detect any unusual traffic or pattern such as multiple failed login attempts. Too many failed attempts will result in an account being blocked to prevent any password brute force attack. In addition, our technical team will be notified so we could assess if it is a legitimate login issue and help to unblock these users when needed.

4.4 Disaster recovery and business continuity

Tacklit employs several mechanisms to ensure high availability and resiliency. Tacklit services are hosted on Google Cloud platform regionally in Australia, the United Kingdom and in the US. Tacklit's service infrastructures are able to self heal by replacing degraded servers with new instances. Servers are also load-balanced with multiple instances and deployed across multiple availability zones.

Customer data is stored regionally in Amazon Web Services data centres which are designed to be highly redundant and replicated across different servers to improve scalability and availability. This also enables zero downtime in the event of server patches and maintenance. The database platform is also fault-tolerant and has the capability to automatically failover to healthy servers so our services can continue to operate without interruption.

We treat data integrity and availability as just as important. To protect your data against data related failure or data corruption, Tacklit has established thorough backup policies for our databases. Your data is constantly backed-up every 2 hours, weekly and monthly. These backups are also stored securely independently from the infrastructure the database resides on.

4.5 Data Ownership

Tacklit is a Data Processor while you are the Data Controller. This means your data is yours, we don't scan it for marketing, advertising nor sell it to third parties.

In line with our Terms of Use we may create data that is de-identified in accordance with our Privacy Policy. This de-identified information is not Personal Information, because it cannot be used to identify any individual, and may be used by us to help us improve our products and services.

Tacklit customers retain the rights to their data ownership. If you request to migrate to another system we will support you by enabling you to make a copy of all your data to move securely.

If a request for data erasure is made, Tacklit will take appropriate steps to mark the data for deletion. The access to the data will be immediately made unavailable and any deletion or removal is done in accordance with our privacy policy.

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

5. Key Policies

5.1 Adherence to required legislation

As a global technology company, Tacklit complies with the specific rules and regulations for each geography in which we operate in relation to the way we gather and handle data.

In the UK we adhere to GDPR and the Data Protection Act. The detail is outlined in our Terms of Use, End User Licence agreement, our Data Processing Agreement and Privacy Policy. In Australia we adhere to the Australian Privacy Act. The detail is outlined in our Terms of Use, End User Licence agreement and our Privacy Policy.

5.2 Data Residency

Tacklit ensures all customer data resides and is processed 'on shore' in their country of origination. This policy extends to third-party services providers we use. For UK customers, data is stored in London data centres where Australian customer data is stored in Sydney data centres.

6. Third-Party Processors

To provide you with the very best service Tacklit partners with world leading technology partners to enable some of our platform capabilities.

We conduct a rigorous assessment of the security of our third-party providers to ensure they employ appropriate levels of security, compliance and privacy policies.

We work with the following, highly reputable providers:

Provider	Services they support for Tacklit	Security information
Google Cloud Platform	Cloud infrastructure	https://cloud.google.com/security
Auth0	Account management	https://auth0.com/security
MongoDB	Data storage	https://docs.mongodb.com/manual/security/
Twilio	SMS and other messaging	https://www.twilio.com/legal/security-overview
SendGrid	Email	https://sendgrid.com/policies/security/
Helpscout	Online customer support	https://www.helpscout.com/company/legal/security/
Sentry	Application error monitoring	https://sentry.io/security/
Stripe	Payment processing	https://stripe.com/docs/security/stripe