IT HANDBOOK

JONATHAN MORRICE - NOVEMBER 2017

perdoo

OVERVIEW

Protecting our customer’s data is the most important thing we do at Perdoo. Due to the nature of the data we store, our users have extremely high expectations when it comes to protecting their data. We understand how important the responsibility of safeguarding this data is to our customers and work hard every day to maintain that trust.

As part of the onboarding process you are obligated to read this document, as well as our Terms & Conditions and Privacy Policy to learn more about our commitment to providing security services.

TWO FACTOR AUTH

You are strictly required to enable two-factor authentication (2FA) and to comply with our password policies for all services that you use. These include Slack, ZenDesk, Chatlio, Heroku, GitHub, Google, Mixpanel, Segment.

As the second factor, it's recommended to use either SMS or the Google Authenticator app if you own a smartphone. We run monthly checks to ensure 2FA is enabled for all users in each service and your account access will be blocked if you cannot comply.

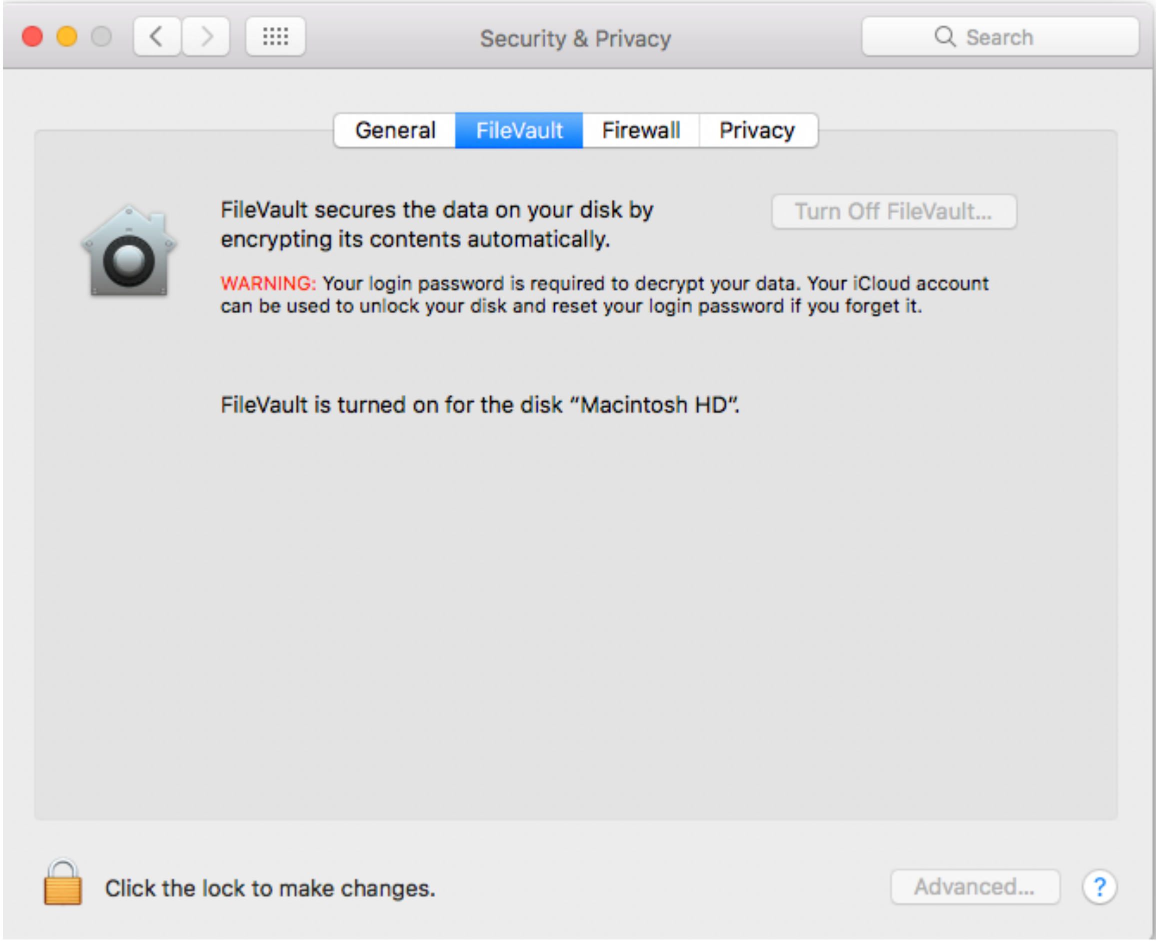
DATABASE ACCESS

Database access is restricted entirely to the Backend Engineering team. All Backend Engineers have access to our Dev and Stage PostgreSQL databases, however access to our production databases is restricted to the following people:

Jonathan Morrice
Co-founder & CTO
+49 173 954 1562
jonathan@perdoo.com

HD ENCRYPTION

Every laptop handed out to Perdoo employees will have an encrypted hard-drive on default. You are required to keep this feature enabled at all times. Should you ever need to rebuild your machine, make sure to re-enable HD encryption from the systems settings under 'Security & Privacy'.



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: Your login password is required to decrypt your data. Your iCloud account can be used to unlock your disk and reset your login password if you forget it.

FileVault is turned on for the disk "Macintosh HD".

Click the lock to make changes.

PASSWORD POLICY

When setting a password for the cloud services we use, you are required to adhere to the following requirements:

- Avoid using the same password twice (e.g., across multiple user accounts and/or software systems).
- Avoid character repetition[citation needed], keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past) and biographical information (e.g., ID numbers, ancestors' names or dates).
- Avoid using information that is or might become publicly associated with the user or the account.
- Avoid using information that the user's colleagues and/or acquaintances might know to be associated with the user.
- Do not use passwords which consist wholly of any simple combination of the aforementioned weak components.

PASSWORD POLICY

- Avoid character repetition[citation needed], keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past) and biographical information (e.g., ID numbers, ancestors' names or dates).
- Avoid using information that is or might become publicly associated with the user or the account.
- Avoid using information that the user's colleagues and/ or acquaintances might know to be associated with the user.
- Do not use passwords which consist wholly of any simple combination of the aforementioned weak components.

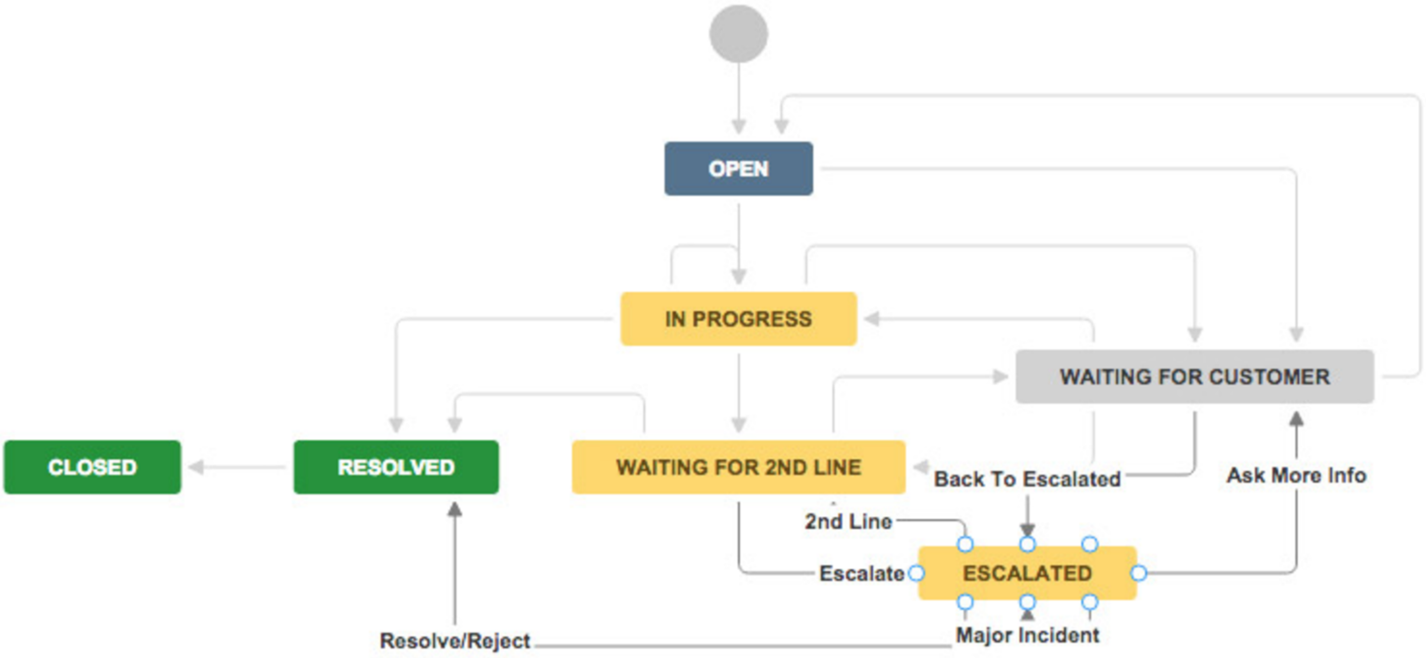
SECURITY AUDITS

Once a year we work with a well-regarded third-party auditor to check our systems for security vulnerabilities of any kind.

We use services like Papertrail and Rollbar to provide an audit trail over our infrastructure and the Perdoo application. Auditing allows us to do ad-hoc security analysis, track changes made to our setup and audit access to every layer of our stack.

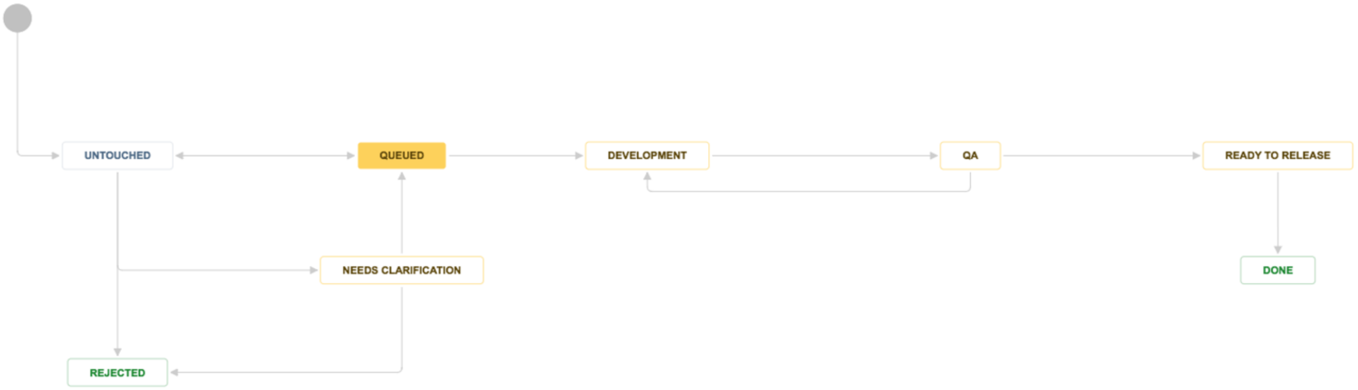
ISSUE ESCALATION

The following workflow is embedded in our JIRA environment for escalating issues as reported by customers



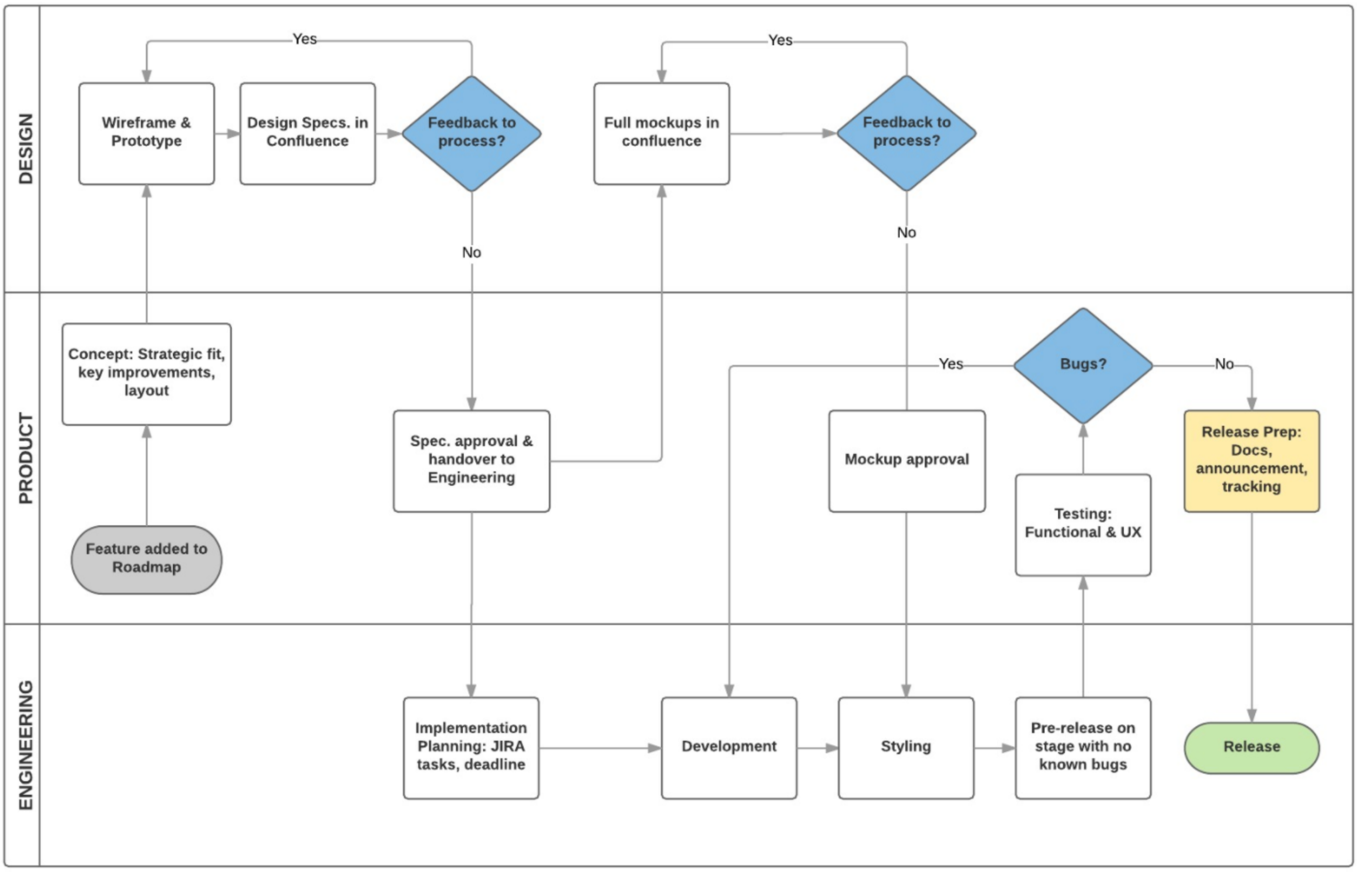
BUG HANDLING PROCESS

The following workflow is embedded in our JIRA environment for handling minor bugs reported internally or externally

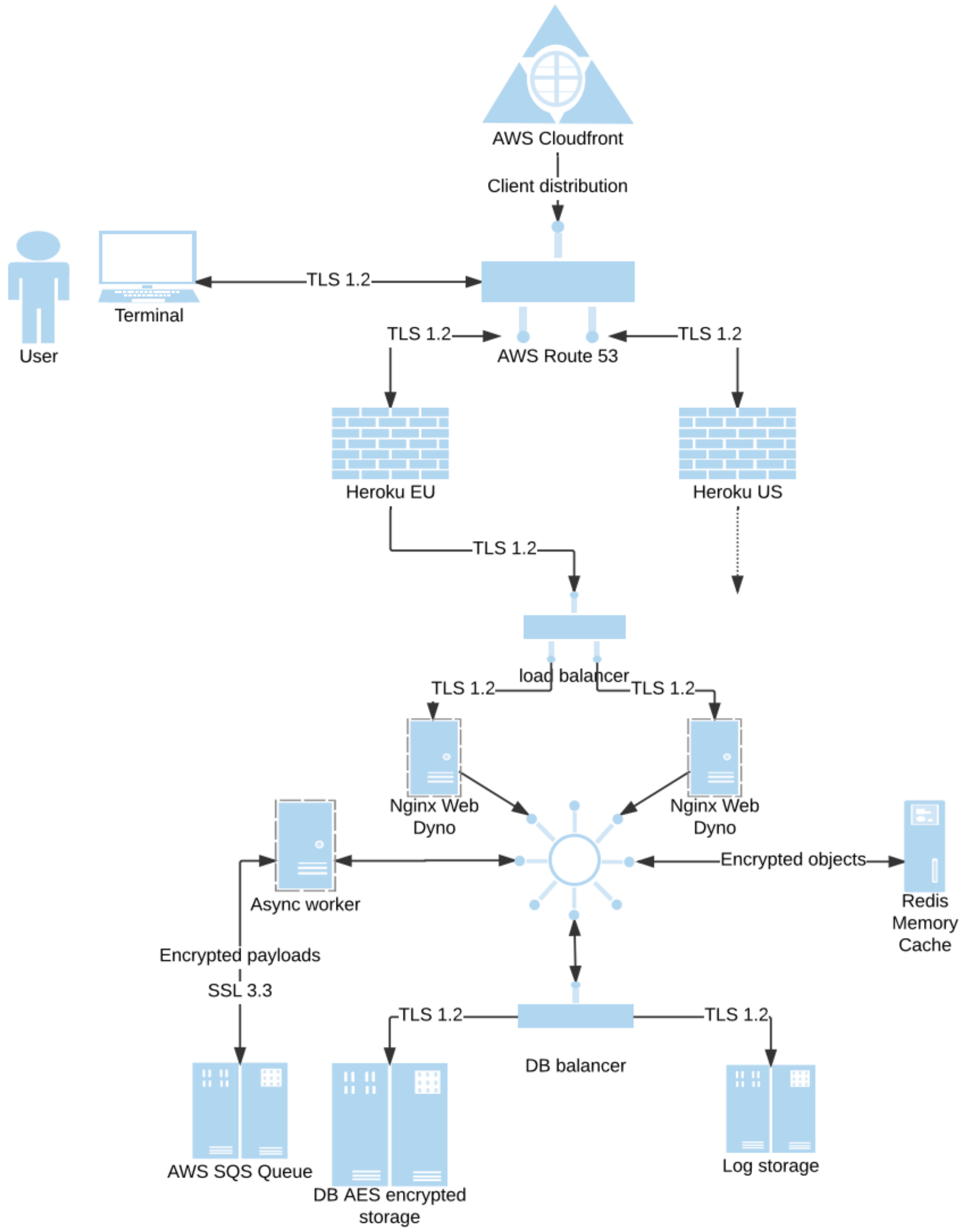


FEATURE DEVELOPMENT

Once a feature is added to our internal product roadmap by one of the PMs, it enters the following process:


DESIGN
PRODUCT
ENGINEERING
Wireframe & Prototype
Design Specs. in Confluence
Feedback to process?
Yes
No
Full mockups in confluence
Feedback to process?
Yes
No
Concept: Strategic fit, key improvements, layout
Feature added to Roadmap
Spec. approval & handover to Engineering
Mockup approval
Bugs?
Yes
No
Testing: Functional & UX
Release Prep: Docs, announcement, tracking
Implementation Planning: JIRA tasks, deadline
Development
Styling
Pre-release on stage with no known bugs
Release

ARCHITECTURE


AWS Cloudfront
Client distribution
User
Terminal
TLS 1.2
TLS 1.2
AWS Route 53
TLS 1.2
Heroku EU
Heroku US
TLS 1.2
load balancer
TLS 1.2
TLS 1.2
Nginx Web Dyno
Nginx Web Dyno
Async worker
Encrypted objects
Redis Memory Cache
Encrypted payloads
SSL 3.3
TLS 1.2
DB balancer
TLS 1.2
AWS SQS Queue
DB AES encrypted storage
Log storage