Wingmate

Security Assessment

Preamble

This document was prepared in response to a Vendor Security Assessment request. Sections are laid out below, along with descriptions and details relating to Wingmate's security process, policies and architecture.

Service Introduction

1. Business Information

a) Company name: Wingmate / Gopher Leads Inc. (d/b/a "Wingmate")
b) Responder Name: Michael Jarema, Matt Leuschner
c) Responder Contact Information: mike@wingmateapp.com/905-399-4291, ml@wingmateapp.com/416-550-6580
d) Date of Response: Nov 15, 2019

2. Company Profile

a) Company Website URL: https://wingmateapp.com/
b) Service Website URL: https://fly.wingmateapp.com/

3. Service Scope Question

a) Name of application or service being provided: Wingmate
b) Description of application or service:
Wingmate is a SaaS system which allows a company's network (technicians, employees, customers, etc) to submit leads from the field. Users use a mobile application to capture, describe and submit leads which are then submitted to the sales team. Wingmate also provides sales teams with a full-featured CRM system to manage and work leads to completion, and various means by which to interface with 3rd party CRM systems.

c) What technology languages/platforms/stacks/components are utilized in the scope of the application?
Our iOS application is built using Objective-C and Swift. Our Android application built in Java. Our web application and backend system is built using Ruby on Rails, deployed to Heroku (PaaS), using PostgreSQL (managed database via Heroku), Redis (managed datastore via Heroku), Memcached (managed caching system provided by Redis Labs), Papertrail (managed logging system provided by Papertrail Inc.), New Relic (application performance monitoring provided by New Relic Inc.), Stripe (credit card handling and processing), Cloudflare (DDOS and breach mitigation), and Bitbucket (source code management) to support our application.

4. Service Hosting

a) Is your service run from your own (a) data center, (b) the cloud, or (c) deployed-on premise only: (b) the cloud

b) Which cloud providers do you rely on?
Heroku (primarily), Redis Labs, Papertrail, each of which relies on Amazon AWS. Also, Cloudflare, New Relic, Customer.io, Bitbucket by Atlassian, Backblaze, and Updown.io.

c) Have you researched your cloud providers best security practices?
Yes, covered in-depth for our main providers here: Heroku (https://www.heroku.com/policy/security), Stripe (https://stripe.com/docs/security/stripe), Cloudflare (https://www.cloudflare.com/privacypolicy/)

d) Which data centers/countries/geographies are you deployed in? Heroku US region.
e) On-premise solution only: no
f) Hybrid Solution (on-premise, cloud): no

5. Supporting Documentation

a) Most recent Application Code Review or Penetration Testing Reports (carried out by independent third-party):
We have engaged Acunetix and Praetorian to see if a penetration test is feasible for us at this stage.

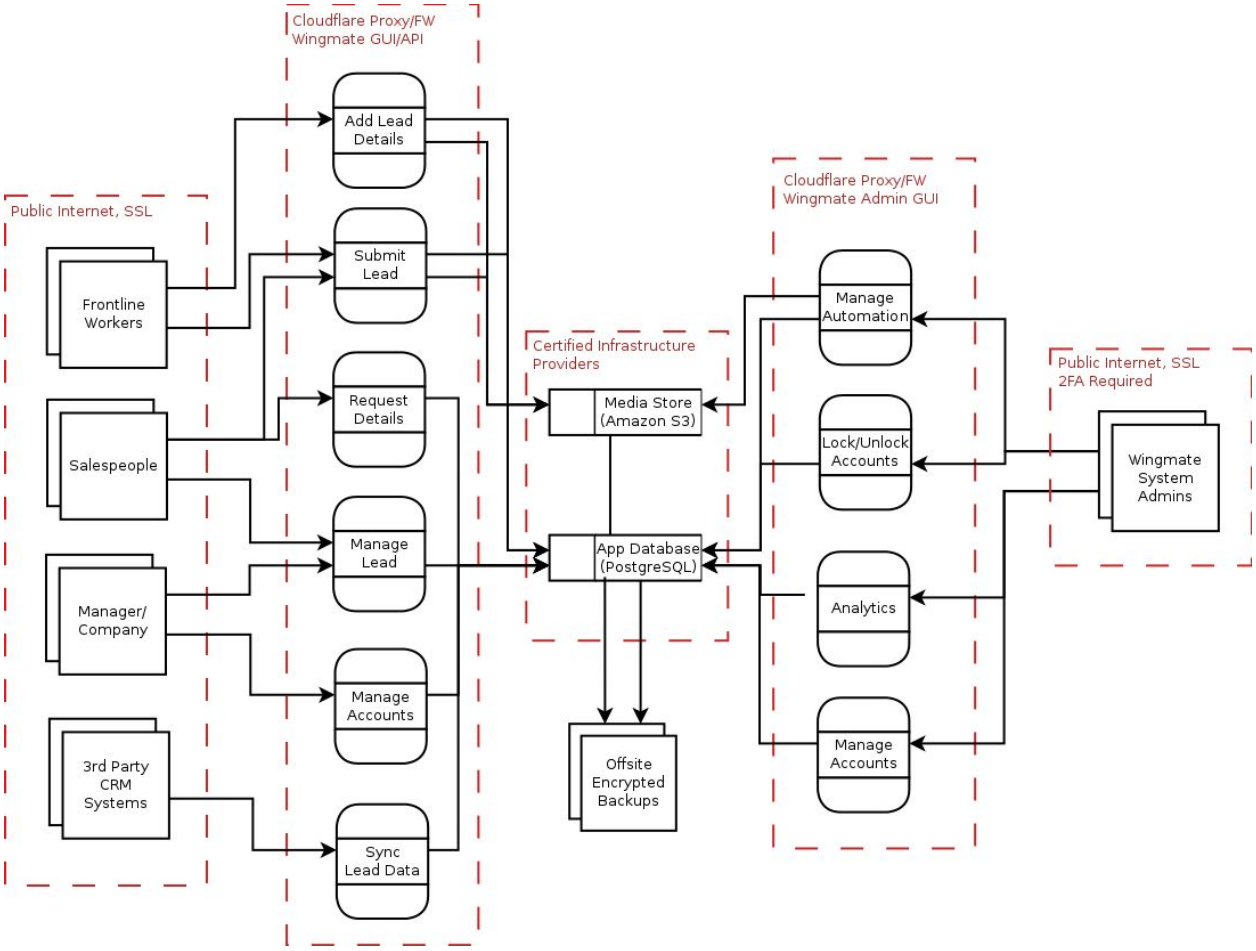
In addition to seeking out a pen-testing/security audit vendor, we've established a responsible disclosure policy to encourage would-be infiltrators to contact us with details in exchange for a bug bounty. Details here: https://wingmateapp.com/responsible-disclosure/

leverage

b) Information Security Policies and Procedures:

- Data Classification Matrix *(download xls)*
- Responsible Disclosure Program
- Web App Security Policy
- Risk Management Program
- Acceptable Use Policy

c) Data Flow Diagram:



d) Any other Documents supporting your responses in this questionnaire (Please provide a description for each document):

- Data Classification Matrix *(download xls)*
- Responsible Disclosure Program
- Web App Security Policy
- Risk Management Program
- Acceptable Use Policy

e) PCI, SOC2 type II or ISO27001 certification reports:

None awarded to Wingmate directly, however our systems are powered primarily by Heroku and Cloudflare with payment processing handled exclusively by Stripe. Some backups are managed using Backblaze.

Heroku is certified under PCI DSS Level 1, HIPAA, ISO 27001, 27017, 27018 and SOC 1, 2, 3. Details here: https://www.heroku.com/compliance

Heroku uses Amazon AWS data-centers, which are certified under ISO 27001, SOC 1, SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley SOX. Compliance details are available here: https://aws.amazon.com/compliance/programs/.

Cloudflare's systems are certified under ISO 27001:2013, SOC 2 Type II, SOC 3, and PCI DSS 3.2.1. Compliance details are available here: https://www.cloudflare.com/compliance/.

Stripe's systems is certified as a PCI Level 1 Service Provider. Compliance details are available here: https://stripe.com/docs/security

Backblaze, a backup provider we use, is PCI compliant:
https://help.backblaze.com/hc/en-us/articles/360022452253-PCI-Compliance

f) Other Independent Audit report (please provide details):
We plan to use the engagement described in 5(a) to guide us as to what, if any, additional auditing is appropriate next.

Security CORE Controls

Data Classification

1. Please describe the customer data you require to provide your service: personal information, financial data, confidential/sensitive data, government data

Personal information:
customer details (company name, company address), individual user details (full name, mobile phone number, most recent login IP, email addresses, hashed passwords)

Financial data:
payout method preference (excludes any bank account or credit card information, which is instead handled by our payment vendor Stripe)

Confidential/sensitive data:
lead details (address, geolocation, associated media and comments, comments by team members working the leads)

Government data: none

2. Please upload your data classification matrix including data definition, access restrictions and minimum controls specific for your service

See Wingmate Data Classification Matrix spreadsheet.
https://wingmateapp.com/wp-content/uploads/2019/11/Wingmate-Data-Classification-Matrix.xlsx

Wingmate Data Classification Matrix

	Existential Risk	High Risk	Medium Risk	Low Risk
Description	Protection of the data is required by law/regulation, or the loss of confidentiality, integrity, or availability of the data or system could have an existential adverse impact on our company (safety, finances, or reputation).	The data identifies customer individuals outside of our system, has a tangible financial or competitive benefit for our clients, or the loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our company (safety, finances, or reputation).	The data is not generally available to the public, or the loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our company (safety, finances, or reputation).	The data is intended for public disclosure, or the loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our company (safety, finances, or reputation).
Corporate Information	-	System administration credentials, vendor credentials/API keys, production secrets, source code, production system backups	Corporate structure, access to staging systems	Public facing website, corporate filings, executive team identities
Personal Information	-	Customer individual data (full name, mobile phone numbers, email addresses)	Customer corporate data (company names, company address/emails), customer individual data (login IPs, hashed passwords)	-
Financial Information	-	-	Payout method preferences	-
Customer Confidential Information	-	Lead details (address, geolocation, associated media and comments, comments by team members working the leads)	-	-

Note that we've included an existential risk column. It is our goal to avoid any data which, if breached, may result in an existential or prosecution risk for our business. If a feature or product development requires us to track and store such information, then it needs to be explicitly discussed and signed off on by senior management before proceeding with development.

Encryption

3. How do you encrypt customer data? Please upload relevant documentation
Our data is stored in Heroku's managed PostgreSQL database, connecting via an SSL connection (TLSv1.2, ECDHE-RSA-AES256-GCM-SHA384 cipher) using strong random credentials (> 320 bits of entropy). Data is encrypted at rest, details here: Heroku PostgreSQL Data encryption

Data Access & Handling

4. Which groups of staff (individual contractors and full-time) have access to customer personal and sensitive data?
Only those with system admin access; currently the President, Customer Success Managers (2) and the CTO.

5. Describe how offsite backups occur and how they are secured
Our production Postgres database has continuous protection enabled, and daily snapshots, handled by Heroku as described in: Heroku Postgres Data Safety and Continuous Protection.

Our clients' lead media (images, audio recordings) are stored in Amazon's S3 service. Stored content has 99.999999999% durability and 99.99% availability characteristics. Further described in: Data Protection in Amazon S3.

We also perform daily snapshots of both our production database and all client lead media. These are stored and encrypted, on both a company system and backed up to Backblaze (same data durability/availability as Amazon S3, see: Backblaze Security).

Authentication

6. How are passwords hashed?
Passwords are hashed using BCrypt, using unique per-user salts, with a cost factor of 14.

7. Is MFA required for employees/contractors to log in to production systems?
MFA is required for system administration access. All logins are required to complete 2FA using a TOTP provided by the Google Authenticator mobile app.

Optional MFA for client access is planned but not yet available to our customers.

Management Program

8. Do you have a dedicated information security team? If so, what is the composition and reporting structure?
We do not currently have a dedicated team. This is something that is managed in part by our CTO and President.

9. Do you have a formal Information Security Program (InfoSec SP) in place?
Yes

10. Please describe your Information security risk management program (InfoSec RMP)?
Linked here:
https://wingmateapp.com/wp-content/uploads/2019/11/Wingmate-Risk-Management.pdf

Policy Execution

11. Please ensure your documented information security policy has been uploaded in section in 'Service Overview'
Linked here:
https://wingmateapp.com/wp-content/uploads/2019/11/Wingmate-Web-Application-Security-Policy.pdf

12. Do your information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?
Our security and privacy policies generally align with industry standards. That said, our systems are powered primarily by Heroku and Cloudflare with payment processing handled exclusively by Stripe. Backblaze is used for some backups.

Heroku is certified under PCI DSS Level 1, HIPAA, ISO 27001, 27017, 27018 and SOC 1, 2, 3. Details here: https://www.heroku.com/compliance

Heroku itself uses Amazon AWS data-centers, which are certified under ISO 27001, SOC 1, SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley SOX. Compliance details are available here: https://aws.amazon.com/compliance/programs/.

Cloudflare's systems are certified under ISO 27001:2013, SOC 2 Type II, SOC 3, and PCI DSS 3.2.1. Compliance details are available here: https://www.cloudflare.com/compliance/.

Stripe's systems is certified as a PCI Level 1 Service Provider. Compliance details are available here: https://stripe.com/docs/security

Backblaze is PCI compliant:
https://help.backblaze.com/hc/en-us/articles/360022452253-PCI-Compliance

13. Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?
Immediate questioning followed by dismissal.

Confidentiality

14. Are all personnel required to sign Confidentiality Agreements to protect customer information, as a condition of employment?
Yes

Acceptable Use

15. Are all personnel required to sign an Acceptable Use Policy? Please attach
Linked here:
https://wingmateapp.com/wp-content/uploads/2019/11/Wingmate-Acceptable-Use-Policy-N.pdf

Network and Application Security Testing

16. How do you test the security of your network and applications? Internal, third parties or both? If so, what is the cadence? Explain your methodology
Regarding a corporate network, we don't have an internal network. Rather, our company is organized around Google's GSuite for email, document management and collaboration. Details on their security architecture are here: G Suite Security and Trust

For our web application, we rely on Heroku and Cloudflare primarily for network security. Heroku's network security policies are here: Heroku Security. In summary, Heroku relies on Amazon's secure, accredited data centers to house and operate all servers and services. Cloudflare's network security product is described here: Cloudflare Security Solutions. It includes DDOS protection, and customer data breach and bot prevention.

Finally, wherever possible, we leverage certified (ISO 27001, PCI, etc.) 3rd party providers with track records of security excellence, and benefit from their expertise through our use of their hardened systems.

Finally, we have engaged Acunetix and Praetorian to see if a penetration test is feasible for us at this stage.

Vulnerability Management/Patching

17. Network/Host Vulnerability Management. Please summarise or attach your network vulnerability management processes and procedures (specifying who executes the procedures and the tools used)?

Our company is organized around Google's GSuite for email, document management and collaboration. We rely on their systems and security teams for vulnerability management, handling of threat identification and mitigation as it pertains to our use of those services and company resources.

18. Application Vulnerability Management. Please summarise or attach your application vulnerability management processes and procedures (specifying who executes the procedures and the tools used)?

Our application is deployed to Heroku, which monitors security advisories/bulletins, and handles patching of their systems and rollouts in a transparent manner. Cloudflare, acting as a proxy/firewall in front of our web-facing systems, employs similar proactive security measures.

Detailed notes regarding Heroku's server and platform changes, including those in response to server or OS vulnerabilities, are found on the Heroku Changelog.

In addition, our application relies on Ruby on Rails, an open-source web development framework. Heroku also alerts our dev team when our framework or components/libraries are identified in security advisories/bulletins or are entering an EOL phase. At this point, our dev team schedules a framework/library update and testing task. Typically this task involves reviewing framework/library changelogs, making the necessary code changes required to support updated framework/library APIs, and inclusion of new regression tests to ensure coverage of new/changed functionality. Prior to production deployment, we ensure all regression tests are passing. This process is managed by our CTO and executed by any senior developer on the team.

Finally, we rely on Heroku's and Cloudflare's security teams to identify, manage and patch vulnerabilities on their servers.

19. Production Patching. How do you regularly evaluate patches and updates for your infrastructure?

Our production systems are managed by our vendors: GSuite, Heroku, Cloudflare. See answers to 17 & 18 for a description of their processes.

20. Production Patching. How does the criticality of the patch (critical, high, medium, low) affect deployment guidelines?

Our production systems are managed by our vendors: GSuite, Heroku, Cloudflare. See answers to 17 & 18 for a description of their processes.

Endpoint Security - End-User

21. Are all endpoint laptops that connect directly to production networks centrally managed?
All laptops are issued to employees by Wingmate and are connected to our network (GOPHER WIFI). Laptops are locked with admin access. Employees are restricted by the device from downloading any software that is not approved by admin. Emails, documents and password resets are all accessible to one admin. As a 3rd party line of defence, we've deployed Desktop Central to all Wingmate issued devices.

22. Describe both standard employee issued device security configuration/features and required BYOD configurations. (Login Password, antimalware, Full Disk Encryption, Administrative Privileges, Firewall, Auto-lock, etc.)

- Login passwords required: minimum 8 characters, no reuse, at least one number & symbol
- Administrative privileges locked
- Execution of untrusted applications is disabled. All software downloads are restricted by device and must go through the admin
- Auto-lock laptops after 30 minutes
- Desktop central is used to manage devices used by Wingmate personnel

Endpoint Security - Production Server

23. What systems do you have in place that mitigate classes of web application vulnerabilities? (e.g.: WAF, proxies, etc)
We rely on Cloudflare and Heroku as a front line of defense to mitigate web application threats.

Specifically:
Cloudflare acting as a proxy/WAF - DDOS mitigation through their expansive network footprint and expertise at identifying patterns of network traffic consistent with attacks, Data Breach Prevention by blocking DNS Spoofing, in-transit data snooping, brute-force login attempts and malicious payload exploits. Details here: https://www.cloudflare.com/security/

Heroku CVE monitoring - for critical CVEs, Heroku scans their system for affected applications and alerts us if our application is impacted, allowing us to proactively address vulnerabilities rather than wait for them to be exploited. Heroku also proactively monitors and secures their infrastructure as per https://www.heroku.com/policy/security.

24. Do you have operational breach detection systems, deception solutions and/or anomaly detection with alerting?
Not within our web application. However, for both GSuite and Cloudflare, their large network footprint allows them to identify patterns in abusive network traffic and proactively block access to our company resources (in GSuite) or to block access to our web application (fronted by Cloudflare).

The sophistication of these providers is vastly beyond what we're able to achieve given our limited resources and focus on the development of our web application.

Infrastructure Security

25. Secrets Management. Describe your secrets management strategy:(auth tokens, passwords, API credentials, certificates)
Secrets exist in two places: 1) production system dashboard on Heroku and 2) in an encrypted backup with the CTO. Access to the production dashboard is limited to technical leadership and managed according to Heroku's security policies. The backup is encrypted with the 256-bit AES algorithm and backed-up to the cloud.

26. Logs. Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?
Access to our company resources (email, documents, calendars) is done through Google's GSuite. GSuite has an extensive audit trail which covers logins, document sharing, calendar events, and more which is accessible to our GSuite administrator.

SSH access is not required to manage our production application. Our application is deployed to a managed PaaS (Heroku) and proxied through a threat detection system (Cloudflare), so SSH sessions and privilege escalation aren't viable nor tracked. Production application configuration changes within Heroku are logged in Heroku's dashboard, whereas application access (for customer use and system admin use) is logged to Papertrail.

Cloudflare keeps track of high-level metrics (number of threats averted, geographic source of threats) and maintains an audit log of all account changes, see Understanding Cloudflare Audit Logs

27. Network Security. Is the production network segmented into different zones based on security levels?
No, not feasible for our size and network requirements. Besides, critical systems (GSuite, Heroku, Cloudflare) are managed by 3rd party vendors and subject to their own stringent security policies.

28. Network Security. What is the process for making changes to the network configuration?
None. Our company resources/email are hosted by Google's GSuite, so access is web-based using SSL. Our application is deployed to Heroku which has its own internal means of HTTP routing, connectivity between the application and database systems. We rely on Heroku's network engineering teams to manage our production application's network configuration.

Cryptography

29. Cryptographic Design. What cryptographic frameworks are used to secure a) data in transit over public networks, b) passwords, c) data at rest?

a) All web traffic to/from our production application servers as well as traffic to/from GSuite for our company resources is protected by SSL/TLS. Cloudflare is our SSL/TLS provider for web traffic.
b) Passwords within our system are salted and encrypted using BCrypt with a cost factor of 14.
c) Customer data, when at rest in our production application database, is secured as outlined here: Heroku PostgreSQL Encryption

30. Key Management. How are cryptographic keys(key management system, etc) managed within your system?
SSL keys/certificates are managed by Cloudflare; we trust them to handle our certificates in a secure manner in accordance with their stringent security policies.

Beyond that, our production application secrets are stored and managed as described in 40 - API Management. They're stored within Heroku's platform dashboard where access is limited to Wingmate leadership and also backed up in an encrypted form on one of our systems. Access is limited exclusively to our technical leadership. In the unlikely chance, our production secrets are lost from Heroku's dashboard and the backup fails, these can be reset with minimal effort by our 3rd party vendors.

Security Awareness

31. Describe your security awareness program for personnel
Our goal is to ensure that everyone at Wingmate has an appropriate level of know-how about security, along with a proper sense of responsibility. Every Wingmate employee is required to review our documents listed in section 5.b. These documents can also be found on our Privacy & Security page here. Employees must illustrate a full understanding of our policies and are tested & monitored periodically throughout the year.

Measures include; sample phishing emails, security training and questioning, annual formal review of policies. We train:

1. When they join the team
2. If an incident occurs (dependant on severity, dismissal may be necessary)
3. At regular intervals

Security is an important part of the conversation at Wingmate. Upper management regularly communicates to all employees that security is essential to running the business. This can take the form of company-wide emails, presentations, brown-bag lunches, or some combination of the above. Communication is clear, regular, relevant, and interactive.

Security training is an ongoing process that we continue to modify and amend as Wingmate grows and changes. That's part of ensuring that our security posture is as mature as it can be based on where we are as a company, and we can protect company & client information respectively.

Monitoring

32. How do you log and alert on relevant security events? (this includes the network and application layer)?

We use updown.io for application availability monitoring, it checks, minute-by-minute for available of our production application and alerts our dev team if the application is unavailable or if there are erroneous responses.

Cloudflare proactively tracks and blocks threats to our production system, see 23 - Endpoint Security - Production Server.

Heroku's logging system notifies our dev team of application request failures beyond a certain threshold (> 5% of requests) within 5 minutes of the start of the event.

Incident Response

33. Describe or attach your Security Incident Response Program?

In the event of a data breach or network attack, our tech leadership will assess and execute the following steps as necessary:

Mitigation

1. Set application to "Under Attack" mode in Cloudflare
2. Block any identifiable IPs or geographic regions involved in the attack.
3. Lock any suspected/compromised accounts within our web application or GSuite.

Notify

1. Email our users that our web application is under attack or we suspect unauthorized access has occurred. Describe briefly the mitigation steps which are in-effect and explain any impact on our users' ability to access our system. Request password resets if

appropriate and commit to sending out timely updates as we discover further details about the issue.

Survey

1. Check logs, audit trails of all of our systems to determine where and to what extent an attack or unauthorized access has occurred.
2. Compare our production data set to recent backups to determine any changes to our data.
3. Use our data classification matrix to determine the severity of any compromised data.
4. Determine exactly which users are impacted, as informed by the above steps.

Recover

1. Redirect all effort necessary to resolve the attack or harden the unauthorized access points within our application.
2. Email detailed notice to those who were affected. The content of the email will be informed by the severity of the issue/data breach. A high-risk breach will require careful handling. In any case, the notice should contain an overview of what happened, how it happened, what was compromised, and how we're going to prevent similar attacks/issues in the future.

Incident Communication

34. Do you have formally defined criteria for notifying a client during an incident that might impact the security of their data or systems? What are your SLAs for notification?
Our policy on notifying customers on any security issues is as follows, and is driven by the sensitivity of the data as highlighted in our Data Classification Matrix.

All customers should be emailed a general, high-level notice indicating that a security issue is suspected and that we're working to investigate it. This notice should briefly describe any mitigation steps which are in effect and explain any impact on our customers' ability to use our system. It should also commit to sending out timely updates as we discover further details about the issue. This email should go out within 2 business hours of the discovery of the issue.

As an incident investigation unfolds, our team will determine where on our Data Classification Matrix any affected/breached data lies.

High-Risk data breaches require one-on-one emails and/or phone calls to affected clients, to describe the data that was affected, how it happened, advice on steps for our client to take to protect themselves, as well as a detailed outline on how we plan to prevent the issues from happening again.

Medium Risk and Low-Risk data breaches require a mass email to the affected userbase. This email will describe the affected data, a clear description of how sensitive the data is, how it happened, as well as a detailed outline on how we plan to prevent the issue from happening again.

These follow up emails should go out within 2 business days of the initial incident occurring, but may be delayed due to resolution efforts and ability of the dev team to provide the required details.

Secure SDLC

35. How do you ensure code is being developed securely?

Here are a few high-level mandates that help us keep security in mind during development:

- Secret management. At no point should any secrets/API keys be included in source code or tracked in our source code repository. They should be supplied by the application environment, with separate secrets/keys in use for development, staging and production environments. Finally, access to production keys must be limited to technical leadership.
- Require relevant OWASP (Open Web Application Security Project) security cheats be reviewed during feature architecture and development so that 1) obvious security considerations become top-of-mind and 2) developers have actionable security strategies relevant to their current task
- Using git-flow. Git-flow is a source code branching methodology that makes parallel development very easy but cleanly distinguishes new development from finished work to allow for isolated testing and code review of new functionality. This permits our development team to more clearly assess security considerations both during coding and code reviews.

In addition, any new data introduced into the system must be cleared with technical leadership and mapped to our Data Classification Matrix. New high- or existential risk data should be avoided if at all possible. Certified and proven 3rd party providers (eg. Stripe for payment processing) should be leveraged instead, if possible.

36. How do you train developers in SSDLC / Secure Coding Practices?

We require new developers to review the following at hire, and existing development team members to review annually, the following:

- The Twelve-Factor App architecture, which in addition to covering performance and code architecture concerns, enforces an application structure which separates config (including secrets) from code and strongly establishes the notion of separate environments for separate use cases.

- Watch and understand OWASP's List of Top 10 Application Security Vulnerabilities, meant to give awareness to the types of issues plaguing applications and attack strategies employed by hackers

Finally, the first couple of sensitive development tasks completed by a new developer are to be scrutinized by senior developer staff, specifically with security considerations in mind. This review shall provide concrete feedback to the new developer regarding their ability to mitigate any security concerns.

Authentication

37. Please describe how you authenticate users: If passwords are used, describe complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options. If different service tiers are available, please describe.
Our application has two tiers of user accounts:

1) Customer accounts. Access is limited to data contributed by and concerning only the company to which these customer accounts belong. Passwords are required to be at least 4 characters long (intentionally short to prioritize convenience for access from mobile devices, especially for front-line staff/drivers). Our system allows for 5 login attempts before locking accounts in order to mitigate the risk of a brute force password attack. Passwords are hashed using BCrypt at a cost factor of 14.
2) System administration accounts. Meant for cross-customer administration. Passwords are required to be at least 8 characters long and users are locked out after 5 failed attempts. 2FA with TOTP using Google Authenticator is required due to account sensitivity. Passwords and 2FA seeds are hashed using BCrypt at a cost factor of 14.

Our web application app does not support SSO.

Role Based Access Control

38. Does your application enable custom granular permissions and roles to be created? Please describe the roles available
Yes.

At a high level, we have two levels of access to our web application: (1) system administrator and (2) customer accounts. System administrator roles are confined to Wingmate personnel and allow for high-level management/configuration of customer accounts. Some Wingmate personnel are not granted system administrator capabilities, but rather have permissions limited to the customer accounts to which they're assigned to serve.

All customer accounts are much more limited in scope. A customer account can be assigned to one or more projects (known as “campaigns”) within our system, but each campaign to which they are assigned must fall under the same company account. This is to ensure that each company has a private silo of its own proprietary data within Wingmate.

Audit logging

39. Which audit trails and logs are kept for systems and applications with access to customer data?

Access to our company resources (email, documents, calendars) is done through Google’s GSuite. These contain customer details/PII such as email correspondence, proposals, meeting requests. GSuite has an extensive audit trail which covers logins, document sharing, calendar events, and more which is accessible to our GSuite administrator.

Our web application, which contains customer data (see 1 - Data Classification), is deployed to a managed PaaS (Heroku) and proxied through a threat detection system (Cloudflare). Production application configuration changes within Heroku are logged within Heroku’s dashboard, whereas application access (for customer use and admin use) is logged to Papertrail.

Cloudflare keeps track of high-level metrics (number of threats averted, geographic source of threats) and maintains an audit log of all account changes, see Understanding Cloudflare Audit Logs.

API Management

40. How does your application store API keys?

Secrets, including API keys, exist in two places: 1) production system dashboard on Heroku and 2) in an encrypted backup with the CTO. Access to the production dashboard is limited to technical leadership and managed according to Heroku’s security policies. The backup is encrypted with the 256-bit AES algorithm, and stored locally and backed-up to Backblaze.

In the unlikely chance, our production secrets are lost from Heroku’s dashboard and the backup fails, these can be reset with some effort by our 3rd party vendors.

Internal Audits

41. How do you conduct internal audits (audits lead by your personnel) of the service? please describe the scope, remediation process and frequency of audits.

With respect to our production application, all code is audited by code review as it progresses through our development process.

Our development process is managed as follows. The whole development team has the ability to build features, fix code bugs, conduct code maintenance work within our source code repository and deploy their work to our testing and staging environments. However, all code:

1. Must have a minimal amount of code coverage within our test suite (> 80% across the board, with 100% coverage on critical functionality where determined by our tech leadership),
2. Must be forked onto a release branch where every line of code is reviewed by other members of the dev team, the test suite must run with 100% pass rate, and integration tests are performed by QA,
3. Can only be merged and deployed to our production environment by our tech leadership team.

Beyond this regular process (bi-weekly, on average) we don't have any other explicit internal audits of our system.

External Audits

42. How do you conduct external (third-party) audits of the service? please describe the scope and frequency of audits.
We have engaged Acunetix and Praetorian to see if a penetration test is feasible for us at this stage.

In addition to seeking out a pen-testing/security audit vendor, we've established a responsible disclosure policy to encourage would-be infiltrators to contact us with details in exchange for a bug bounty. Details here: https://wingmateapp.com/responsible-disclosure/

Finally, wherever possible, we leverage certified (ISO 27001, PCI, etc.) 3rd party providers with track records of security excellence, and benefit from their expertise through our use of their hardened systems.

42. (a) Please provide a copy of the most recent report (as per Service Introduction tab, section 5).
None conducted, see above.

Certifications

43. Which IT operational, security, privacy-related standards, certifications and/or regulations you do comply with?

None explicitly, but we trust 3rd parties with the relevant certifications to provide infrastructure and service to us.

Heroku is certified under PCI DSS Level 1, HIPAA, ISO 27001, 27017, 27018 and SOC 1, 2, 3. Details here: https://www.heroku.com/compliance

Heroku itself uses Amazon AWS data-centers, which are certified under ISO 27001, SOC 1, SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley SOX. Compliance details are available here: https://aws.amazon.com/compliance/programs/.

Cloudflare's systems are certified under ISO 27001:2013, SOC 2 Type II, SOC 3, and PCI DSS 3.2.1. Compliance details are available here: https://www.cloudflare.com/compliance/.

Stripe's systems is certified as a PCI Level 1 Service Provider. Compliance details are available here: https://stripe.com/docs/security

Backblaze is PCI compliant:
https://help.backblaze.com/hc/en-us/articles/360022452253-PCI-Compliance

43. (a) Please provide a copy of the most recent report (as per Service Introduction tab, section 5).
None conducted, see above.

Privacy

44. Do you seek a right to use or own customer derived data for your own purposes? Please describe.
No, customer data is owned solely by our customers, is only used internally to improve our service. At no point is it available for 3rd parties or anyone in the company without explicit system admin privileges.

45. Is your Privacy Notice/ Privacy Policy externally available? Please provide the URL.
https://wingmateapp.com/app_privacy/