PRIVATE FLIGHT GLOBAL LIMITED

Security Policy

PRIVATE FLIGHT

Contents

1. Overview

1.1 Purpose

The purpose of this information & security document is to communicate, inform and demonstrate the high-level security policy and architecture for Private Flight's Catering Management Platform (CMP).

This document is intended to provide sufficient detail about the solution so that:

- Clients can understand how their information and data is handled including standards used.
- Clients can understand security measures provided and mitigation responses.
- Third party security agencies can assess security compliance suitability.

1.2 Policy Content & Guidelines

1.2.1 Information Security Governance

- The Information Security and Risk Committee oversees an Information Security Programme, which includes information security strategy, principles, policy, objectives, and other relevant components.
- The programme ensures that stakeholders within Private Flight are involved in decisions relating to information security.
- The programme includes means for ensuring effective communication in support of information security.
- Management allocates sufficient resources and staff attention to adequately address information security.

1.2.2 Information Asset Classification & Management

- All company information assets are classified according to the Private Flight
- Information Classification Standard.
- All company information assets have an identified information owner and is managed and handled in accordance with the classification standard and related standards, procedures and guidelines.

2. Terms & Definitions

The following information contains the glossary of the common terms, definition and acronyms used in this document.

API - Application Programming Interface.
CMP - Private Flight's Catering Management Platform.
Azure - Microsoft's cloud based PaaS.
PaaS - Platform as a Service.
IaaS - Infrastructure as a Service.
SaaS - Software as a Service.
reCAPTCHA - Google reCAPTCHA has anti-bot protections.
API Gateway - Abstracted proxy, that receives external API requests, enforces throttling and security policies, passes requests to the back-end service.
CloudFlare - DNS, content acceleration and threat mitigation.
RTO - Return To Operation objective. Standard industry disaster recovery benchmarks use to identify levels of SLA.
SLA - Service Level Agreement, assures level of redundancy is in place and tested regularly to ensure uptime of the service is meeting or exceed target uptime levels.
VPN - Virtual Private Network via Azure secure access to back-end Services of CMP.

3. Security Architecture

3.1 Security Goals

The following security goals were considered for this solution:

ID	Goal	Comments
SG-1	The solution must have common infrastructural security controls in place, which are relevant to the services that are exposed within.	The platform has a number of infrastructure security measures in place: • Bastion Host for all remote administration of the platform. • Remote administration is restricted and accepts sessions from users on VPN. • OS hosts are patched quarterly with updates and hotfixes. • Network ingress permits only ports 80 and 443 to load balancer instance. • Remote logins are logged and reviewed monthly. Security must be based on a level high enough to assure Private Flight the confidence required of a platform to comply with “IN-CONFIDENCE” classification.
SG-2	The overall architecture must have sufficient security controls, so that the platform can be certified/considered as “IN-CONFIDENCE”	The platform is designed with this classification in mind. This is achieved by: • Separation of concerns. • Account and Branch data is always only accessed as long as the user’s security credentials permit such access. • The platform only allows one account/branch to be interacted at a time, eliminates risk of cross account/branch bleed.
SG-3	The solution must utilise security best practices and tools to assure compliance.	The platform utilises the following practices: • OWASPs Principles (See: https://www.owasp.org) • TLS/SSL is utilised for all web endpoints and insecure port 80 requests are automatically redirected to 443 by default. • Threat mitigation firewall and filtering is utilised. • Backups and data is encrypted with keys rotated quarterly. • Encryption at rest is treated as default. • Database/ data is routed based on tenant via data router.
SG-4	Auditing and logging tools must be employed throughout critical areas of the solution, so that an audit trail exist.	The solution utilises transactional logging and historical records to assist in identifying when and who made changes. e.g.: Settings. Orders and changes to them within the platform are preserved by versioning. The latest version is displayed. The majority of data held within the platform is never deleted but rather flagged as deleted and hidden from view. This permits Private Flight to be able to restore accidental / intentional deletions.

3.2 Security Constraints

The following security constraints has been identified as follows:

ID	Constraint	Comments
SC-1	The solution will not employ the use of other external IdP providers such as Social logins for the purpose of authentication.	Given the “IN-CONFIDENCE” classification and the requirement to accommodate client’s needs, no external dependency is given for external IdP providers in respect for authentication purposes. The solution is essentially stand-alone and does not depend on external tooling for verification purposes.

3.3 Assumptions

The following assumptions were given, with regards to the overall solution design:

Assumption	Comments
Users may not prefer to be burdened with additional security controls such as two-form factor authentication.	Given that users of the platform are generally flight attendants, they require the need to be able to rapidly log in at any time to check the status of orders, most commonly at remote locations. The security measures put into place mitigate the security concern and risk due to: • Threat mitigation firewall and filtering will detect if users are accessing the platform from insecure locations. (e.g.: Known IP ranges that has previously been marked as suspect) • Private Flight Operation's staff monitors orders and modifications 24/7 and are trained to observe abnormal behaviour with the ability for them to intervene.
The use of an external threat mitigation firewall and filtering service (CloudFlare) is sufficient and well-honed to mitigate attacks and unauthorised access.	Consideration was given to utilise an dedicated firewall appliance. This was ruled as insufficient as in order to deny requests from suspect locations, the platform needs to utilise a service that leverages from a real time database of sources that may be malicious. CloudFlare was selected on this basis, given the level of market saturation and rules being updated frequently makes this a good tool to combat suspect requests. For example, with the volume of user credentials being leaked to the public (https://haveibeenpwned.com), CloudFlare retains the ability to deny brute force / login attempts from sources that are known to originate or retain leaked information.

3.4 Regulations & Standards

The solution complies with the following standards and regulations:

Goal	Comments
OWASPs Top 10	The platform utilises all of OWASPs top 10 guidelines to mitigate and assure users, stakeholders and clients that all common vulnerability patterns has been addressed, mitigated and handled.

3.5 Security Controls

The following security controls has been employed for the CMP platform:

Control name	Description	Comments
External Firewall	Provides an external perimeter protection for Private Flight, allowing for specific access rules to the platform. • Packet inspections • DoS mitigation • IP Blocking • IPS • Request filtering. • Cross Request Forgery mitigation. • Filtering source reputations (Deny access for suspect sources)	Controls key ingress/egress points to the platform and ensures access is clean, policed and safe.
IDPS/IPS	Intrusion Prevention System (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances, that monitor network and system activities for malicious activity. The main function of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block and report it.	This is currently enforced on the external firewall. The hosting infrastructure is battle hardened with only two network ingress points: • Via CloudFlare, sanitised requests are forwarded onto the load balancer which then distributes requests to web servers. • Remote Administration access is via a bastion host and can only be accessed via IP whitelisted sources. *NOTE: Remote administration is only granted for qualified and security vetted engineers.* Security events such as detected intrusions are raised and notified automatically.
Hardened instances	OS hosts and web servers within the platform infrastructure are hardened, locked down with only the minimal features as required. All hosts also have an internal firewall that is locked down and only allows a very small range of ports open to permit functionality. Instances are maintained and patched on a quarterly basis.	SSL (443) is not utilised within the internal hosting environment as the SSL requests are offloaded at the load balancer / edge of the network.
Anti-Virus Capability & Scanning	Ingress firewalls must scan all inbound attachments and requests to ensure requests entering into the environment are free of viruses. Suspect attachments are removed from the request by the firewall prior to entering the load balancer.	
Google reCAPTCHA	Authentication (Login) page ultilises reCAPTCHA.	Prevents brute force of customer credientials to prevent unauthorised access.

3.6 Identity & Access Management

3.6.1 Security User Roles

The following security user roles are supported:

User	Description	Comments/additional information
External business (Azure engineers)	Engineers responsible for the hosting platform.	While they have absolutely no control and visibility of data and operating systems, they're considered a functional security role given they'll be directly maintaining the underlying systems.
Private Flight's Developers (DevOps)	Private Flight's Developers / DevOps, who are involved in supporting the platform with enhancements, new features and bug fixes.	Will require access to the source code in order to facilitate modifications. Database files are encrypted and only accessible from within the Private Flight Azure Virtual Network. Changes made are peer reviewed and audited to ensure compliance and standards are met. Developers have no access to the hosting environment.
External Integration Services	Vendors include: • Mailgun email notification • Xero Accounting (internal PFGL) • Stripe Payment gateway • XE.com cCurrency and exchange rates. • Time and Date.	External vendors have no access to data held within the CMP. Private Flight sets the integration authentication and has the ability to revoke this anytime.
System Administrators	Administrators of the Private Flight CMP.	Require admin level access to the platform to undertake diagnostics, maintenance, support customers and configure the platform. Access is via a restricted gateway with secured tokens.
Private Flight's Operations Team and Customer Success Managers/Senior Management	Operations Staff members to monitor live orders and provide functional support to business users and customer managers	Authentication and access control with client data is limited to live and historical orders for the purpose of providing assistance to business users and customer managers. Private Flight's Operations Team are authenticated via a private internal tool with an abstracted set of credentials, separated from the business user's credentials. Operations personnel have no database access.
Business Users	Business executives and staff, who wishes to place orders, review reports, data and trends relating to their catering orders.	Authenticated within the system credential store. User's access the platform via URL. Roles and access levels given to business users are dictated by Business Administrators or Private Flight's Operations Team.

Business Administrators	Business users that accesses the platform for the purpose of administering the business's account. Including settings, users and policies.	Authenticated within the own credential store. Users' access the platform via URL. Access rights are initially granted by Private Flight during the initial on-boarding phase or by other Business Administrators.

3.7 Authentication

User authentication and authorisation within the Catering Management Platform resides within itself as a black box solution and does not rely on external parties or tooling.

This was implemented due to:

- Increased level of security by eliminating external reliance.
- The need to enable Private Flight to utilise its own encryption strategies that is bespoke and customised to suit "In-Confidence" classification.

To ensure backward support for older browsers and devices, authorised cookies are utilised to persist authorisation and APIs for mobile apps usage leverages OAuth with JWT bearer tokens.

Users' credentials are made up of the following:

- Unique user based salt value, that is 256 characters in length and randomly generated. Each time the password is changed, the salt is re-generated.
- Password is encrypted utilising RSA 2048 bit encryption in conjunction with the randomly generated salt value.

By entering three subsequent invalid logins to the platform for any given account, the platform will automatically trigger a temporary suspension of the user's account for 10 minutes. This is done to mitigate brute force attacks by returning false positives.

3.8 Access Rules

Users within the platform are given access, depending on their status. These rules are broken down as below:

Rule	**Description**	**Comments/additional information**
Account Owner	Reserved for the account holder. Usually account owner will retain administration access by default, but this can be turned off.	
Admin Access	Full administration access to the account.	Administration functions made available include: • All Branch-level aircraft overview. • General Settings. • Financial Settings. • Email Preferences. • AOC Documents. • Order Documents • Manage Aircraft • Manage Users. • Preferred Providers. • Notes • Location Representatives. • Passenger Service Cost Budget Range.
Create Order	Users with this access rule will only be permitted to create and manage their own catering and offloading orders.	

Reports	Users with this access rule will be permitted to view, generate and compose dynamic reports. Report access is controlled by a permission set. Users see only data related to their aircraft unless modified.	• Catering Closed Report • Catering By Service Report • Catering By Category Report • Catering Update Report • Offloading Request Report • Offloading Closed Report • Offloading Update Report • Presentation Menu • Grocery Reports • Monthly Management Report • Monthly User Management Report. • Monthly Aircraft Management Report • Yearly Management Report • Yearly User Management Report • Yearly Aircraft Management Report • Flight Feedback Reports.
Financial	Users with this access rule will be permitted to view, query and print invoices issued against the account for orders raised.	Has a limited access to Management Report to allow viewing of financial information.
Favourites Menu Manager	Permits the user to create or maintain favourites templates to be utilised by other users for their catering orders.	

The design of the access rules policy within Private Flight's Catering Management Platform, allows multiple access rules to be assigned to a user within an account.

For example: A financial manager will require the Financial and Reports access rules but won't need administration, nor the ability to create orders and favourites.

In conjunction with the access rules above, users also have the ability to observe and amend orders for other users within the same account. This is done on three levels:

- None (Default – This rule will not allow the user to view orders made and administered by other users).
- Everyone (This rule permits the user to observe, view and amend orders made by other users within the account.
- Specific User (This ad-hoc policy allows administrators to specify which user within the account another user can observe and amend orders for).

4. Operating Considerations

This section describes the operating considerations for the overall platform, issues, risks, impacts and how they are mitigated.

4.1 Availability & Reliability

The following are the availability and reliability considerations given:

Ref	Consideration	Rationale	Comments/additional information
AR-1	The platform must be capable of supporting a regular maintenance schedule of planned outages for all systems within scope. Minor changes should be executed without incurring system outages.	Critical to ensure continued operation of the CMP platform. Once each quarter, there are planned outages as necessary to undertake patching of the host instances. Critical part of Private Flight's infrastructure for compliance, support, security and maintainability.	Code updates to the CMP platform such as new features, improvements, updates and bug fixes (if any) are pushed into production after a rigorous testing phase. Code updates are planned events and incurs an outage of no more than 10mins at a time and is conducted at low peak times.

AR-2	The platform must be available 24/7	The services provided to the client are treated as absolute mission critical and expected to be used around the clock.	As per AR-1 above, it is currently subject to rolling updates as planned outages are necessary for continued security adherences. Improvements to planned outages are being explored.
AR-3	Support for the platform will be required 24/7	Private Flight provides a 24/7 Operations Support team, which solely monitors all live orders and assist customers' with support enquires.	
AR-4	The failure of any component or the overall solution must not result with more than 2 mins of data loss.	The risk of transactional data in transit is high and would cause issues and reputational damage to Private Flight.	This RTO target of 2mins is mitigated by the use of database replication to a secondary data centre. In an event of a fault, the platform fails over to the secondary data centre. Currently, replication of changes is delayed by roughly 2-15 seconds, which is well inside the RTO accepted range.
AR-5	Disaster recovery and fail-over tests for the solution must be conducted at least once a year.	Necessary to validate and confirm solution durability. Helps to identify red flags and mitigate them before a real event occurs.	
AR-6	The solution must be able to support 99.99% or greater availability each month (excluding planned outages) NOTE: Private Flight expects between 2-4 planned outages per year for routine maintenance and upgrades.	The platform must be highly available and have several redundancies in place to ensure all services remain unimpacted in the event of a service degradation or outage. 99.99% availability means that the platform cannot be offline for more than 4.38 mins per month for unplanned outages.	To date, over the past 3 years, the platform has not suffered an unplanned outage due to the level of redundancies and measures put into place.
AR-7	The platform must be able to support a Recovery Point Objective (RPO) of 5 mins.	Design of the geographical distinct fail-over will accommodate for this criteria.	
AR-8	The platform must be able to support a Recovery Time Objective (RTO) of 2 mins.	Design of the geographical distinct fail-over will accommodate for this criteria.	

4.2 Capacity & Performance

The following are the capacity and performance considerations for the platform:

Ref	Consideration	Rationale	Comments / Additional information
CA-1	All systems and resources provisioned within this solution must contain sufficient headroom of 40%.	Necessary to facilitate scaling and peak load requirements.	
CA-2	All APIs must be capable of processing the threshold of 500 rps (Requests per Second) for each API.	Must be able to accommodate high usage at peak times.	
CA-3	The platform must be capable of scaling up / down resources in an elastic fashion to cater for peak demand.	Necessary to support continuity and traffic load.	Private Flight's CMP platform currently runs on a high performance cluster of web servers with load balancers that automatically detects bursts of traffic and adds additional servers to ensure SLA is not degraded as a result.

CA-4	The solution must allow for throttling of requests based on: 1. IP Address 2. User Account	Prevents users from abusing the platform or adversely impacting the usage and experience of the platform by other users.	The platform utilises CloudFlare that automates this throttling and denies connections from sources that have an abnormally high count of failed logins and/or requests.

4.3 Continuity

The following are the continuity considerations given for the platform:

Ref	Consideration	Rationale	Comments / Additional information
CO-1	The platform must have automatic fail-over to a geographically distinct location in the event of a critical failure to ensure operations remain unaffected.	Required to meet 24/7 availability targets and RTO/RPO of 2 mins and 5 mins.	Private Flight's CMP platform has dual data centre redundancy, each residing in a geographically distinct location.
CO-2	The platform must be stateless and hold no data or information that only resides within the platform.	Necessary directive to ensure that there is nothing special or data held in the platform - that isn't held elsewhere (e.g. backups) By having the platform stateless, means that the ability to rebuild the environment should such an event occur, would not result in the loss of critical information.	
CO-3	Cloud vendors that are utilised within the solution must have an acceptable failover and DR strategy in place that is auditable / verified.	Cloud vendors must ensure they have this level of redundancy otherwise, risk losing critical components of the solution.	The platform does not directly depend on any external cloud vendors for this reason alone. However, data feeds such as currency and date/time updates has this risk of outages, but the platform is designed to cater for full loss of those services and will continue to operate unaffected.
CO-4	Backups of any databases and any form of data must be conducted at least daily and held outside of the solution.	Backups should be held off-site that is accessible in the event where Private Flight requires to restore data at short notice.	Full database backups are done daily with differential backups done every 2 hours. Backups are stored outside of both data centres in use within an encrypted volume and maintained for 30 days.
CO-5	Any data and databases held within the solution should have replication services to keep both the primary and fail-over nodes in sync.	Necessary to enable the requirement for hot fail-over. Replication should not breach the 2 min RTO objective.	The platform utilise geographical replication of the database layer, in such an event of an outage, this fails over automatically.
CO-6	There should be a maintained contacts register for engineers and stakeholders to utilise in the event of a failure or disaster.	Essential to ensure the platform's continuity is in place and key individuals are identified.	Private Flight has three primary layers of technical support: • IaaS provider has near time support for hardware failures. • Private Flight Ops Team will evaluate and assess the severity of the fault. • Private Flight's Hosting Engineering Staff are on call 24/7. In most cases the issue is resolved by the IaaS provider.

CO-7	Disaster recovery credentials should be held securely in more than two locations and used in the event of an disaster, should current engineers are not available.	Ensures business continuity and reliance.	The Private Flight Executive team has access to these recovery credentials, which are stored in a safe within the office. This is required as internet/networking may go offline in an event of a disaster.
CO-8	Continuity drills and tests should be conducted at least once yearly to ensure compliance and preparations.	Useful to validate current continuity plans and identify weaknesses to improve upon.	

4.4 Data Handling & Encryption

The following are the data handling & encryption considerations for the platform:

Ref	Consideration	Rationale
DH-1	Data retention via backups is explicitly held for no more than 30 days.	Ensures the information held within backups is secure, relevant and eliminates historical information where trends and past information could potentially be calculated if obtained.
DH-2	In the event of disks and storage media that holds backups or production data is retired, they are destroyed or zero padded according to DoD Security guidelines.	Necessary precaution to ensure data cannot be recovered from storage media that has been released from service.
DH-3	The data held within databases and storage media is encrypted at rest by default.	Ensures all data is encrypted automatically by the database itself and adds another layer of protection to secure storage media from malicious means.
DH-4	Deletion and removal requests from the business (client), all data is removed and destroyed.	Due to the nature of the platform, it is not possible to immediately delete data until after 30 days when the backup retention expires.
DH-5	Backups must retain at least 30 days of historical changes and data.	Necessary to ensure that rollbacks and recovery of data is possible. This is limited to 30 days as backup archives are large and quickly become irrelevant once past this threshold.
DH-6	Backups of client data must be encrypted.	Backups are always encrypted using a 256 bit key that is changed quarterly.

4.5 Deployment & Implementation

The following are the deployment and implementation considerations for this solution:

Ref	Consideration	Rationale
DI-1	CI/CD pipelines are utilised to streamline deployments of APIs and containers to the platform.	Standardise deployment and helps to assist all instances are automated and configured the same way.
DI-2	Each application group will have its own dedicated load balancer.	Necessary to permit geographical failover and increase availability.
DI-3	The solution must have the following environments: • TEST (Systems Integration testing) • STAGING (External Acceptance Testing) – Known as Pre-Prod. • PROD (Production)	Only the STAGING and PROD environments will utilise geographical fail-over, required to facilitate testing.

4.6 Scalability

The following are the scalability considerations for the platform:

Ref	Consideration	Rationale	Comments / Additional information
SC-1	As each application group will have it's own load balancer, this is done to permit scaling policies to be applied as such: • Scale up by adding more instances to rotation by either increased requests or instances whereby resource utilisation passes a set threshold. • Scale down by removing additional instances from rotation when its detected that either requests has been reduced or instances whereby resource utilisation has dropped.	Caters for maximum elasticity and availability. All consumers should not observe degraded performance as a result.	Load balancers will require an cooling off period before scale-down is triggered to prevent scale-up being triggered in short period of time (eg: Lull between requests)
SC-3	The platform must be capable of serving at minimum of 500 rps (Requests per Second)	Necessary to comply with business requirements, catering to a burst of traffic.	*NOTE: When performing a cold start-up, response times may be in breach of response time metrics but this is limited to the first several requests until the service has warmed up.*
SC-4	The platform must utilise CDN offloading in an event to accelerate the platform performance for all users accessing the system from all corners of the globe.	Necessary business requirements.	Primary bulk of users on the platform are Flight Attendants and coperator centralised operations teams, accessing the system from various airports across the globe. Some regions may have poor internet connectivity or excessive data transfer rates so the use of Azure to serve CDN content closer to them and in most cases within the same region, helps improve availability and performance of the application.

4.7 System Management, Monitoring & Administration

The following are the system management, monitoring and administration considerations for this platform:

Ref	Consideration	Rationale	Comments / Additional information
SM-1	All components within the solution must be capable of streaming log based events for aggregation and analysis.	Required to assist technical diagnostics, audit and security compliance.	
SM-2	All errors, warnings and exceptions must be logged for review.	To support problem and incident analysis.	Also necessary to review security cases to determine the service is robust and no security events has occurred.
SM-3	All security points within the solution must log events.	To support security audit and problem / incident analysis.	

4.8 Incident Management

Private Flight's technical engineers has a business requirement and mandate to document all security incidents and take all possible steps to safeguard the integrity of the platform. This includes data and customer information security.

All reports are reviewed by the Private Flight Security Team and necessary steps are taken to avoid any identified risks. All incident reports are kept for future reference. Private Flight follows best practices to manage incidents including incident identification, logging, categorisation, prioritisation and initial diagnosis. Escalation, if necessary, to Level 2 Support for resolution, closure and communication to effected customers (if any).

As part of Private Flight's IT Security policy:

- An Information Systems Disaster Recovery Plan is developed, maintained and tested in a manner that ensures the ability of the business to continue operations as required by the Private Flight Business Continuity Plan.
- Security incident reporting and response procedures are developed and maintained by the Technical Lead. They are published and accessible as deemed appropriate. All users are informed of procedures which are relevant to them.

4.9 Logical Access

Private Flight has implemented industry best practices to prevent unauthorised logical access, damage and interference to its information-holding assets, prevent loss, theft or compromise of its information assets and interruption of the business's activities.

This policy covers areas such as, but is not limited to:

- Access authentication, use of approved identification, passwords and two factor processes and biometrics wherever necessary.
- Network access controls.
- Application access controls for Management Application used by Private Flight personnel.
- Information access controls.
- Encryption techniques.
- External access requirements for VPN.
- Cloud access controls.
- Limiting production environment to Private Flight office IP Address.

4.10 Physical Access

Physical access to the Catering Management Platform is heavily restricted and only available for the following:

- Private Flight's Infrastructure IaaS provider (Engineers only has access to the underlying bare metal host and has no access to data or operating systems running the platform.
- Private Flight's technical team has access to the operating systems and encrypted data and can only be accessed via VPN.
- Private Flight's technical team has been vetted and background checks confirmed on a regular basis.

There are no services or functions held locally within Private Flight's offices that the platform is dependent upon.

PRIVATE FLIGHT

www.private-flight.com