DJI FlightHub 2 — Data Security Clarification FAQ

Response to Customer Security Questionnaire

Date: March 2026

Product: DJI FlightHub 2

Reference Links:

- DJI Trust Center: https://www.dji.com/trust-center

- FlightHub 2 FAQ: https://www.dji.com/global/flighthub-2/faq

- ISO Certification: https://www.dji.com/hk-en/trust-center/resource/security-audits-certification

- DJI Privacy Policy: https://www.dji.com/hk-en/policy

- FlightHub 2 User Guide: https://terra-1-g.djicdn.com/4670436537e14b5c822b1c7f97b8aac9/es_user_guide/v7.0/DJI_FlightHub_2_User_Guide_v2.4.pdf

---

PART 1: CERTIFICATIONS & THIRD-PARTY ASSESSMENTS

Q1. Does DJI FlightHub 2 hold official certifications such as ISMS, STAR certifications, or have they undergone third-party assessments?

A: Yes. DJI FlightHub 2 holds the following official certifications:

Certification	Certifying Body	Scope	Reference

ISO 27001	British Standards Institution (BSI)	Information Security Management System	https://www.dji.com/hk-en/trust-center/resource/security-audits-certification
ISO 27701	British Standards Institution (BSI)	Privacy Information Management (GDPR/CCPA compliance)	Same link above

Additionally:

- 2024 Security Audit by FTI Consulting (independent US-based security firm) — confirmed security posture
- CCPA Compliance (California Consumer Privacy Act)
- GDPR Compliance (EU General Data Protection Regulation)

DJI's security and privacy program follows **ISO 27001** as its baseline standard.

Certificate download link: https://www.dji.com/hk-en/trust-center/resource/security-audits-certification

---

Q2. What is the track record of DJI FlightHub 2 service provision?

A: DJI FlightHub 2 was officially launched in **2022**. As of the date of this document, it has been in commercial service for **3+ years**. The service is actively deployed across enterprise customers globally in sectors including public safety, infrastructure inspection, agriculture, and mining.

Q3. What items are covered in DJI FlightHub 2's terms of service?

A: DJI's terms of service and privacy policy cover the following:

- ✅ Scope of responsibility (service provider vs. user)
- ✅ Confidentiality and data protection obligations
- ✅ Changes in service content (advance notice provided)
- ✅ System and network availability (SLA coverage)
- ✅ Prohibition of unauthorized access by DJI to user data without authorization
- ✅ Data handling upon service termination (deletion process defined)
- ✅ User data is NOT used for AI training without explicit user consent

Reference: https://www.dji.com/hk-en/policy

Q4. What is the governing law and jurisdiction for disputes?

A: DJI's terms of service include provisions for governing law and jurisdiction. For Japanese enterprise customers, **the applicable law and jurisdiction should be confirmed and explicitly agreed upon in the enterprise contract/service agreement**. Customers are encouraged to negotiate these terms directly with DJI's enterprise sales team.

Q5. How is user data handled upon service termination?

A: Upon account cancellation, DJI follows its Privacy Policy and applicable laws. The cancellation process permanently deactivates the account and deletes associated user data. After deletion, the data is **no longer accessible or recoverable**.

Specifically:

- Data deletion is performed through a combination of physical deletion and logical deletion procedures
- After deletion, data cannot be accessed or restored
- DJI complies with applicable data protection laws regarding deletion timelines

PART 2: IDENTITY & ACCESS MANAGEMENT

Q6. What ID management functions does FlightHub 2 support?

A:

Function	Supported?	Notes
Unique User IDs	✅ Yes	Via DJI unified account system
Unique Administrator IDs	✅ Yes	Organization Admin role
Display list of IDs	✅ Yes	Via FlightHub 2 admin panel
Register / Modify / Delete User and Admin IDs	✅ Yes	By organization administrator
Restrict User ID changes to Admin IDs only	✅ Yes	Role-based access control

Role types in FlightHub 2: Organization Administrator, Project Manager, Pilot, Viewer. Role assignment and management is documented in the FlightHub 2 User Guide.

> *Reference: FlightHub 2 User Guide: https://terra-1-g.djicdn.com/4670436537e14b5c822b1c7f97b8aac9/es_user_guide/v7.0/DJI_FlightHub_2_User_Guide_v2.4.pdf*

Q7. What is the user lifecycle management policy?

A:

- Add: Users register through DJI's unified Member Center (member.dji.com)
- Modify: Users update account information through Member Center's account management function
- Delete: Account cancellation process permanently deactivates the account and deletes user data

Authentication uses **OAuth 2.0 protocol**. Upon login, a time-limited token is generated; all subsequent FlightHub 2 access requires this token.

PART 3: AUTHENTICATION

Q8. Does FlightHub 2 support Multi-Factor Authentication (MFA)?

A: FlightHub 2 supports multi-factor authentication through the following methods:

Authentication Method	Supported?
ID / Password	✅ Yes
SMS One-Time Password	✅ Yes
Email One-Time Password	✅ Yes
TOTP (Authenticator App)	✅ Yes (via verification code)
Single Sign-On (Enterprise SSO)	✅ Yes (Enterprise accounts)

Q9. What authentication security functions are available?

A:

Security Function	Supported	Details
Suspend authentication credentials (account lock)	✅ Yes	Automatic lockout after excessive failed attempts
Force password reset	✅ Yes	Via Member Center
Account lockout after repeated login failures	✅ Yes	Locked after **10 failed attempts within 7 days**
Mask reason for authentication failure	✅ Yes	Error messages do not disclose specific failure reasons
Inactive session auto-logout	✅ Yes	Default: **90 days** of inactivity (this is account-level inactivity, not per-session timeout)

Q10. What is the password management policy?

A:

Password Requirement	Status
Minimum 8 characters	✅ Required
Combination of letters and numbers	✅ Required

Common/default passwords prohibited	✅ Prohibited
Previously used passwords prohibited (reuse restriction)	✅ Prohibited
Passwords masked on-screen when typing	✅ Yes
Passwords stored encrypted	✅ Yes (AES-256 equivalent hashing)
Users can change their own passwords	✅ Yes

Q11. Does FlightHub 2 support additional PIN (second password) separate from the main password?

A: No. FlightHub 2 does **not** currently support a separate PIN code as a second password factor beyond the standard login credentials.

Q12. Does FlightHub 2 support IP address-based access restriction (whitelist/denylist)?

A: According to DJI R&D: IP address whitelisting is **available** as a feature. However, this appears to be under evaluation for specific deployment scenarios. Customers requiring strict IP restriction should confirm the configuration method (organization-level vs. user-level) with DJI enterprise sales before deployment.

Q13. Does FlightHub 2 support client certificate authentication?

A: Client certificate authentication is **not currently supported** in the standard cloud version of FlightHub 2.

PART 4: ACCESS CONTROL

Q14. What access control functions are available?

A:

Access Control Function	Supported	Details
Session timeout on inactivity	✅ Yes	Default 90-day account inactivity period
Access rights changes restricted to Admin IDs	✅ Yes	Role-based access control
Time-based access restrictions	❌ No	Not available
DDoS protection	✅ Yes	DDoS protection deployed at network perimeter
Web Application Firewall (WAF)	✅ Yes	WAF deployed
IDS/IPS (Intrusion Detection/Prevention)	✅ Yes	HIDS (Host-based IDS) deployed

PART 5: VULNERABILITY MANAGEMENT

Q15. Are vulnerability and risk assessments conducted for FlightHub 2?

A: Yes.

- External professional security firms and DJI's internal security team conduct regular security scans and security audits of FlightHub 2
- Vulnerability response by severity level:

- Critical/High vulnerabilities: **Patched within 24 hours**; users notified and versions updated as appropriate

- Medium vulnerabilities: Addressed within standard patch cycle

- Low vulnerabilities: Tracked and resolved in scheduled releases

- Penetration testing: Sdlc and version security audits are conducted internally, and penetration tests are conducted externally on a regular basis. penetration test reports cannot be shared externally. External penetration testing is conducted at least once per year.

- 2024 Independent Audit: A security audit was conducted by FTI Consulting (US-based independent security firm) in 2024.

PART 6: ENCRYPTION

Q16. Is communication encryption implemented? What TLS version is supported?

A: Yes. All user communication with FlightHub 2 is encrypted.

Protocol	Encryption	Minimum Version

HTTPS (Web access)	TLS	**TLS 1.2 minimum; TLS 1.3 supported**
WebSocket connections	WSS (WebSocket Secure)	TLS 1.2 minimum
MQTT (IoT/drone telemetry)	MQTTS	TLS 1.2 minimum

- TLS 1.0 and TLS 1.1 are disabled.
- Only TLS 1.2 and TLS 1.3 are supported.

Reference: https://fh.dji.com/ (server TLS configuration)

Q17. Is data encrypted at rest?

A: Yes.

- Database encryption: AES-256 encryption at rest
- Encryption key management: Keys are stored separately (not co-located with encrypted data) and subject to regular rotation aligned with the product lifecycle
- Backup encryption: Leverages AWS's data backup encryption mechanisms

---

PART 7: CONNECTION RESTRICTIONS

Q18. Are access restrictions available (e.g., by source IP address)?

A: IP whitelisting is listed as an available security control in FlightHub 2 (confirmed in DJI's Sheet3 response: "Available"). The specific configuration interface (organization-level or user-level) should be confirmed with DJI enterprise support.

PART 8: LOG MANAGEMENT

Q19. What logs does FlightHub 2 capture and retain?

A:

Log Type	Captured?	Retention Period	Configurable?
Authentication logs (login/logout, failures, password changes)	✅ Yes	**180 days** (default)	Subject to user requirements
User activity / operation logs	✅ Yes	**180 days** (default)	Subject to user requirements
Admin/privileged operation logs	✅ Yes	**180 days** (default)	Subject to user requirements
DBMS audit logs	✅ Yes (included)	**180 days** (default)	—

Q20. How are logs protected?

A:

- Logs are stored in the backend with data masking (sensitive fields anonymized) and necessary encryption
- Access to production logs is controlled by role-based access management — only authorized administrators can access logs
- Sensitive data fields are encrypted before being written to logs

---

Q21. Can customers view, search, or export logs for audit purposes?

A: Currently, **self-service customer log access (view/search/export) is not supported** in the standard FlightHub 2 interface.

- If log access is required for audit purposes, customers should contact DJI enterprise support or their account manager to arrange log extraction
- DJI will only release logs for forensic investigation if required by applicable law or a valid binding order from a governmental body (e.g., subpoena or court order), and only with the user's data processing authorization

---

PART 9: DATA AVAILABILITY & BACKUP

Q22. What is the backup and restore capability?

A:

Backup Attribute	Details
Backup type (within 7 days)	**Incremental real-time backup**
Backup type (7–30 days)	**Scheduled incremental full backup**
Maximum recovery point (RPO)	**Any point within 7 days** (real-time); **backup snapshots within 30 days**
Recovery time objective (RTO)	RTO time is within 2 hours, RPO time is 0
Backup encryption	Yes — leverages AWS backup encryption mechanisms

---

PART 10: DATA CONFIDENTIALITY & TENANT SEPARATION

Q23. How is tenant data separated in FlightHub 2?

A: FlightHub 2 is a **multi-tenant SaaS service**. Data separation is implemented as follows:

Layer	Separation Method
Physical storage	Data is physically co-located (shared infrastructure)
Database layer	**Logical separation** via unique user/organization IDs
Application layer	Logical separation enforced by system access controls
Data storage middleware	Shared, separated by uniqueness of user IDs

Q24. Where are the servers storing data located?

A:

User Region	Cloud Provider	Data Center Location
Japan users	Amazon Web Services (AWS)	**Virginia, USA** (primary); Frankfurt, Germany (additional)
Other international users	Amazon Web Services (AWS)	Virginia, USA or Frankfurt, Germany

Mitigation options:

1. **FlightHub 2 On-Premises** — DJI launched an on-premises version in 2025 that allows data to be stored locally within the customer's own infrastructure, eliminating the data residency concern

AWS Data Center security reference: https://aws.amazon.com/compliance/data-center/controls/

Q25. Is additional software installation required to use FlightHub 2?

A: No additional software installation is required for the standard web-based FlightHub 2 access.

- Web browser: Chrome 92 or above (Chrome 102+ recommended)
- No thick client, plug-in, or VPN software required
- Access via standard public internet connection

PART 11: INFORMATION DISCLOSURE & OPERATIONAL STATUS

Q26. Can operational status be confirmed upon customer request?

A: Yes, FlightHub 2 provides operational status information through the following mechanisms:

1. **After-sales support team:** Customers can contact DJI enterprise support for operational status inquiries
2. **System information panel:** Status announcements are posted within the FlightHub 2 interface
3. **AWS infrastructure transparency:** As FlightHub 2 is hosted on AWS, customers can reference AWS's data center compliance documentation

For SLA-specific uptime commitments, these should be defined in the enterprise service contract.

PART 12: ADDITIONAL SECURITY MEASURES

Q27. Does FlightHub 2 provide DDoS protection and security monitoring?

A: Yes. The following security infrastructure is in place at the network perimeter and within the system:

Security Control	Status

DDoS Protection	✅ Deployed
Web Application Firewall (WAF)	✅ Deployed
Host-based Intrusion Detection System (HIDS)	✅ Deployed
Security monitoring / anomaly detection	✅ Active
Security Operations Center (SOC) monitoring	✅ Yes (internal security operations team)
IDS/IPS signature and anomaly-based detection	✅ Yes

Q28. What is the Enterprise SSO capability?

A:

SSO Attribute	Details
Protocol supported	**OAuth 2.0**
SAML 2.0	❌ Not confirmed as supported
Azure AD integration	❌ Not currently supported
Force SSO for all org users	❓ Not confirmed — please verify with DJI enterprise
Identity provider (IdP) compatibility	DJI's own member center; Enterprise SSO options should be confirmed with DJI

Q29. Can DJI access customer data?

A: DJI does **not** access user data without explicit user authorization. DJI personnel will not handle user-protected data without authorization. This commitment is stated in DJI's Privacy Policy and Terms of Service.

Admin access to infrastructure is logged via:

1. Monitoring logs for online data operations
2. Audit logs for the administrative backend

Q30. Incident management and severity classification

A:

Severity Level	Classification Criteria
S (Critical)	Large number of affected customers; significant business impact
A (High)	Moderate number of affected customers
B (Medium)	Limited customer impact
C (Low)	Minimal impact; cosmetic or minor issues

Classification is based on:

1. Number of affected customers
2. Number of after-sales complaints

Customer incident reporting: FlightHub 2 provides a user feedback submission function. However, customers currently **cannot view the progress of their submitted incident reports** within the platform — this is a noted limitation.

SUMMARY: COMPLIANCE GAP ANALYSIS

The following table summarizes key compliance gaps relative to the Japanese customer's security requirements:

Requirement	Status	Gap / Mitigation
Official certification (ISO 27001)	✅ Compliant	ISO 27001 via BSI; certificate available
Official certification (ISO 27701)	✅ Compliant	ISO 27701 via BSI
SOC 2 certification	❌ Not held	Gap — no SOC 2 available
Data center in Japan	❌ Non-compliant	Data stored in AWS Virginia/Frankfurt; consider On-Premises version
Log retention ≥ 1 year	❌ Non-compliant	Default 180 days; gap of ~6 months
MFA support	✅ Partial	Supported, but cannot be forced org-wide by admin
IP address restriction	✅ Available	Available; verify configuration with DJI
Client certificate authentication	❌ Not supported	Gap — no alternative confirmed
Separate PIN (2nd password)	❌ Not supported	Gap
TLS 1.2+ (TLS 1.0/1.1 disabled)	✅ Compliant	TLS 1.2 minimum; TLS 1.3 supported
AES-256 at-rest encryption	✅ Compliant	AES-256 database encryption

Tenant logical separation	✅ Partial	Logical only; no physical separation
Dedicated tenancy (single-tenant)	❌ Not available (cloud)	Consider FlightHub 2 On-Premises
Customer log access/export	❌ Not available (self-service)	Must request via support
Penetration testing evidence	✅ **There are both internal and external ones.**	Reports cannot be shared externally
Vulnerability patching (Critical < 24h)	✅ Compliant	Critical/High patched within 24 hours
Backup (7-day any point RPO)	✅ Compliant	Real-time incremental within 7 days
Defined RTO	✅ Not formally defined	2 hours

APPENDIX: KEY REFERENCE LINKS

Resource	**URL**
DJI Trust Center	https://www.dji.com/trust-center
FlightHub 2 ISO 27001 / 27701 Certificate	https://www.dji.com/hk-en/trust-center/resource/security-audits-certification
DJI Privacy Policy	https://www.dji.com/hk-en/policy
FlightHub 2 FAQ	https://www.dji.com/global/flighthub-2/faq
FlightHub 2 User Guide (v2.4)	https://terra-1-g.djicdn.com/4670436537e14b5c822b1c7f97b8aac9/es_user_guide/v7.0/DJI_FlightHub_2_User_Guide_v2.4.pdf

AWS Data Center Security	https://aws.amazon.com/compliance/data-center/controls/
DJI Security White Paper	https://www.dji.com/trust-center/resource/white-paper
FlightHub 2 Server Location (DJI Support)	https://support.dji.com/help/content?customId=en-us03400006620
FlightHub 2 On-Premises (2025)	https://enterprise.dji.com/flighthub-2-on-premises

---

DJI FlightHub 2 Information Security FAQ — English Version

Questions marked ⚠️ require further clarification or contractual negotiation with DJI enterprise team