

# Security Considerations for Travel to or Through Hong Kong

## EXECUTIVE BRIEF

### Executive Summary

Hong Kong's security and legal environment has undergone significant transformation since 2020, with material implications for international travelers; including faculty, staff, students, and research affiliates. Recent March 2026 enforcement amendments substantially expand government authority over digital devices, personal data, and traveler conduct, even for those transiting through Hong Kong International Airport.

For higher education institutions (where travel often involves research data, intellectual property, and international collaboration) these changes introduce heightened legal, compliance, and data security risks that require proactive policy alignment and traveler education.

### Key Risk Areas

#### 1. Expanded Government Authority Over Digital Devices

Authorities may legally compel travelers to provide passwords or decryption keys for phones, laptops, and other devices.

This authority applies broadly, including individuals under investigation and those in transit.

Refusal is a criminal offense, with penalties up to:

- 1 year imprisonment
- HK\$100,000 fine
- Providing false or misleading information may result in up to 3 years imprisonment.

Faculty and researchers traveling with sensitive research data, grant-funded materials, or unpublished work may face forced disclosure risks.

#### 2. Elimination of Traditional Confidentiality Protections

Authorities have clarified that professional privilege (e.g., legal, medical) does not apply during device inspections.

Confidential student data, research subject information, and institutional communications may not be protected which raises FERPA, HIPAA, and grant compliance concerns depending on data exposure.

#### 3. Broad and Expanding National Security Laws

Hong Kong's legal framework now includes three overlapping regimes:

- National Security Law (2020):
  - Covers secession, subversion, terrorism, and foreign collusion
  - Extraterritorial reach which applies globally regardless of nationality
- Safeguarding National Security Ordinance (Article 23, 2024):

# Security Considerations for Travel to or Through Hong Kong

## EXECUTIVE BRIEF

- Adds offenses such as espionage, sabotage, and “external interference”
- Allows detention without charge up to 16 days
- 2026 Enforcement Amendments:
  - Expand search, seizure, and digital access powers
  - Enable confiscation of materials deemed “seditious”

Academic activity (research topics, collaborations, public statements) could be interpreted under broad national security definitions

Increased risk exposure for:

- Study abroad programs
- International research partnerships
- Faculty engaging in geopolitical or policy-related work

## 4. Data Privacy and Cybersecurity Exposure

Travelers should assume:

- Device contents may be inspected
- Encryption may not protect data if access is compelled

Elevated risk of:

- Intellectual property exposure
- Grant or sponsor compliance violations
- Institutional data breaches

## Recommended Institutional Actions

### 1. Update Travel Risk Policies

Reclassify Hong Kong as a “heightened data risk” destination

Require pre-travel approval for:

- Research-related travel
- Travel involving sensitive data

### 2. Implement Device & Data Protocols

Mandate use of:

- “Clean” or loaner devices for travel
- Cloud-based access only (no local storage)

# Security Considerations for Travel to or Through Hong Kong

## EXECUTIVE BRIEF

Prohibit travel with:

- Sensitive research data
- Confidential student or employee records
- Internal communications archives

### 3. Strengthen Traveler Education

Clearly communicate:

- Legal obligation to comply with device access requests
- Penalties for refusal or misinformation

Set expectations:

- Travelers should assume full device visibility by authorities

### 4. Align with Compliance & Risk Stakeholders

Partner with:

- Legal counsel
- Information security teams
- Export control / research compliance offices

### 5. Review Travel Program Controls

Evaluate:

- Booking restrictions or approval workflows
- Duty of care tracking for travelers in-region

Consider:

- Enhanced pre-trip briefings
- Real-time traveler monitoring tools

## Strategic Takeaway

Hong Kong remains a major global transit and business hub, but its evolving national security framework introduces non-traditional travel risks, particularly around data access, legal exposure, and academic activity.

For higher education institutions, this is less about whether to allow travel and more about how to responsibly enable it through:

# Security Considerations for Travel to or Through Hong Kong

## EXECUTIVE BRIEF

- Strong governance
- Clear traveler protocols
- Tight alignment between travel, legal, and IT security functions