International Fund for Public Interest Media

Information Technology (IT) Security Policy

Version:	1.0
Policy Owner:	Finance Director
Date of AFC Approval:	15 April 2025
Review Schedule:	Every two (2) years
Most Recent Review:	April 2025
Next Review:	April 2027

1. Introduction

The International Fund recognizes the critical importance of information security in safeguarding its data, systems, and operations. This IT Security Policy establishes the fundamental principles, responsibilities, and controls necessary to protect the confidentiality, integrity, and availability of the Fund's information assets. It provides a structured framework for mitigating security risks, preventing unauthorized access, and ensuring compliance with legal, regulatory, and contractual obligations. The policy applies to all employees, contractors, and third-party vendors who interact with the Fund's IT systems, whether on-premises or remotely. By adhering to these guidelines, the International Fund aims to foster a security-conscious culture and enhance its resilience against evolving cyber threats.

2. Scope of Policy

This IT Security Policy applies to all employees and contractors of the International Fund who access, manage, or store organizational information and IT resources. It covers both logical and physical security aspects, including user account management, authentication protocols, security awareness training, incident response, data encryption, and cloud security.

The policy also establishes requirements for securing company-owned devices, ensuring network protection, and enforcing strict access controls for office premises. Compliance with these security measures is mandatory to safeguard the confidentiality, integrity, and availability of the International Fund's information assets.

3. Compliance and Review

All employees and contractors of the International Fund are required to comply with this IT Security Policy. Any violation may result in disciplinary action, including but not limited to access restrictions, formal warnings, contract termination, or legal consequences, depending on the severity of the breach.

The IT Service Provider, in collaboration with the Deputy Chief Executive Officer, is responsible for monitoring adherence to the policy and addressing any compliance issues.

This policy is reviewed bi-annually, or more frequently if necessary, to account for emerging security threats, regulatory changes, and technological advancements. Reviews are conducted by the IT Service Provider and the General Counsel, with final approval by the Deputy Chief Executive Officer. Any updates or revisions will be communicated to all employees and relevant stakeholders to ensure continued awareness and compliance.

4. Definitions

IT Service Provider – The designated external entity (Stiqibit LLC) responsible for managing and maintaining the International Fund's IT infrastructure, security, and support services.

Application Owner – An individual or department responsible for managing a specific application, ensuring compliance with security policies, and granting or revoking user access.

Multi-Factor Authentication (MFA) – A security mechanism requiring users to verify their identity using two or more authentication factors, such as a password and a one-time code sent to a mobile device.

Single Sign-On (SSO) – A centralized authentication system (OKTA Verify) allowing users to access multiple applications with a single set of login credentials.

Data Encryption – The process of converting sensitive information into a secure format to prevent unauthorized access, both at rest and in transit.

Security Incident – Any event that compromises the confidentiality, integrity, or availability of the International Fund's information assets, including but not limited to data breaches, malware infections, and unauthorized access.

Access Control – Policies and technologies used to restrict and manage user access to IT systems, applications, and physical locations based on role-based permissions.

Virtual Private Network (VPN) – A secure, encrypted connection that allows employees to access the International Fund's network remotely while protecting data transmission from unauthorized interception.

Firewall – A security device or software that monitors and controls incoming and outgoing network traffic to prevent unauthorized access.

PGP (Pretty Good Privacy) email encryption - A cryptographic method used to secure email communications by encrypting the content to ensure confidentiality, integrity, and authentication. It uses a combination of public-key and symmetric encryption to protect messages from unauthorized access. Recipients decrypt messages using their private key, ensuring that only intended parties can read the content. PGP encryption helps safeguard sensitive information from interception, tampering, and unauthorized disclosure.

5. Policy Statement and Principles

5.1 Logical security

5.1.1 Information security policy awareness

Employees of the International Fund receive regular security awareness training to ensure they understand their roles in protecting information. This annual training is mandatory and covers at least such key topics as phishing awareness, safe browsing practices, and reporting security incidents.

5.1.2 Application classification

As part of the Data Retention Policy, the International Fund has established a list of critical applications to ensure key systems are identified and assigned a designated owner.

5.1.3 User Accounts Management

Any creation, modification, or deletion of access rights for reading or writing within applications and data storage must be authorized by email by the application owner or the employee's direct manager.

Upon hiring, the International Fund's HR Business Partner, in collaboration with the new employee's direct manager, compiles a list of necessary applications and data storage access. This list is then communicated to the IT Service Provider and the respective application owners.

The application owners, as designated in the Data Retention Policy, are responsible for reviewing active accounts and user rights at a frequency they deem necessary, ensuring alignment with the job responsibilities of the respective users. All unnecessary or excessive access rights should be revoked.

5.1.4 User Identification and Authentification

A unique and nominative user ID and password are required for every user. Generic accounts (e.g., administrators) must be kept to a minimum and managed by the designated application owners.

The International Fund has established the following password management and security rules, which all employees must follow:

- Passwords must contain at least 12 characters.
- Previously used passwords or their variants must not be reused.
- Commonly used passwords are prohibited.
- Individual passwords must be kept confidential and must not be shared with others under any circumstances.
- The same passwords must not be used across different services and systems.

- Where available, Single Sign-On (SSO) must be used. If SSO is unavailable, unique passwords must be used and securely stored in a password management system.
- Multi-Factor Authentication (MFA) must be enabled for all systems that offer this option.

5.1.5 Security Incident and Problem Management

All employees, contractors, and third-party vendors must report any suspected security incidents immediately to the IT Service Provider via the designated #ithelp channel on Slack.

Security incidents are categorized based on severity and impact, including but not limited to:

- Unauthorized access or data breach
- Malware infection
- Phishing attack
- Denial of Service (DoS) attack
- Insider threat.

Upon receiving an incident report, the IT Service Provider conducts an initial assessment to determine the nature and severity of the incident. In collaboration with International Fund personnel, the IT Service Provider identifies appropriate containment measures to prevent further damage.

To fully eradicate the incident, the IT Service Provider determines the root cause and implements a plan to remove any malicious or unauthorized components. Systems are subsequently restored to a known-good state.

The Finance Director is responsible for coordinating internal and external communications regarding the incident, including its scope, impact, and lessons learned, ensuring timely and accurate updates to stakeholders. The International Fund General Counsel must be consulted regarding potential legal and regulatory reporting requirements.

5.1.6 Antivirus

Antivirus software is installed on all International Fund devices. The IT Service Provider conducts regular monitoring to ensure compliance, tracking antivirus software versions, protection status (enabled/disabled, reboot required, etc.), and identifying any infected or at-risk devices.

5.1.7 Data Encryption and Protection

As a rule, all sensitive data, whether at rest or in transit, must be encrypted using industry-standard encryption protocols. Encryption keys should be managed securely

and updated periodically. The use of unencrypted removable media (e.g., USB drives, external hard drives) is prohibited unless explicitly approved by the Finance Director.

The International Fund employees must use PGP email encryption for communications whenever feasible. Exceptions may be made when encryption is impractical, such as when sending emails to recipients outside the International Fund. However, if security concerns arise when communicating with stakeholders in high-risk jurisdictions, encrypted emails should be prioritized. When email is not a practical option for sharing documents - whether due to volume or file size - employees must use the SendSafely platform for secure file transfer.

5.1.8 Cloud Security and Third-Party SaaS Applications

The International Fund must ensure that cloud service providers comply with security and data protection requirements. Employees must only use the cloud storage and collaboration tools approved by the IT Service Provider. Third-party vendors with access to the International Fund data must undergo a security assessment before integration.

5.1.9 Remote Work and VPN Usage

All International Fund employees working remotely must connect via a secure VPN and avoid public Wi-Fi networks unless using a secured mobile hotspot. Work-related activities must be conducted on International Fund-approved devices only. Screens must be locked when not in use, even in private home environments.

5.2 Physical security

5.2.1 Personal devices physical security

All workstations at the International Fund are company-owned Mac OS laptops. Employees must never leave their work devices in an unsecured location. The following general security rules apply:

- Do not allow friends or family to use work devices.
- Never leave the laptop unattended and always store it securely when not in use to prevent unauthorized access.
- When traveling, always keep the device in your possession as hand luggage.
- Exercise caution in airports, particularly at security checkpoints.
- Immediately report lost or stolen laptops to the Deputy Chief Executive Officer and the IT Service Provider.
- Secure any paper documents containing sensitive data in a locked location when not near your workspace.

5.2.2 Network Security Management

The International Fund's network is secured with firewalls at the network perimeters to prevent unauthorized access. The IT Service Provider reviews firewall inbound and outbound rules at least once a year to ensure they remain up to date. Additionally, network security devices are regularly monitored, with a dedicated process in place to detect and manage security incidents effectively**.**

5.2.3 Access Control for Office Premises

Access to the International Fund's office space must be restricted to authorized personnel only, with badge-based entry or biometric access where applicable. Visitor logs should be maintained, and guests must always be escorted by an employee. Employees must not prop open security doors or share access credentials.