Welcome the stranger.
Protect the refugee.

HIAS INFORMATION SECURITY POLICY

Effective: _____

I. Purpose

HIAS has an Information Security Program consisting of an array of policies, procedures, controls and measures. This Information Security Policy (ISP) is the foundation of this program and ties together all other policies as they relate to information security and data protection. HIAS's ISP covers all aspects of how we identify, secure, manage, use and dispose of information and physical assets as well as acceptable use protocols, remote access, password and encryptions. All information security policies and procedures should be read and referred to in conjunction with each other, as their meaning, controls and measures often overlap.

Information and physical security is the protection of the information and data HIAS creates, handles and processes in terms of its confidentiality, integrity and availability from an ever-growing number and wider variety of threats, internally and externally. Information security is extremely important and HIAS is committed to preserving Information Security of all physical, electronic and intangible information assets across the business, including, but not limited to all operations and activities.

We aim to provide information and physical security to:

- Protect client, beneficiary, staff and 3rd party data
- Preserve the integrity of HIAS and our reputation
- Comply with legal, statutory, regulatory and contractual compliance
- Ensure business continuity and minimum disruption
- Minimize and mitigate against organizational and business risk

II. Applicability

This Policy binds all staff employed or engaged by HIAS, whether in the United States, our country offices or in our resettlement support centers, including, permanent staff, fixed term and temporary staff, third-party representatives or sub-contractors, volunteers, interns and agents. For purposes of this Policy, the foregoing parties are collectively referred to as "HIAS Staff and associated personnel." Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

III. Compliance

HIAS is committed to collecting, processing, storing and destroying all information in accordance with the: (a) Regulations (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, known as the General Data Protection Regulation ("GDPR"); (b) data protection laws of the countries in which HIAS operates; and (c) any other associated legal or regulatory body rules or codes of conduct that apply to HIAS's business and/or the information HIAS processes and stores.

Where any provision of this Policy conflicts with a law or regulation, the law or regulation shall trump and supersede the conflicting provision.

IV. Purpose

The purpose of this document is to provide HIAS's statement of intent on how it provides information security and to reassure staff, clients and third-parties involved with HIAS their personally identifiable information (PII) is protected and secure from risk at all times. The PII HIAS manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of information.

V. Objectives

HIAS has adopted a set of principles and objectives to outline and underpin this policy and any associated information security procedures. PII will be protected in line with all our data retention and security policies and the associated regulations and legislation. The Data Protection Officer (DPO) of HIAS has the overall responsibility for the governance and maintenance of this document and its associated procedures. HIAS's Chief Information Officer (CIO) will review this policy and all data protection policies at least annually to ensure compliance with IT requirements and rules. HIAS's DPO collaboration with HIAS's General Counsel will review all policies annual to ensure business, legal, statutory and regulatory requirements and rules.

VI. Procedures & Guidelines

A. Access to Personally Identifiable Information (PII)

HIAS Staff and associated personnel will only be granted access to the PII they need to fulfill their role within the organization. Staff and associated personnel must not pass on PII to others unless they have also been granted access through appropriate authorization.

B. Secure Disposal of Information

Care needs to be taken to ensure information assets are disposed of safely and securely and in accordance with relevant procedures. HIAS uses secure shredding bins to assist in disposal of all documents [no longer required for a legitimate business purpose] containing PII. Electronic PII information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the HIAS, unless the disposal is undertaken under contract by an approved disposal contractor.

C. Data Encryption

Encryption methods are used to protect confidential and personal information within HIAS and when transmitted across data networks. HIAS Staff and associated personnel also use encryption methods when accessing HIAS network services, which requires authentication of valid credentials (usernames and passwords). Where confidential data is stored on or accessed from mobile devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders) the devices themselves are encrypted, irrespective of ownership. Where data is subject to an agreement with an external organization, the data should be handled (stored, transmitted or processed) in accordance with the organization's specified encryption requirements. Where there is a requirement to remove or transfer personal information outside of HIAS, it must always be kept in an encrypted format. Encryption must be used whenever appropriate on all remote access connections to the organization's network and resources.

D. Remote Access

It is the responsibility of all HIAS Staff and associated personnel with remote access privileges to HIAS's network, to ensure their remote access connection is given through HIAS's secure Virtual Private Network (VPN) – Cisco AnyConnect Secure Mobility Client. Secure remote access is strictly controlled via password authentication. At no time, should any HIAS employee provide their login or email password to anyone else.

E. Firewalls & Malware

HIAS understands adequate and effective firewalls, malware and protected gateways are one of the main and first lines of defense against breaches via the internet and our networks. Our Information Technology (IT) Department ensures anti-virus applications is running on all computers, networks and services and is updated and compliant. HIAS's Chief Information Officer (CIO) and IT Department is responsible for checking the log of all scans and for keeping

these applications updated and compliant. Systems are regularly scanned and assessed for unused and outdated software with the aim of reducing potential vulnerabilities and IT routinely removes such software and services from devices where applicable. The IT Department also has full responsibility for ensuring the latest application and software updates and/or patches are downloaded and installed, keeping our security tools current and effective. Security software is reviewed and updated monthly, or sooner where updates or patches are released.

F. Information on Desks, Screens and Printers

HIAS Staff and associated personnel who handle confidential paper documents should take appropriate measures to protect against unauthorized disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight in locked drawers and/or secure central filing spaces [for example a file library] at weekends and at other unattended times. Care should also be taken when printing confidential documents to prevent unauthorized disclosure. Computer screens on which confidential or personal identifiable information is processed or viewed should be protected [for example by privacy screens] and sited in such a way they cannot be viewed by unauthorized persons. All computers should be locked while unattended, please refer to HIAS's Clear Desk/Clean Desk Policy for procedures and more information.

VII. HIAS, payment card industry security standards, card storage & disposal

HIAS complies with the industry leading Payment Card Industry Security Standards Councils regulations and guidance. HIAS does not retain any donor data and/or credit card information. HIAS uses a third party secure payment gateway to process all transactions. HIAS understands the payment card brands directly (Visa, MasterCard etc.) enforce compliance with the PCI Data Security Standards (PCI DSS) and remain updated with any regulations and codes of conduct as they apply to HIAS.

VIII. Security Breach Management

HIAS has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed in HIAS's Data Breach Policy and Procedures. HIAS's Data Breach Policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

A. Breach Monitoring & Reporting

HIAS has appointed a Data Protection Officer (DPO) reporting to HIAS' General Counsel who is responsible for accompanying HIAS's Information Technology Department in review and investigation of any data breach involving personal identifiable information, regardless of the severity, impact or containment. HIAS Staff and associated personnel should report all data

breaches and incidents immediately to the DPO, following the procedures detailed in the Data Breach Policy. The DPO accompanying HIAS's IT Department and collaborating with the appropriate country office personnel will investigate all data breaches and incidences, even in instances where notifications and reporting are not required. To ensure gap and pattern analysis are used and available, HIAS will retain a full record of all data breaches and incidents. The DPO and IT Department will collaborate to revise and/or update any process or system where a system or process failure has given rise to a data breach or incident.

IX. Contact Information

HIAS Staff and associated personnel with any questions, concerns, or complaints about this Policy should contact HIAS's Data Protection Officer (DPO), Simone Walton by email at dpo@hias.org or by mail as per below:

HIAS, Inc.
1300 Spring Street, Suite 500
Silver Spring, MD 20910
Attn: Simone Walton, Data Protection Officer/Risk and Compliance Manager

X. Responsibilities

HIAS Staff and associated personnel are responsible for protecting and ensuring the security of the information to which they have access. Staff and associated personnel are responsible for ensuring all information in their direct work area is managed in accordance with this policy and any subsequent procedures or documents. HIAS will ensure staff do not attempt to gain access to information not necessary to hold, know or process and restrictions and/or encryptions are in place for specific roles within the organization relating to personal and/or sensitive information.

XI. Changes and Updates to this Policy

HIAS reserves the right to make changes and updates to this Policy as required. If modified the Policy will be made available to all HIAS Staff and associated personnel and on HIASnet indicating the date of the latest revision, and HIAS will comply with applicable law.