IABS Security Operating Procedures (SyOPS)
IFB Users

1. Scope

These Security Operating Procedures (SyOPs) cover:

- **The Error! Unknown document property name. information assets (hardware, software and data) at the Production. Pre-Prod and DR sites;**
- **The Error! Unknown document property name. Authorised Users (IFB);**

SyOPs detail the way in which the security controls and countermeasures, as defined in the Risk Management & Accreditation Document Set (RMADS) Part 3, must be executed.

1.1 Implementation

The SyOPs are presented within the RMADS as a complete document covering all the procedures for all Users.

1.1.1 **All Authorised Users of** Error! Unknown document property name.

As a prerequisite of being given access to **Error! Unknown document property name.** information assets, all Users must:

- read these SyOPs;
- complete, sign and submit the Form of Undertaking (Section 6).

1.1.2 **Changes**

When significant changes are made to **Error! Unknown document property name.**, the RMADS will be reviewed and might be amended. In this case, **Error! Unknown document property name.** Users will be informed of the changes and will be required to confirm their understanding of the changes.

1.1.3 **Authorisation**

These SyOPs are authorised by the IABS Accreditor and issued in accordance with the requirements contained in the Security Policy Framework

2. Responsibilities

2.1 System Manager

The System Manager is responsible for the correct operation and use of **Error! Unknown document property name.**.

The System Manager must:

a. identify the induction and training needs of **Error! Unknown document property name.** Authorised Users;

b. ensure all **Error! Unknown document property name.** Users are trained in:

   i. the operation of **Error! Unknown document property name.** appropriate to their business need and role;

   ii. password and token care and management;

   iii. incident reporting procedures.

c. consider the business need for all requests for changes to **Error! Unknown document property name.** hardware and software before submitting them to the Change Advisory Board (CAB);

d. consult with the CAB for any proposed change

e. inform the IABS Security Manager of any changes to be made to **Error! Unknown document property name.**;

f. carry out initial immediate investigation of security incidents involving **Error! Unknown document property name.**;

g. report all security incidents to the Accreditor via the HOIT Head of Security.

2.2 All Users

Error! Unknown document property name. Authorised Users are responsible to the System Security Officer for the day to day secure operation of **Error! Unknown document property name.**.

All **Error! Unknown document property name.** Authorised Users

a. must not allow any other person to use their **Error! Unknown document property name.** accounts, regardless of whether or not that other person is an Authorised User of **Error! Unknown document property name.**.

b. must not export, copy or otherwise remove information from **Error! Unknown document property name.** except in strict accordance with their business need;

c. must not import any software into **Error! Unknown document property name.** under any circumstances other than after explicit authorisation by the IABS Security Manager/System Manager.

d. Must not add or remove any hardware or firmware to or from **Error! Unknown document property name.** equipment

3. System Operating

3.1 Passwords

3.2 Physical Security

4. Media Management

4.1 General

The term “media” refers to any media holding protectively marked information - this includes paper as well as optical and magnetic media.

Media that have been used in the Laptop PCs must be marked and handled as SECRET items.

All media associated with **Error! Unknown document property name.** servers, removable and fixed, must be clearly marked with the protective marking of RESTRICTED.

Media that have been used in **Error! Unknown document property name.**, or have held Protectively Marked data:

a. must not be used on other systems of a lower protective marking unless the media have undergone approved downgrade procedures in accordance with HMG Infosec Standard 5

b. must be handled and disposed of strictly in accordance with HMG IS5

On completion of work, Authorised Users must secure all protectively marked media in locked containers.

4.2 Malicious Code

Any recordable media might carry a Virus or malicious code (i.e. Trojans/Worms).

Before any media are used in **Error! Unknown document property name.** the media must be checked to confirm that they do not contain any malicious code This is achieved by automatic use of **Error! Unknown document property name.** internal antivirus software to check the media before data on the media is accessed. This can also be accomplished by a dedicated standalone Anti Virus workstation.

If a User experiences any unusual behaviour from **Error! Unknown document property name.** or its applications, it must be assumed that malicious code might be present, and the following actions must be taken:

a. do not carry out any further activity on the workstation/Laptop PC;

b. inform the IABS Security Manager immediately;

c. make a paper record of the incident, including what actions were performed on the system in the period leading up to the incident. These should be retained and submitted to the IABS Incident Management Team and the IABS Security Manager;

5. Security Incidents

5.1 General

A security incident is any event which either results in an actual security breach or creates potential for a security breach to occur.

All Users of **Error! Unknown document property name.** must be aware of the need for security of information in the **Error! Unknown document property name.** environment. Adherence to these Security Operating Procedures will minimise the risk of a security incident occurring.

5.2 Incident Reporting

Any person discovering a security incident must report it immediately to HOIT Service Management, who must escalate the incident to HOIT Head of Security, in accordance with HOIT policy. Prompt action might prevent a simple incident from becoming a major incident.

Failure to report an incident is a serious offence and might lead to disciplinary action.

5.3 Emergencies

In any emergency situation, **the primary aim is the safety and protection of personnel**.

In the event of an emergency (e.g. fire, flood, external threat attack), the first consideration MUST be the protection of life. Only if it is safe to do so, then the following ordered actions should be taken with regard to **Error! Unknown document property name.**:

a. Workstations
   i. save any unsaved data;
   ii. close all applications;
   iii. remove and secure any removable media;
   iv. shut down the workstation;
   v. switch off power to the PC and monitor.

b. Laptop PCs
   i. remove any removable media;
   ii. powerdown the laptop;
   iii. remove the Flagstone device;
   iv. secure the Laptop PC and the Flagstone device in a suitable container.

c. Servers
   i. save any unsaved data;
   ii. close all applications;
   iii. stop all database services;
   iv. perform full off-line backup;
   v. remove and secure any removable media;
   vi. shut down the server;
   vii. switch off power to the server and monitor.

d. Physical
   i. Secure Server Room Doors
   ii. Return Server Room Keys
   iii. Return Secure Dongles
   iv. Lock secure furniture
   v. Clear documents from printers
   vi. Secure RapIDs

6. Key Contacts

Role	Contact	Contact Details
IABS Accreditor	Phil Clive	
HOIT Change & Release Management Team		
HOIT Crypto Custodian	Keith Morris	
HOIT Head of Security	Phil Thornton	
IABS Service Management	Carol Brown	
IABS Security Manager	Anthony Brown	
Home Office IT Service Desk		0845 000 0050
HOIT Incident Management team		xxxx12

7. Glossary

BS	Baseline Standard
CAB	Change Advisory Board
CAPS	CESG Assisted Products Service
CESG	Communications-Electronics Security Group
CIO	Chief Immigration Officer
CTC	Counter Terrorist Check
DR	Disaster Recovery
DSU	Departmental Security Unit
GPG	Good Practice guide
IABS	Immigration & Asylum Biometric System
IFB	Immigration Fingerprint Bureau
IL	Impact Level
ITIL	IT Infrastructure Library
ITHC	IT Health Check
HOIT	Home Office IT
HSM	Hardware Security Module
KEK	Key Encryption Key
PGP	Pretty Good Privacy
RMADS	Risk Management Accreditation Document Set
RTP	Risk Treatment Plan
SC	Security Check
SWG	Security Working Group
SyOps	Security Operating Procedures
UKBA	UK Borders Agency

8. Form of Undertaking

This form replaces, where applicable, the previous IAFS form. It must be photocopied, completed and returned to the IABS Security Manager (FAO: Anthony Brown, 4th Floor, xxxxx by every Authorised User of **Error! Unknown document property name.**. An email from users acknowledging acceptance of the terms in the SyOps will also be accepted.

The User account will not be authorised or activated until this form has been received by the IABS Security Manager. Where account are already activated, these may be suspended if the SyOps has not been signed and returned by 20 days from receipt.

- I have read and understand **Error! Unknown document property name.** Security Operating Procedures.
- I understand my responsibilities as a User of **Error! Unknown document property name.**.
- I have received and understand **Error! Unknown document property name.** User Training.
- I have received my username and initial password.
- I will protect my password and not reveal it to any other person for any reason.
- If I suspect that my password has been compromised I will inform the IABS Security Manager as soon as possible.
- I will inform the IABS Security Manager if and when I no longer need my account on **Error! Unknown document property name.**.
- I acknowledge that my use of **Error! Unknown document property name.** will be monitored.
- I undertake to observe **Error! Unknown document property name.** Security Operating Procedures and to take all reasonable precautions to ensure that I do not breach the security of **Error! Unknown document property name.**.
- I understand that if I fail to observe **Error! Unknown document property name.** Security Operating Procedures I might prejudice the UKBA business interests, and that I might have my account on **Error! Unknown document property name.** suspended and/or be liable to disciplinary action.

Name: ..... Post: .....

Signature: ..... Date: .....