*All gists in the following extract have been underlined

The SIS database User
Security Operating Procedures (SecOps)
(abridged version for End users and Line managers)

Freedom of Information Act 2000: This document relates to the measures taken to protect an information System that holds sensitive material/information arising directly or indirectly from, or relating to the clandestine activities of the intelligence and security services. As such, the document in its entirety is entitled to **absolute exemption** under section 23 of the Freedom of Information Act.

Approvals		
Role	**Signature**	**Date**
[redacted]		
Author		
[redacted]		
Security Approval		

Date	Issue	Comment
Jan 09	Draft 0.1	First draft for review derived from the corporate system Generic SecOps and the database SEC OPS
Feb 09	Draft 0.2	Amendments following review comments from [redacted]
Feb 09	Final 1.0	Final version following sign off from [redacted]

Contents

Introduction

1 This document is the database Security Operating Procedures (SecOps) for users of the system. It is intended for all users who possess read only access of the database and no additional privileges.

Scope of SecOps

2 These SecOps apply to secure operation of the the database system which is on a standalone network and is accessed through the corporate system [redacted]. They do not apply to the development or integration environments.

3 These SecOps are in addition to the generic corporate system SecOps. Generic corporate system SecOps are applicable to the database. Users requiring additional privileges should refer to the database Security Operating Procedures (ref 5).

Compliance with SecOps

4 Everyone who is expected to comply with these SecOps shall have access to a copy of the appropriate section or sections of the SecOps. They shall be required to acknowledge they have read and understood the relevant sections and agree to act in accordance with them. Any person found to be in breach of these security procedures shall be subject to investigation by the Security Authorities, and may be subject to disciplinary action and/or civil prosecution.

5 All users of the database are required to comply with these SecOps. Every user will be required to sign a copy of the database SecOps User Declaration, which will be placed on their staff file, to acknowledge their agreement to comply with the SecOps relevant to their role. This process will be repeated whenever a new version of the SecOps is issued and, in any event, at least once a year.

Compliance with ISO/IEC 27001:2005

6 SIS is formally committed to achieving compliance with the ISO/IEC 27001:2005 – the international standard for the management of information security. Accordingly, the security section is in the process of devising an ISO 27001-compliant Information Security Management System (ISMS) and will be issuing a number of related procedures, guidelines and standards. In addition to following the SecOps documented below, all staff will be expected to comply with these procedures, guidelines and standards, once they are issued.

7 In particular, all staff should be aware that effective management of security requires that records should be maintained that will provide evidence, to management and to auditors, that the ISMS is being operated correctly. Accordingly, as a general principle, staff are expected to keep records of all security-relevant actions and decisions. These records must be legible, readily identifiable and retrievable.

Protective Marking

8 The database system shall have a Risk Management Accreditation Document Set (RMADS) which will explicitly state the protective marking which the system is allowed to process.

Roles and Responsibilities

9 Responsibility for secure operation of the system and compliance with these SecOps is a matter for everyone who uses it, whether as an end-user, or as someone involved in its day to day management and administration.

10 Anyone with access to the system should read and comply with the general procedures set out in the "End User" section of this document.

11 Whilst everyone has a general responsibility for system security, some roles have additional security-related responsibilities, and these are documented in the unabridged version of the database system SecOps.

12 Anyone who occupies any of the roles in the following list should read and comply with the rules in the appropriate section of the unabridged version of the database System SecOps.

a. Technical Services Manager
b. Technical Services Staff
c. Network Manager
d. Network Management Staff
e. Computer Suite Manager
f. Computer Operators
g. Security Department
h. Help Desk
i. Business Continuity Manager
j. Configuration Manager
k. Change Manager
l. Records Management
m. System Sponsor

13 The remainder of this SecOps deals with the security controls assigned to the following roles:

End User

n. Line Manager

End User

Information Labelling and Handling

14 All hardcopy output from the system shall bear the appropriate protective marking and shall be handled in accordance with that protective marking. The rules for handling protectively marked material are set out in the SIS previous policy guidance (available via the SIS intranet pages).

15 [redacted]

16 [redacted]

17 [redacted]

18 [redacted]

19 [redacted]

20 [redacted]

21 [redacted]

Line Manager

Roles and Responsibilities

22 A Line Manager shall be responsible for ensuring that their staff's security roles and responsibilities are defined and documented.

23 A Line Manager shall be responsible for ensuring that their staff receives appropriate training in Information Security Awareness.

Access Control

24 A Line Manager shall be responsible for granting authorization for members of their staff to be given access to the database system in order to carry out their duties. The line manager is responsible for verifying if access to the database is required. [redacted]

25 End user Access to the database is restricted [redacted].

Annex A : Reporting of Security Incidents

A.1 The process of incident reporting is of vital importance in maintaining the overall security of the system.

[redacted]

User Declaration

I acknowledge that I have read the above SecOps, that I understand them, and agree to abide by them.

SIGNATURE:

DATE of SIGNATURE:

STAFF NUMBER:

DESIGNATION:

NAME (Print):