Security Industry Authority

APPENDICES TO SCHEDULES

SIA LICENCING OPERATIONS CONTRACT

Security Industry Authority

- and -

British Telecommunications plc

CONTRACT

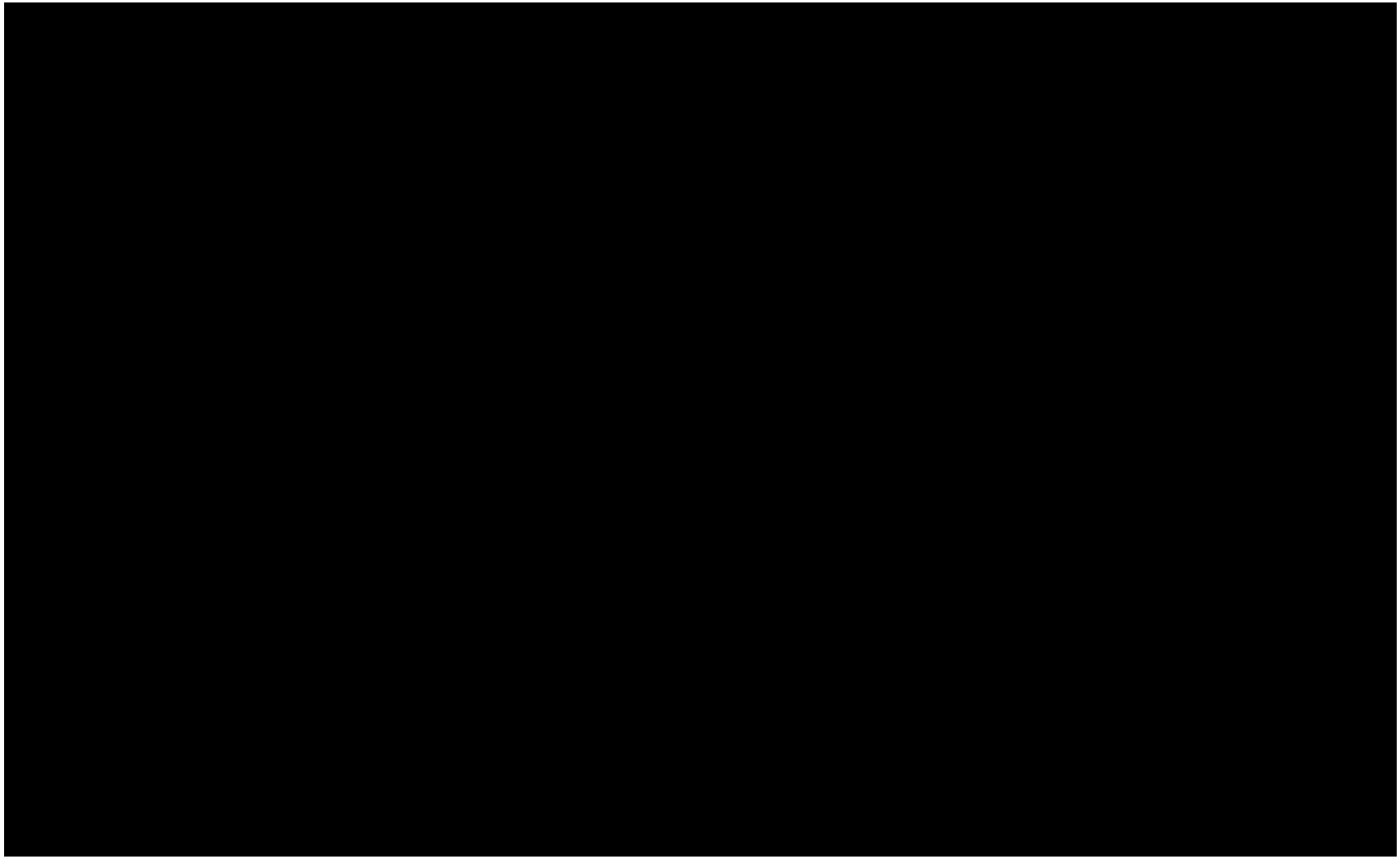
relating to

the supply of
ICT Goods and Associated Services

VERSION DRAFT 0.1

CONTENTS

1. APPENDIX ONE: SERVICE CREDIT CALCULATOR



2. APPENDIX TWO: KEY PERSONNEL

3. APPENDIX THREE: OUTLINE SECURITY PLAN

Outline Security Plan

Example Draft Security Plan

Introduction

This document is the Draft Security Plan for the 'xxxxxxx' for the Home Office.

Purpose and Scope

The purpose of this document is to describe the service in such a manner that Accreditation may be achieved.

The scope of this document is limited to defining the security aspects of the xxxxxxx network.

Terms and Abbreviations

BC	Basic Check
CAPS	CESG Approved Products Scheme
CESG	Communications and Electronics Security Group
HMG	Her Majesties Government

Change History

Issue	Date	Change
0.1		Initial draft

Part 1: Basic Information

The Scope of the Accreditation

The subject of accreditation is the xxxxxxx network

Links and Dependencies

The security strategy for xxxxx complies with the following legislation and standards:

a) The Data Protection Act 1998
b) The Regulation of Investigation Powers Act 2000
c) The Computer Misuse Act 1990
d) The Manual of Protective Security
e) CESG Memorandum 26 – Passwords for Identification and Authentication
f) CESG Memorandum 22 – Protective Monitoring
g) CESG Infosec Manual T – Transport Layer Protocol – Implementation Recommendations for HMG Protectively Marker Material
h) CESG Infosec Standard 5 – Secure Erasure of Protectively Marked Information
i) JSP 440 – Defence Manual of Security
j) ISO27001

IT Resources

Hardware:

Software:

Business Functions Supported by xxxxxxx

Asset Valuations

Confidentiality Requirements:

The xxxxxxx will store data at xxxxxx

Availability Requirements:

.

Integrity Requirements:

The integrity of the data being transferred over xxxxx must be maintained and any unauthorised changes may impact the operation xxxxxx albeit at a xxxxxx level.

User Groups

Access to the service from a user perspective will be from service subscribers who will all be cleared to at least BC.

Security Personnel – Responsibilities

The following individuals within the CONTRACTOR have responsibilities for xxxxx:

Compliance Audit and Re-accreditation Arrangements

As a minimum, the XXXXXX shall be audited.

Part 2: Risk Management Documents

Risk Management Summary

The threats to the confidentiality, integrity and availability of information..

Residual Risk and Requirement for Assured Barriers

1. The residual risk and requirements for assurance barriers were derived using HMG Infosec Standard 1 – Residual Risk Assessment Method

Risk One – Un-authorised Access to Data

Countermeasures

Access Control Measures

Identification and Authentication (ID&A) Measures

Protective Monitoring

Object Reuse (remanence)

Communication Security and Cryptographic Requirements

System Security Maintenance

Virus prevention:

Contingency Measures:

System Maintenance:.

Business Continuity

a) The business continuity plan for XXXXXX is contained in document XXX/YYY.

References

Ref	Description	Reference	Date
1	The Data Protection Act 1998		
2	The Regulation of Investigation Powers Act 2000		
3	The Computer Misuse Act 1990		
4	The Manual of Protective Security		
5	CESG Memorandum 26 – Passwords for Identification and Authentication		
6	CESG Memorandum 22 – Protective Monitoring		
7	CESG Infosec Manual T – Transport Layer Protocol – Implementation Recommendations for HMG Protectively Marker Material		
8	CESG Infosec Standard 5 – Secure Erasure of Protectively Marked Information		
9	JSP 440 – Defence Manual of Security ISO27001		
10			

Appendix 1

External Attackers to XXXXXX Data

Parameter	Selection	Value
Combined Impact Value	Un cleared attackers, impact Level 3	11.2
Environmental Factors	Normal	0
Number of Potential Attackers	Greater than 5000	2.0
Cumulative Opportunity	Over 80 hours, low facilities	0
Level of Publicity	Known	0
Protective Monitoring	Partial	-0.3
Quantity of Data	Greater than 1 Gbyte	0
Assurance of barriers	Barrier equivalent to EAL3 (CAPS Approved)	-3

Total Residual Risk Indicator 9.9

Appendix 2

XXXXXX staff to Subscriber Data

Parameter	Selection	Value
Combined Impact Value	BC attackers, impact Level 3	7.4
Environmental Factors	Normal	0
Number of Potential Attackers	11-50	0.4
Cumulative Opportunity	Over 80 hours, Extensive facilities	2.0
Level of Publicity	Known	0
Protective Monitoring	Partial	-0.3
Quantity of Data	Greater than 1 Gbyte	0
Assurance of barriers	None assured	0

Total Residual Risk Indicator 9.5

Part 3: Security Operating Procedures

The Scope of These Operating procedures

These Security Operating procedures describe the mandatory requirements for all users to maintain the security of XXXXXX..

Routine Requirements

You are personally responsible for:

Password and Token Management

Starting an XXXXX Session

XXXXX Access Sessions must only be made from the thin client access

While Running a Session

When working with classified information ensure.....

Completing a Session

Close down

Incident Management Procedures

Incident Reporting Procedures

XXXXXXX

Acceptance of Responsibility

I, the undersigned, have read and agree to comply with the XXXXXXX Security Operating Procedures.

I understand that failure to comply with these Operating procedures shall be treated as a serious disciplinary matter.

Signed: Date

Name (In Block Letters)

Staff Designation (In Block Letters)

Accreditation Certificate

I confirm that the Security Operating Procedures contained within Accreditation Document Set reference xxx **Error! Unknown document property name.** satisfactorily implement the agreed Risk Management Statement. The IT resources described may therefore be operated in accordance with those Procedures. They remain subject to the compliance checks and re-accreditation conditions described in the Accreditation Document Set.

Signature: Date:

Name: Post:

4. APPENDIX FOUR: IMPACT LEVELS

IS1 Impact Level	Impact of Compromise	e-Government Impact Level	MPS Protective Marking
N/A	• Minimal inconvenience to any party • No risk to any party's personal safety • Minimal financial loss to any party • No damage to any party's standing or reputation • No distress caused to any party • No assistance in the commission of or hindrance to the detection of crime	0	Nil
1	• Minor inconvenience to any party • No risk to any party's personal safety • Minor financial loss to any party • Minor damage to any party's standing or reputation • Cause minor distress to any party • No assistance in the commission of or hindrance to the detection of crime	1	Nil
2	• Significant inconvenience to any party • No risk to any party's personal safety • Significant financial loss to any party • Significant damage to any party's standing or reputation • Significant distress caused to any party • Assistance in the commission of or hindrance to the detection of crime	2	Nil
3	• Substantial inconvenience or distress to any party • Risk to any party's personal safety • Substantial financial loss to any party, or cause loss of earning potential to, or facilitate improper gain for, individuals or companies • Substantial damage to any party's standing or reputation • Prejudice the investigation or facilitate the commission of crime • Breach proper undertakings to maintain the confidence of information provided by third parties, or statutory restrictions on disclosure of information (except DPA where other impact statements should be used) • Make it more difficult to maintain the operational effectiveness or security of UK or allied forces • Impede the effective development or operation of government policies • Disadvantage government in commercial or policy negotiations with others • Undermine the proper management of the public sector and its operations	3	RESTRICTED

4	• Materially damage diplomatic relations, that is, cause formal protest or other sanctions • Prejudice individual security or liberty • Cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations • Work substantially against national finances or economic and commercial interests • Substantially undermine the financial viability of major organisations • Impede the investigation or facilitate the commission of serious crime • Seriously impede the development or operation of major government policies • Shut down or otherwise substantially disrupt significant national operations	Nil – seek advice from the security authorities	CONFIDENTIAL