Specialist Reporting Agencies
Secure Web Site Application
1. Background

In the past, Crown Office & Procurator Fiscal Service (COPFS) had two distinct methods in place to allow Specialist Reporting Agencies (SRAs) to report the details of cases for prosecution to the Department.

One of the methods used by SRAs was simply the physical submission of the relevant paper document(s). This method was used where the use of secure networks and/or the creation of an electronic reporting application were not cost-effective for the participant.

From 01 January 2006, the only method for reporting to the PF is electronically. Many SRAs use a secure e-mail system, allowing the transmission of Standard Prosecution Reports (SPR) and ancillary documents over secure communication lines. The secure email transport is reliant on organisations achieving accreditation for the Government Secure Intranet (GSI), the Government Secure Extranet (GSX) or the Criminal Justice Extranet (CJX). These networks are, primarily, used by larger organisations.

COPFS realised that many SRAs could not provide a cost-effective means of reporting electronically and decided to investigate the possibility of establishing a secure web site that would provide this facility.

The developed web site has been in operation since August 2005 functioning under its own URL. It is not integrated into the existing COPFS web site and there is no ‘branding’ of the web site as a means of providing some anonymity.

2. Scope, Exclusions and Benefits

2.1.1 Scope

The SRA provides the functionality for users to:

2.1.1.1 Login securely
2.1.1.2 Submit an email to the COPFS helpdesk for forgotten password
2.1.1.3 Create, Edit, View, Delete and Submit Standard Prosecution Reports (SPRs)
2.1.1.4 Create, Edit, View, Delete and submit SPR related auxiliary documents, such as Witness Statements
2.1.1.5 View and Delete Registered SPRs
2.1.1.6 Submit requests for Scottish Criminal Records Office (SCRO) details.
2.1.1.7 View and Delete SCRO responses received.
2.1.1.8 Maintain passwords
2.1.1.9 Request changes to registered account information
2.1.1.10 Send simple text mail messages to the designated COPFS mailbox

2.1.1 Exclusions

The SRA website does not include:

2.1.1.11 Direct access to Scottish Criminal Records Office
2.1.1.12 Direct access to Crown Office operational database information
2.1.1.13 Management information reports

2.1.1 Benefits

2.1.1.14 Menu and form driven report completion
2.1.1.15 Information entered carried forward i.e. no re-keying
2.1.16. Real-time validation of data
2.1.17. Drop down menus
2.1.18. Charge Database on-line
2.1.19. Faster submission.
2.1.20. An error report (if applicable) notified quickly on SPR submission
2.1.21. A PF Reference Number generated quickly for correctly submitted SPRs. (Easier dialogue with PF Offices as number can be quoted for fast search)

3. System Requirements

To access the website you will require a PC that has access to the Internet e.g. dial-up modem, broadband, T1, etc. In addition, the PCs used to access the site must have one of the following browsers –
3.1. Internet Explorer 5.5 or above OR
3.2. Netscape 6.0 or above
An email address, though not essential, is highly desirable. Crown Office would use this for the transmission of administrative details only.

4. Registration

Each person within your Agency or Organisation who is approved to submit cases to the PF must be registered individually. Each person should complete the attached Form SRA1 (attached as Annex A) and submit this to their manager/director for authorisation on behalf of the Agency/Organisation.

On receipt of the form, Crown Office will validate the contents and, if correct, register the Agency and the user on its national database systems. The user will receive their digital certificate[1] by recorded delivery (addressee only).

[A digital certificate is an electronic means of establishing your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder’s public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient (Crown Office in this case) can verify that the certificate is real.]

5. Training

When a user is first registered, they will not be permitted to immediately send reports to the PF live system. Each user will be initially registered as a Trainee and permitted to use the system to practice the preparation of SPRs and other documents on-line. In addition to their certificate each user will receive a copy of the “User Guide to the SRA Website”. This will explain how to login, change details, provide an overview of preparing case data, completing documents on-line and information about receipting from COPFS systems.

6. Sending Live Reports

You will be able to send live cases to the PF when you have undertaken the successful completion of approximately 5 cases as a “Trainee”. It is estimated that this number of cases per trainee should be sufficient to prepare for the live environment. The site has been developed to highlight errors as you enter information and will also provide useful error information should your report not apply to the COPFS database. When you are comfortable
with the operation of the site in Trainee mode and wish to move to live status, you simply contact the COPFS Help desk and the change will be effected almost immediately.

7. Website Layout

The screens have been created to align with standard Windows© look and feel but will not carry logos or other graphic images. This is deliberate and is intended to assist those who are using a low-speed dial-up connection. There are examples of a wide variety of screens at Annex B. Note: The colours and layout might differ slightly on the final application.

8. Security

The website contains a secure application and sub-judice information. There are, therefore, some practical guidelines that you should follow for the operation of the system. These are contained within "Information Security Guidance for SRAs" that is contained at Annex C.

9. Annex A (Application Form)

Completed forms should be sent to:

Crown Office ISD, 8th Floor
Procurator Fiscal Office
29 Chambers street
Edinburgh
EH1 1LD
23/11/2012

Please see the next page
<table>
<thead>
<tr>
<th>AGENCY NAME</th>
<th>HQ ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Line 1 *</td>
<td></td>
</tr>
<tr>
<td>Address Line 2 *</td>
<td></td>
</tr>
<tr>
<td>Address Line 3</td>
<td></td>
</tr>
<tr>
<td>Address Line 4</td>
<td></td>
</tr>
<tr>
<td>Post Code</td>
<td></td>
</tr>
<tr>
<td>Telephone Number *</td>
<td></td>
</tr>
<tr>
<td>Fax Number *</td>
<td></td>
</tr>
<tr>
<td>Email (if applicable)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APPLICANT’S LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Line 1 *</td>
</tr>
<tr>
<td>Address Line 2 *</td>
</tr>
<tr>
<td>Address Line 3</td>
</tr>
<tr>
<td>Address Line 4</td>
</tr>
<tr>
<td>Post Code</td>
</tr>
<tr>
<td>Telephone Number *</td>
</tr>
<tr>
<td>Fax Number *</td>
</tr>
<tr>
<td>Email *</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APPLICANT DECLARATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>I declare that I am an employee of the above named organisation and have approval to submit information to the Crown Office and Procurator Fiscal Service in relation to criminal proceedings. I have read and agree to abide by the guidelines detailed in the “Information Security Guidance for SRAs.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signed*</th>
<th>Date*</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Name (BLOCK CAPITALS)*</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Position (BLOCK CAPITALS)*</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>AGENCY AUTHORIZATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>I confirm that the person named above is an employee of the above named organisation and has approval to submit information to the Crown Office and Procurator Fiscal Service in relation to criminal proceedings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signed*</th>
<th>Date*</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Name (BLOCK CAPITALS)*</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Position (BLOCK CAPITALS)*</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Method of Certificate Delivery*</th>
<th>DISKETTE</th>
<th>COMPACT DISC</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>of Readiness (if not immediate)*</th>
</tr>
</thead>
</table>

* Mandatory Entry

<table>
<thead>
<tr>
<th>CROWN OFFICE USE ONLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENCY ID CODE</td>
</tr>
<tr>
<td>AGENCY LOCATION CODE</td>
</tr>
<tr>
<td>USER CERTIFICATE ID</td>
</tr>
<tr>
<td>Details validated on (date)</td>
</tr>
<tr>
<td>By (Signature &amp; BLOCK CAPITALS)</td>
</tr>
<tr>
<td>Details registered on (date)</td>
</tr>
<tr>
<td>By (Signature &amp; BLOCK CAPITALS)</td>
</tr>
</tbody>
</table>
10. Annex B (SRAII Screens)

Landing Page

Prosecution Reports Screen
Add New Incident

Charge Picker Screen
## Witness Report Main

### SPR Menu

- Home
- Prosecution Reports
- Your Investigations
- Witness List
- Change Order
- User Menu
- Help
- Copyright

### SPR Menu Details

- 5 Name: John Doe
- 5 Surname: Smith
- 5 Witness Type: Test

### Witness List

<table>
<thead>
<tr>
<th>Name</th>
<th>Surname</th>
<th>Witness Type</th>
<th>Date of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Doe</td>
<td>Smith</td>
<td>Test</td>
<td>01/01/1970</td>
</tr>
</tbody>
</table>

### Civilian Witnesses

<table>
<thead>
<tr>
<th>Name</th>
<th>Surname</th>
<th>Witness Type</th>
<th>Date of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jane Smith</td>
<td>Doe</td>
<td>Test</td>
<td>01/02/1971</td>
</tr>
</tbody>
</table>

### Agency Officer Witnesses

<table>
<thead>
<tr>
<th>Name</th>
<th>Surname</th>
<th>Witness Type</th>
<th>Date of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Brown</td>
<td>Davis</td>
<td>Test</td>
<td>02/01/1972</td>
</tr>
</tbody>
</table>

## Witness Report Detail

### SPR Menu

- 5 Name: John Doe
- 5 Surname: Smith
- 5 Witness Type: Test

### Witness Details

- **Name:** John Doe
- **Surname:** Smith
- **Witness Type:** Test
- **Date of Birth:** 01/01/1970
- **Age:** 40
- **Occupation:** Accountant
- **Contact Details:**
  - Telephone: 123-456-7890
  - Email: johndoe@example.com
- **Additional Details:**
  - Vulnerability Category: High
  - Vulnerability Specifics: None
  - Responsible Person: Jane Smith
  - Date of Involvement: 02/02/2020
  - Resolved Incident Type: Test
  - Additional Notes: None
11. Annex C (Security Guidance)

1. Section 1 – Introduction

1.1. Purpose and Scope

The purpose of this guidance is to define a security framework for users requiring access to the Crown Office and Procurator Fiscal Service (COPFS) secure website created for Specialist reporting Agencies (SRAWEB). The guidance should be read by staff responsible for the security of criminal case information in all non-police organisations with SRAWEB access.

This guidance has been produced for non-police users requiring access for the creation and updating of case records.

The content of this guidance accords with the ISCJIS Baseline Security document. This guidance does not seek to supersede that document.

If your organisation has already agreed the ISCJIS BSD document and Policy Statement, the information contained hereafter will be considered an aide-memoire.

The scope of this document includes aspects of security designed to protect:

Confidentiality ensuring that any information obtained via SRAWEB is disclosed only to authorised users for legitimate purposes;

Integrity ensuring that SRAWEB information is not changed or deleted, except by authorised users with a legitimate reason;

Availability ensuring that the SRAWEB is available for use when required.

1.2. Background

This guidance has been based on a risk analysis.

The guidance is mainly concerned with security issues and should be regarded as according with the security measures required under Principle 7 of the Data Protection Act 1998 (DPA).

Other documents, which relate to this guidance are:

ISCJIS Baseline Security Document

1.3. Structure

Section 2, System Description, summarises the purpose of SRAWEB, the information stored on the system and the principal users. Organisations with access to SRAWEB information are described in this document as Information Users (IUs).

This section also contains a summary of Legal and Statutory Obligations relevant to the SRAWEB and the way in which the information it holds is accessed and used.

Security Roles and Responsibilities describes a number of key roles in the management of information security and clarify how these roles are to be fulfilled for the SRAWEB. The impact of increasing non-police use of the system is also considered.
Section 3, Summary of Risk Analysis, provides a brief description of the principal threats to, and the vulnerabilities of, the SRAWEB system. It also describes the likely impact of breaches of security involving SRAWEB information.

Section 4, Security Policy identifies high-level security requirements. These are expanded in Appendix A.

Section 5, Administration of Security, defines who is responsible for maintaining this document and when, and under what circumstances, it should be reviewed.

Appendix A, Connection Rules, defines the security controls to be complied with in the local systems of Information Users.

Appendix B, Required Skills, lists the knowledge, experience and skills required for the SRAWEB roles identified in Section 2.

2. Section 2 - System Description

2.1. Introduction

This section describes the scope of the SRAWEB system and its environment. The following aspects are covered:

System Outline - an overview of SRAWEB

SRAWEB Information Users - the organisations which have access to SRAWEB information;

System Configuration - a brief description of the hardware and software infrastructure used to deliver the SRAWEB service to users;

Legal and Statutory Obligations - a description of legislation governing the way in which the SRAWEB and the information it holds is accessed and used;

Security Roles and Responsibilities - describes a number of key roles in the management of information security and clarifies how these roles are to be fulfilled for the SRAWEB;

Data Access Policy - defines two levels of policy to control access to SRAWEB data.

2.2. System Outline

The SRAWEB

The SRAWEB provides a repository for SRA information on persons who are/will be the subject of criminal proceedings.

The SRAWEB systems are located within a site under the direct control of COPFS and is accessed from Windows based systems situated at the premises of an authorised agency. At present, there is no Disaster Recovery solution in place and Business Continuity would be provided by reverting to paper-based reporting.

The data held on the SRAWEB relates to:

a) Criminal Cases
This comprises records that form the basis for SPR construction e.g. individuals who will be reported for alleged offences – also recorded

b) Ancillary Documentation

This comprises information related to cases held on SRAWEB e.g. Witness Statements
The data held on the SRAWEB is classified under the government's protective marking scheme as ‘RESTRICTED’.

The following organisations have access to the SRAWEB:

- Government Agencies and departments
- Other non-police reporting Agencies

The access to SRAWEB is granted for the purpose of: reporting alleged offenders/offences for consideration by Procurators Fiscal aiding the administration of justice

2.3. Legal and Statutory Obligations

The principal areas of legislation which apply to the security of the SRAWEB are:

- The Data Protection Act 1998;
- The Computer Misuse Act 1990;

The Data Protection Act 1998 governs the security and proper use of personal information and makes special provisions in respect of sensitive data. The information held on the SRAWEB is predominantly sensitive data in terms of the Act.

Processing of personal data held on computer systems and specific manual systems must be notified under the Act and information may, with some exemptions, only be used by, or disclosed to, persons covered by the notification. The Act contains eight Data Protection Principles governing the way personal data is stored and processed. For the purposes of this policy, the most important is the Seventh Principle, which states:

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

The Computer Misuse Act 1990 makes it a crime to knowingly access a computer system or modify its contents without permission. It applies whether the access comes from within or outside the organisation. The Act is worded so that it applies not only to direct access, but also where the user is entering instructions on a computer system other than the one affected e.g. a local computer terminal. An offence is only committed if the access is unauthorised and the user is aware that it is unauthorised.

Any user who knowingly accesses SRAWEB information other than for authorised purposes is, therefore, committing an offence and may be subject to internal disciplinary procedures/criminal proceedings.

Information Users must ensure that their staff are aware of what constitutes unauthorised access. The SRAWEB and any local systems through which the SRAWEB information may be accessed should, when possible, display a warning to this effect as part of the login process.
The Official Secrets Act 1989 makes it an offence to disclose official information that could be detrimental to the national interest. It applies to Crown Servants, government contractors or a person who has, or has had, official information in their possession. For the purposes of the Act 'Crown Servant' includes civil servant, members of the armed forces and the police.

An offence is committed under the Act if the information is disclosed without lawful authority. Information is disclosed with lawful authority if, and only if, it is disclosed in accordance with official duty. Information is protected by the Act under a number of categories of which the following is relevant to the use of the SRAWEB:

Crime: information the disclosure of which
results in the commission of an offence or
facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody or
impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders or
which is such that its unauthorised disclosure would be likely to have any of those effects.

2.4. Security Roles and Responsibilities

This section defines:

- ownership of the SRAWEB system and responsibilities for the data;
- other roles associated with the security and data protection of information in the light of proposals to extend SRAWEB access;
- a policy on the reporting and investigation of security incidents.

There is an established principle that the accuracy of each SRAWEB record is the responsibility of the organisation that created it or the organisation that last updated it. Where originators receive data from other sources, e.g. a Scottish Police Record Office (SPRO), they should take positive steps to manage their relationship with the source to ensure that the quality of the data received is maintained i.e. quality assurance of the information initially provided to SPRO/Scottish Criminal Records Office (SCRO).

The accuracy of the data remains the responsibility of the source, but its privacy becomes the recipient’s responsibility. The source retains responsibility for the privacy of the data up to the point at which the recipient receives the information.

The COPFS Departmental Security Group formulates policy on the protection of information on the SRAWEB. This forum under the direction of the Management Board defines the COPFS Information Security Policy.

There are a number of other principal roles required for the management of SRAWEB security. The roles are either:

central, which will be functions of COPFS and will be concerned with policy, strategic matters and administration of the central SRAWEB system; or

local, that is, they should exist in the organisation of each Information User and will be concerned with the use of SRAWEB information and the security of the IU’s own systems and networks through which access is made to the SRAWEB.
The following roles are defined in detail below:

Crown Office IT Security Officer (ITSO)
Crown Office/Local Data Protection Officer (DPO)

The IT Security Officer (ITSO) role is required centrally at COPFS for the SRAWEB system. The ITSO is responsible for ensuring that appropriate security management actions are taken to protect the confidentiality, integrity and availability of the information stored and processed on the system. This responsibility includes:

- ensuring that security measures are implemented on central SRAWEB facilities in accordance with COPFS Information Security Policy;
- regular liaison with Data Protection Officers on information security matters;
- monitoring audit logs for unauthorised system management activities and unauthorised attempts to access the system;
- documenting operator and administrator procedures required to implement this security policy in a security manual;
- assisting in the investigation of security incidents;
- submitting regular reports on information security to:
  - confirm that regular security actions have been undertaken
  - report changes to user authorisations;
  - report any security incidents and the actions taken to resolve them

The Data Protection Officer role is required centrally at COPFS for the SRAWEB system and locally at IUs. The Data Protection Officer is responsible for implementing the data access policy and will have day-to-day responsibility for protecting the data. This responsibility should include:

1. identifying, reviewing and testing local application controls;
2. confirmation of the accuracy, completeness and legitimacy of transactions;
3. informal monitoring of local staff compliance with policy;
4. monitoring of system audit logs relating to application use;
5. liaison with the central and IU ITSOs on security matters;
6. assisting in the investigation of security incidents.

The local Data Protection Officers also undertake internal audit functions, checking for compliance with policy, procedures and standards.
3. Section 3 - Summary of Risk Analysis

3.1. Introduction

Specific risks to COPFS systems have been determined by a process of risk assessment, undertaken partly by an in-house team (PD3002 & some CRAMM) under guidance from the Department CLAS Consultant/BS7799 Lead Auditor and partly (IS1& IS3) by the Department CLAS Consultant. The processes taken into account include:
HMG Infosec Standard No. 1 Assurance Requirements for IT Systems (June 2003)
HMG Infosec Standard No. 4 Comsec Requirements
HMG Infosec Standard No. 3 Interconnecting Business Domains (January 2003)

3.2. Threats and Vulnerabilities

Some of the specific threats identified are relevant to COPFS IT Security only and will not be reproduced in this document. Examples of common threats are:-

3.2.1. External hacking - which in this context may broadly be defined as attempts to gain unauthorised access to the COPFS from external networks for a variety of malicious or unauthorised objectives, such as illicit access to (or collection of) information, illicit changes to information, and destruction of information.

3.2.2. Internal hacking - which involves much the same issues as external hacking except that it is carried out by individuals from hosts within the security domains of members of the Government Secure Intranet community rather than from the Internet. This means that the individual may have detailed knowledge of the technical environment and/or of the information being transmitted across the Intranet. Hence, both the threat and vulnerability are potentially greater than for external hacking.

3.2.3. Denial of service - interrupting and degrading computing services.

3.2.4. Technical failures leading to denial of service and/or loss of integrity of data in transmission at the time of failure.

3.2.5. Dissemination by internal users of sensitive information to unauthorised recipients.

3.3. Impact of Security Failures

The greatest impact would be caused by deliberate modification or destruction of SRAWEB information, which could result in:

3.3.1. the high cost of disruption resulting from the need to defer work, or use paper based means of reporting.

3.3.2. ineffectiveness in the criminal justice system as a result of failures to report offences

3.3.3. the adverse media interest which would be generated by these problems.

3.3.4. The impact of illegitimate disclosure of SRAWEB information could also be very high. Possible impacts include:

3.3.4.1. the whereabouts of individuals being traced e.g. witnesses, thereby jeopardising their personal safety;

3.3.4.2. apprehension of criminals being compromised if they were aware of being the subject of agency interest;

3.3.4.3. legal implications of breaching the Data Protection Act;

3.3.4.4. adverse media interest.

Accidental modification of SRAWEB information would have a lower impact than either of the foregoing. Although the consequent breach of security could be seen as similar to those of deliberate modification, the overall impact would be lower as there would be the intention and ability to correct the data.
4. Section 4 - Security Policy

4.1. Security Policy Statements

All Local Authority (LA) SRAs must confirm that they have completed and submitted a signed copy of the ISCJIS Information Security Policy Statement.

Local Authority IUs are responsible for maintaining their own Policy as defined in the ISCJIS Baseline Security Document.

Compliance with ISCJIS Baseline Security Document is subject to mandatory external audit on behalf of the ISCJIS Data Protection and Security Group (DPSG), which may consider disconnection of an LA system from the SRAWEB in severe cases of non-compliance.

Access to the SRAWEB by authorised users will be by the use of a valid unique User ID, password and digital certificate. Under no circumstances should these be shared.

All actions by a User ID/Certificate must be accountable to that User ID/Certificate.

The Integrity of data is of paramount importance to COPFS and this relates to the use of the SRAWEB. Agencies should strive to maintain the accuracy of the data submitted via SRAWEB process.

5. Section 5 - Administration Of Security

5.1. Introduction

This section defines who is responsible for maintaining this document and when, and under what circumstances, it should be reviewed.

5.2. Date of Expiry of this Document

The COPFS ITSO will maintain the scope, applicability and content of this document under review in the light of technological evolution of the system and changes in criminal justice environments.

This policy will be formally reviewed annually and in any event prior to the next significant change to the system, its management, or related policies if earlier.

5.3. Responsibility for SRAWEB Security

Responsibility for review and revision of this document rests with the COPFS ITSO, reporting to the COPFS Information Security Group.

5.4. Permitted Changes

Nationally Classified Information

The SRAWEB will not be used to store or process nationally classified information above ‘RESTRICTED’.

5.5. Accreditation
The authority for non-police agencies to connect to the SRAWEB will be determined by the COPFS Information Security Group. Local Authority accreditation will be performed by the ISCJIS Data Protection and Security Group.

6. Connection Rules

6.1. Introduction

6.1.1. This section defines security rules for the connection of computer systems in IUs to the central SRAWEB system. The rules apply to all methods of connection. The objectives of the rules are to safeguard:

6.1.1.1. The physical assets and security of the central SRAWEB
6.1.1.2. The security of data owned by all SRAWEB Information Users.

6.1.2. The rules are specified under the following headings:

6.1.2.1. Access Control
6.1.2.2. Authentication
6.1.2.3. Security Audit Logging and Monitoring
6.1.2.4. Data Integrity
6.1.2.5. Data Communications
6.1.2.6. Physical Protection
6.1.2.7. System Management
6.1.2.8. Business Continuity
6.1.2.9. Systems Development and Maintenance
6.1.2.10. Personnel
6.1.2.11. Security Incidents
6.1.2.12. Audit

6.2. Access Control

User Identities

6.2.1. The term user may be defined as a person, system or process. Authorised users must only be able to access the SRAWEB after supplying a valid user identity and password. The user identity must be unique to a single individual within the IU. Users are accountable for all actions performed with their user identity.

User identities must:

6.2.1.1. be deleted or disabled by COPFS as soon as the individual is no longer authorised to access the system;
6.2.1.2. never be re-allocated to a different user.

6.2.2. System management workstations and terminals must not be left logged on when not in use.

6.2.3. All user access devices (terminals, PCs, workstations) must, when connected to the SRAWEB be:

6.2.3.1. wherever possible, be disabled if there is no activity for a period of 30 minutes;
6.2.3.2. wherever possible be installed in offices which can be locked securely when unoccupied or failing this suitable safeguards are in place;
Access by Contractors & Other External Personnel

6.2.4. IU Systems through which access is made to the SRAWEB must be accessible only to staff who need access to the system for a legitimate business purpose.

Access to Transactions/Data

6.2.5. The access rights given to a user must

   6.2.5.1. be approved by a users line manager or senior officer and COPFS

   6.2.5.2. be the minimum required by the individual to perform his or her job effectively.

6.2.6. The capture of data from the SRAWEB onto removable disk storage is forbidden, unless expressly permitted by the Data Controller or his representative.

Handling of Printed Output

6.2.7. Printed output containing SRAWEB information must be:

   6.2.7.1. printed only within a secure area or when the printer is attended and the output is removed immediately;

   6.2.7.2. copy and page numbered in such a way as to indicate clearly if part of the document is missing;

   6.2.7.3. protected against inadvertent disclosure at all times, including when being sent by internal/external post

   6.2.7.4. disposed of by shredding or an approved alternative method.

6.2.8. The issue, transmission, storage and destruction of documents must be subject to formal procedures.

Handling of Media

6.2.9. A2.10 All SRAWEB data must be cleared from media prior to disposal or destruction. An approved technique, which obliterates the data, should be used; simple deletion might not sufficient.

6.2.10. The issue, transmission, storage and destruction of media should be subject to formal procedures.

6.3. Authentication

Information Users connected to the SRAWEB

6.3.1. All forms of authentication, whether they are passwords, machine-readable cards, authorisation codes or any other device, are unique to an individual and must not be shared with, or disclosed to, any other individual.

6.3.2. The user of a particular password, card, or other means of authentication is responsible for its safekeeping.

6.3.3. Authentication information held on IU systems must be protected against access by any unauthorised user.
6.3.4. Current policy is that the SRAWEB will authenticate users logging in

6.3.5. Every user identity must be protected by a password. For users of SRAWEB transactions, passwords must be at least eight characters long and changed at defined intervals not exceeding 30 days. Password must satisfy 3 of the following 4 criteria:

   6.3.5.1. At least 1 English lowercase character (a through to z)
   6.3.5.2. At least 1 English uppercase character (A through to Z)
   6.3.5.3. At least 1 numeral (0 through to 9)
   6.3.5.4. At least one non-alphanumeric character (character other than a-z, A-Z, 0-9)

6.3.6. Users are responsible for changing their passwords.

6.3.7. SRAWEB Workstations must not be sited in areas accessible to the public.

6.4. Data Integrity

6.4.1. Wherever possible, criminal record data created, modified or deleted on the SRAWEB system must be checked at the time of data entry to confirm that the data is accurate with respect to the source document and that the update is legitimate and authorised.

6.4.2. Updates to criminal records must be quality assured by sampling techniques using the information recorded about the transactions in system logs.

6.5. Data Communications

6.5.1. Where an IU shares a local network with other organisations that have no authority to access the SRAWEB, it is the responsibility of the IU to ensure that all other systems connected to the network do not breach the connection rules defined in the Information Security Policy.

6.6. A6 Physical Protection

6.6.1. IUs must ensure that, where practicable, during or in the aftermath of fire, water damage or other natural disaster, no unauthorised access to the SRAWEB system is possible;

6.7. Business Continuity

6.7.1. Maintaining an adequate SRAWEB service in the area served by an IU is the responsibility of the IU’s ITSO, who should ensure that adequate plans are made to recover from a local disaster.

6.8. Systems Development And Maintenance

Identification of Security Requirements

6.8.1. Under no circumstances should an IU undertake vulnerability/penetration testing on the SRAWEB application. Attempts at unauthorised access may constitute a criminal offence.

6.9. Personnel
6.9.1. Personnel authorised to have access to SRAWEB information must be vetted to Basic Check (BC) by the IU.

6.9.2. Any system authorisation must be revoked promptly when:
   6.9.2.1. a member of staff leaves;
   6.9.2.2. a member of staff transfers to a new post;
   6.9.2.3. a member of staff is suspended from duty;
   6.9.2.4. after an organisational restructuring or re-allocation of roles and responsibilities if the current authorisation is inappropriate to the new role.

6.10. Security Incidents

Definition

6.10.1. A security incident is any actual or suspected failure in SRAWEB information security including:
   6.10.1.1. accidental or deliberate destruction of information;
   6.10.1.2. accidental or deliberate modification of information;
   6.10.1.3. accidental or deliberate disclosure of information;
   6.10.1.4. deliberate and unauthorised unavailability of the SRAWEB system;
   6.10.1.5. unauthorised access to the SRAWEB system;
   6.10.1.6. misuse of SRAWEB data;
   6.10.1.7. theft of SRAWEB assets.

Reporting

6.10.2. Security incidents may come to notice in a variety of ways. Where breaches are not major and are discovered internally they should be reported to the IU Data Protection Officer and/or IU ITSO for action.

6.10.3. Serious security incidents and complaints from members of the public about security incidents must be reported to COPFS without delay. The COPFS ITSO must however be informed of all such incidents.

6.11. Audit

Introduction

6.11.1. The main audit log will be that of the SRAWEB at COPFS and audit functions will be performed by COPFS staff using that log.

Events to be logged

6.11.2. The events, which should be logged by IU’s for audit purposes, are:
   6.11.2.1. an attempted break-in to the SRAWEB;
   6.11.2.2. actual/suspected misuse of the SRAWEB
   6.11.2.3. changes in authorised SRAWEB users

6.11.3. The system records sufficient information to enable the individual user to be identified separately, along with an account of all transactions performed.

6.11.4. The identification of the originator is important in order to maintain accountability for the legitimate use of the SRAWEB system.