

**OFFICIAL  
OFFICIAL**

# **Working Together Agreement between the Scottish Environment Protection Agency and Police Service of Scotland**

## **Environmental Authorisations (Scotland) Regulations 2018 Radioactive Substances Activities**

### **What we want to achieve by working together on regulatory decisions**

- This agreement is between Scottish Environment Protection Agency (SEPA) and the Police Service of Scotland (Police Scotland), a constabulary established under the Police and Fire Reform (Scotland) Act 2012.
- Protection of people and the environment in relation to activities prescribed under the Environmental Authorisations (Scotland) Regulations 2018 (EASR), involving sealed radioactive sources, and an aggregate of sources, in categories 1 to 4, as defined by the International Atomic Energy Agency (IAEA) in Categorisation of Radioactive Sources (RS-G-1.9);
- Sharing of information on regulated activities, where it relates to the protective security of sealed radioactive sources in IAEA categories 1 to 4; A co-ordinated and consistent approach to the activities of SEPA and Police Scotland in relation to EASR;
- Avoid potential conflicting requirements while exploiting synergies to attain the appropriate level of protective security.

### **Roles and responsibilities (of each participating organisation)**

- SEPA is the regulator for EASR and has responsibility for the authorisation of radioactive substances activities;
- Under EASR (Schedule 8 paragraph 17) SEPA is required to consult the police on the security of premises where any activity involving sealed radioactive sources in IAEA Categories 1 to 4 is carried on. SEPA must consider any security advice or guidance it receives from the police in relation to such premises;
- Police Scotland is responsible for providing dedicated Counter Terrorism

**OFFICIAL  
OFFICIAL**

**OFFICIAL  
OFFICIAL**

Security Advisers (CTSA) to provide advice on reducing the vulnerability of businesses to terrorist threats. CTSA are trained, tasked and co-ordinated by the National Counter Terrorism Security Office (NaCTSO), a specialist police organisation that works in partnership with the Centre for the Protection of National Infrastructure (CPNI) to reduce the impact of terrorism in the United Kingdom and enhance the UK's resilience to terrorist attack;

- CTSA's are responsible for advising SEPA on the adequacy of protective security arrangements at sites applying for a permit for an activity involving the management of a sealed radioactive source in IAEA categories 1 to 4. The advice provided by a CTSA will be consistent with national guidance provided by NaCTSO. The authority given to CTSA for advising on protective security arrangements will come from the regulator, SEPA, through EASR.
- Once a permit has been granted, CTSA's will conduct annual inspections of premises to ensure that protective security arrangements remain adequate and report any non-compliance to SEPA so that appropriate enforcement action can be taken.

**How we will work together**

**SEPA and Police Scotland will:**

- Continue to build a structured interaction at all levels, including areas of strategy, work programming, and operational regulation;
- Exchange information and advice in a timely manner during the process of formal regulatory decision making;
- Make every effort to resolve differences on regulatory matters before any specific requirements are placed upon the operator of a regulated facility.

**SEPA will:**

- Consult with Police Scotland on applications for new permits involving the management of sealed radioactive sources in IAEA categories 1 to 4;
- Consult with Police Scotland on applications for variations to existing permits, involving the management of sealed radioactive sources in IAEA categories 1 to 4, if that variation will affect the security of the site;
- Consult with Police Scotland on applications for surrender of permits involving the management of sealed sources in IAEA categories 1 to 4;

**OFFICIAL  
OFFICIAL**

**OFFICIAL**  
**OFFICIAL**

- Send Police Scotland all relevant information from the application in a standard format agreed between SEPA, Police Scotland and NaCTSO within a period of 10 working days from the date that the application is duly made. Any documentation containing personal details will be processed and retained in compliance with the Data Protection Act, 2018, and General Data Protection Regulations (GDPR);
- Give consideration to any advice received from Police Scotland in the determination of the relevant application and in imposing any limitations or conditions;
- Identify Single Point of Contact (SPOC) for Policy and Operations to liaise with the Police Scotland regional points of contact;
- Notify Police Scotland of any information that might affect the security of sealed radioactive sources in IAEA categories 1 to 4 that SEPA becomes aware of in the course of its duties under EASR;
- In exceptional circumstances where CTSA's cannot conduct annual site visits SEPA will make contact with sites highlighting the process to follow should any security concerns arise.

**Police Scotland will:**

- Arrange for an inspection of any such premises using or containing an IAEA category 1-4 source by a CTSA;
- Provide advice on the adequacy of protective security arrangements, as per NaCTSO guidance, on a premises-specific basis;
- Provide a documented response after an inspection in a standard format agreed between SEPA, Police Scotland and NaCTSO (Appendix 1).
- Retain such records, which may contain personal information, in compliance with GDPR;
- Respond within a period of 30 working days (6 weeks) after the receipt of EASR application information from SEPA to allow SEPA to meet its statutory obligations (unless a longer period is agreed with the applicant).
- Where appropriate, and on behalf of SEPA, conduct an annual security review of all sites in their area to ensure that security standards are being maintained, providing the appropriate SEPA Inspectors a detailed summary of security provisions at each site. The purpose of this is to establish if there are any differences in site security year on year and ensure SEPA are aware of any emerging security issues;
- In exceptional circumstances, where CTSA's cannot conduct annual site visits in person, they will make contact with sites to ensure security

**OFFICIAL**  
**OFFICIAL**



**OFFICIAL  
OFFICIAL**

remains adequate and seek their reassurance that security provision remains unchanged or adequate for the sources being held ;

- CTSA to contact the appropriate SEPA Inspector where security non compliance issues arise that require regulatory intervention;
- Identify regional points of contact to liaise with the SEPA Policy and Operations SPOCs.

**Dispute Resolution**

Under the Environmental Authorisations (Scotland) Regulations 2018, SEPA as regulator, will have the final decision should any dispute arise.

**Review**

This Working Together Agreement will be reviewed every five years or where there is a significant change to legislation or procedures to be adopted within this time frame.

**Signed by:**



**Janice Milne  
Head of Function (Energy)  
Scottish Environment Protection Agency**


**02/12/20**

**Police Scotland**

**Appendix 1**

**OFFICIAL  
OFFICIAL**

 <b>POLICE SCOTLAND</b> <small>Keeping people safe</small> POILEAS ALBA	<b>CTSA SITE ASSESSMENT REVIEW</b>			<b>NaCTSO</b> <small>National Counter Terrorism Security Office</small>
	Name of Site			 <b>COUNTER TERRORISM POLICING</b>
Site Contact(s)				
Address	Telephone	Further Contact Details / E-mail address / Web site		
		http://www.		
	Mobile			
National Grid Reference (NGR)				
Northings / Eastings				
Brief description of the site and its function				
Sources / Substances held including quantities.				
Any other relevant information.				

 Scottish Environment Protection Agency Buidheann Dìon Àrainneachd na h-Alba	<b>SEPA – Information</b> (Forward to SEPA, by e mail, pages 2 onwards)	
	EAS / Reference Number	

**SECURITY – Complete where applicable**

Access Control Site / Building		
Specific Security (to include details relevant to sources or substances held)	Doors	
	Locks	
	Windows	
	CCTV	
	Alarm	
	Guarding	

**SECURITY MANAGEMENT**

<b>Personnel Security</b>	<b>HMG Baseline Personnel Security Standard (BPSS) – following are mandatory</b>		
	Right to work– Nationality and Immigration Status (including an entitlement to undertake the work in question)	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	Identity– ID Data check (electronic identity authentication- name, address, aliases, links, accounts, etc.)	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	Criminal Records– Search for unspent convictions only (Basic Disclosure)	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	Employment history check– Confirmation of past 3 years employment (minimum) history / activity	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	In addition, candidates are required to disclose any significant periods spent abroad (6 months or more in the past 3 years).		
	<b>There should be a holistic approach to Security / Management, therefore consideration must be given to the following:</b>		
	Ongoing personnel management	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	Challenge culture / tailgating	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	Post-employment procedures	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	Contractor / visitor screening / vetting	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>Details:</b>			

<b>Planning</b>	<b>SITE SECURITY PLAN (SSP) : All headers MUST be completed and the document, when completed, retained securely</b>
-----------------	---



**OFFICIAL  
OFFICIAL**

			Date	Completed
	SSP template forwarded to site? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
	<p><b>Note:</b> the Site Security Plan (SSP) contains details on:</p> <ul style="list-style-type: none"> <li>• Security of Information incidents</li> <li>• Reporting of Crime / Security preparation</li> </ul> <p><b>Consideration should be given in:</b></p> <ul style="list-style-type: none"> <li>• Bomb Procedures Plan</li> <li>• Search Plan</li> </ul>			
	<b>Details:</b>			
	Response to an increased threat? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
	<b>Details:</b>			
	Have you tested your Security Contingency Arrangements / Emergency Plans? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>		Date	
	How often are these Arrangements / Plans reviewed?		Date	
	NaCTSO Security Requirements Guidance provided to site? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>		Date	
	NaCTSO Version			
Site Survey	CT <input type="checkbox"/> Crime <input type="checkbox"/> N/A <input type="checkbox"/>			
Security Assessment	Green <input type="checkbox"/> Amber <input type="checkbox"/> Red <input type="checkbox"/>			
Date last reviewed				
CTSA offered products	ACT Suite of Products		Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
	SCaN Suites of Products		Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
	Bespoke CT input agreed relevant by CTSA / site		Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
	<b>Details:</b>			
CTSA Recommendations / Requirements & Updates			Date achieved / Progress update	





**OFFICIAL**

**OFFICIAL**

## **Partnership Agreements Information Assurance Authorisation Process**

In order that Information Assurance (IA) can gain confidence in Police Scotland (PS) Partnership Agreements being correctly authorised for use, we must ensure that all parties have had sight of, and agreed to, the documented terms, prior to publication to our Intranet.

Partnership Agreements take many forms, such as Information Sharing Agreement (ISAs), Memorandums of Understanding (MoUs), Service Level Agreements (SLAs) and the like. The following authorisation process applies to all, but may require slight variation, dependent on the agreement type.

1. **IA Administration:** When the Information Assurance Officer (IAO) is content that the agreement is ready for signature, the IAO logs this on the SharePoint Task Action Log, and inserts the appropriate date in the 'IA Authorised Field';
2. **IA Authorisation:** The IAO emails the PS Single Point of Contact (SPOC) advising that the agreement is ready for signature and the following requirements:
  - Any 'pre-signature' changes to the document version authorised by IA, such as date and signatory details **MUST** be embodied by the SPOC before presenting for signature...These changes will create the 'FINAL' document version;
3. **Signature:** Due to the current prevalence of homeworking, two options will be provided in respect of signatures:

**Option A:** The FINAL document version is to be saved and printed off by the authoring partner SPOC and presented for signature:

- Where PS are the document author, PS signs first;
- Where a Partner is the author, that partners signs first (this is simply protocol);
- The first signatory scans the signed FINAL document to PDF, then forwards this PDF to the next signatory by email **from their own mailbox** (NOT by anyone else on their behalf). The covering email should confirm the signatory's approval of the attached FINAL document;
- The second signatory prints the received PDF, signs it, then scans the signed copy to PDF and forwards to the next signatory;
- This continues until each signatory has signed and emailed confirmation, and the document is returned to the authoring partner's signatory/SPOC;

**Option B** Where there are no print/scan facilities available to the signatory, the

**OFFICIAL**

## OFFICIAL

signatory will forward the document being authorised by email to the next signatory **from their own mailbox** (NOT by anyone else on their behalf).

## OFFICIAL

Page 1 of 2

V1.0 – A1120

## OFFICIAL

- The covering email will include a statement expressly authorising the attached document (mentioned by actual title and version) (with wording along the lines of:  
  
‘I approve [insert document name & version] on the [insert date] on behalf of [insert organisation] which is attached to this email’.
  - The email **must** come from the personal mailbox of the authoriser and not be sent on their behalf. This is to permit a chain of authorisation to flow in the same manner as has been described in Option A.
  - The document will be passed from signatory to signatory, each adding their own authorising email, until it is finally returned to the authorising signatory or their SPOC.
4. **Distribution:** The authoring signatory/SPOC must now forward the scanned document (now having all partner signatures appended) for distribution to all partners. This may not be the most legible of documents at this stage, and must be accompanied by the MS Word ‘FINAL’ document for publication use. Confirmation emails should also be forwarded to all parties. Together these documents will represent our ‘electronic proofs’.
  5. **IA Registration:** The IAO receives the electronic proofs (as described above) from the authoring SPOC’s mailbox and registers the date of receipt in the ‘ISA Completed’ field on SharePoint;
  6. **IA Publication:** the IAO edits the ‘FINAL’ MSWord document to reflect the signatory details shown of the scanned PDF and creates a ‘clean copy’. The IAO saves this document as a PDF and publishes same to the Partnership Working Arrangements site (a template for the correct site field entries will be provided);
  7. **IA Notification:** the IAO notifies the PS SPOC that the agreement has been published and provides a hyperlink to the published document;
  8. **SPOC Operational Distribution:** The PS SPOC notifies Corporate Comms Channel Development (or their Divisional Site Manager) of the details required on their local/operational Intranet Page and provide the document link sent by IA.

## OFFICIAL

**OFFICIAL**

**OFFICIAL**  
Page 2 of 2

**V1.0 – A1120**

**OFFICIAL**



