

Security Declaration and Risk Assessment – Invitation to Tender

Please refer to the documents: “Security in the Supply Chain – Guidance Notes ref: Infsec-cont-001” and the [Document Classification Mini-Guides](#) for further information on the regulations and the Sellafield Ltd Process before completing this form.

It is a requirement of the security regulations for the nuclear industry, that all companies working on Government Protectively Marked Information (PMI) must protect that information in an appropriate way.

Government Protective Markings (i.e. RESTRICTED) may apply to contracts that are to be awarded by Sellafield Ltd, as well as the documentation that is released at the Invitation to Tender Stage.
(Sellafield Ltd documentation may also have a Commercial marking; this information is protected in similar way).

Sellafield Ltd is responsible for ensuring that all contractors working on Sellafield Ltd contracts that carry a Government Protective Marking can meet the required security standards to protect the information they are given. The ‘Need to Know Principle’ is key:

All Government PMI and Sellafield Ltd COMMERCIAL information should be treated with the ‘Need to Know Principle’– it should only be able to be accessed by those people who NEED to see the information to carry out their work.

As such, companies* wishing to tender for Sellafield Ltd contracts are required to complete and return this Security Declaration Form and provide a copy of their security policy and procedures.

*As this includes sub-contractors, consortium members etc, you are requested to forward a copy of this Declaration form and supporting documents listed above to each company as you decide to involve them for each tender or after the placement of contract.

Completing the Declaration and Risk Assessment

The Declaration should be completed by a Company Director or by an appointed Security Controller/Security Contact. If your company does not already have a Security Controller/Contact then you must appoint the duty of Security Liaison to an appropriate member of your staff.

- **Part 1 – Company Details.** To be completed for every Tender. A separate form is required for each separate location.
- **Part 2 – Company Security Requirements.** To be completed once every 12 months other than the exceptions listed below under the ‘What Happens Next’ section. It should be supported by a copy of your Security Policy and Security Instructions.
- **Part 3 – Declaration.** This declaration is stating that the company, at this location, can secure the “hard copy” documents to the minimum required level and can enforce the “Need to know” principle.
- **Part 4 – IT Risk.** If the contract will involve the electronic processing or storage of PMI or Sellafield Ltd Commercial information electronically, please also complete the IT Risk Assessment in Section 4 (if not, please mark the box at the start of section 4 only).

The Declaration and Risk Assessment can be completed manually or electronically.

To complete on the computer, please type your answers into the highlighted fields (or click Yes/No boxes) and print off to sign the declaration.

Returning the Declaration and Risk Assessment

The Declaration and supporting documentation shall be return to Sellafield Ltd via CTM by the due date and time. Late submissions will not be considered. Supporting information that cannot be emailed should be posted to the address overleaf.

If completing this process as a potential sub-contractor you must ask the company, tendering as the prime contractor to submit your Declaration and supporting information via their CTM submission.

GENERAL NOTES:

- The Invitation to Tender documentation will not be protectively marked higher than RESTRICTED. The documents marked RESTRICTED will only be issued in hard-copy (paper) format only.
- The documents marked COMMERCIAL may be issued electronically (via CTM system).
- You should not be required to create any PMI documentation as part of the Invitation to Tender. (Guidance on how to avoid creating PMI will be issued separately in a Security Aspects Letter relating to the scope of the tender)

What happens next?

Once you have submitted a Declaration and supporting information, it will be subject to review by Sellafield Ltd Security Department. If you are deemed to meet the required standard for receiving the Protectively Marked documentation, you will be issued with a formal Tender Authorisation Certificate (TAC). This certificate can be referenced in future tender submissions to avoid repeating the full process each time.

Once Sellafield Ltd have authorised your company at the declared location, this will last for 12 months. It is superseded only by:

- ❖ The completion of another Declaration once the 12 month period lapses
- ❖ The completion of another Declaration upon changes that effect security being made to this location
- ❖ The issue of a Certificate of Approval (issued after a Security Assessment of the premises/location if the contract is awarded to you)

A Security Aspects Letter (SAL) will be issued by Sellafield for your signature before any PMI can be issued to your company as part of the invitation to tender. This is to acknowledge that you fully understand the reason for protective markings and how to keep that type of information secure.

You will be responsible for issuing a SAL to all sub-contractors for their signature prior to any PMI being forwarded to them. A copy of all SALs must be sent to Sellafield Ltd (Contract Security). As previously stated, all locations must be approved prior to receiving PMI.

If you are awarded a contract involving PMI, you will be subjected to a full security assessment at this location before the contract can commence. If you have already been assessed by Sellafield Ltd and the assessment Certificate of Approval is still valid then it may be that no further assessment is required. Sellafield Ltd Security Department will confirm requirements at that time.

What happens if we do not meet the requirements at Tender Stage?

If the declared location does not meet the minimum requirements, the Sellafield Ltd Security Department will be able to advise any measures that you must put into place to enable you to meet the correct standard. Once all recommended actions have been completed, you will go through the assessment process again to check the requirements have been met, and formal notification will be issued as per the process above.

Our Contact Details

If you have any queries about this process that are not covered in the guidance documents, or you would like to provide any feedback, please contact the Contract Security Team, details below:

Sellafield enquiries: 019467 79605 or 019467 71534

Risley enquiries: 01925 832054

Email: contract.security@sellafieldsites.com

Contract Security
B113
Sellafield Ltd
Seascale
Cumbria
CA20 1PG

If you are completing this for a particular Invitation to Tender, please provide the CTM system reference number. RFQ:

If you are not completing this for a particular Invitation to Tender, but for general RESTRICTED hard-copy approval, please mark this box: (In these cases submissions should be by email to *contract.security@sellafieldsites.com*)

1. COMPANY DETAILS

Company Name								
Registration Number								
Registered Head Office Address								
Location at which the tender and contract will be carried out (full address. One location per form ONLY)								
Has this location been approved for processing Government PMI above Restricted level, and to what level?	Hard Copy (paper)				Electronic			
	NO <input type="checkbox"/>	CONFIDENTIAL <input type="checkbox"/>	SECRET <input type="checkbox"/>	TOP SECRET <input type="checkbox"/>	NO <input type="checkbox"/>	CONFIDENTIAL <input type="checkbox"/>	SECRET <input type="checkbox"/>	TOP SECRET <input type="checkbox"/>
Approving authority:								
Security Contact Details								

a) Have you (the company) been subject of a security assessment at this location before (and been issued with a Certificate of Approval by Sellafield Security Department)?	Y <input type="checkbox"/>	N <input type="checkbox"/>
If Yes, please provide the certificate number, then go to question c. (If you have been assessed but not received a certificate please contact the Security Department for advice)	PSEC/	
b) Have you (the company) had a Tender Authorisation Certificate issued at this location before?	Y <input type="checkbox"/>	N <input type="checkbox"/>
If Yes, please provide the certificate number, then answer question c.	TAC/	
c) If you have answered Yes to either a) or b), have there been any changes made to this location that may affect the security since your last declaration or security assessment?	Y <input type="checkbox"/>	N <input type="checkbox"/>
If Yes, please provide details separately and then sign the Declaration. (Please refer to the Security in the Supply Chain guidance note for criteria) If No, please go to Question 3 to sign the declaration.		

2. COMPANY SECURITY REQUIREMENTS
Policies and Procedures

In order to meet the required security level for receiving hard-copy RESTRICTED or COMMERCIAL information, your company must employ the use of an up to date Security Policy and Security Procedures. You must submit a copy of Security Policy & relevant Procedures to Sellafield Ltd along with the Declaration before you may be approved for receiving the PMI.

The Policy must cover: Personnel Security, Physical Security, Information and IT Security. It is advised that your company works at a minimum to the principles of ISO27001 for information security if no full accreditation of your information security systems has been granted. The Procedures should detail the use of lockable office furniture or security furniture to protect sensitive information and assets, controls to keys for that furniture (ie: only those personnel who need to access the information/assets should have access to those keys), access control to rooms/offices/areas that house the lockable cabinets, security of offices overnight or out-of-hours.

Personnel

For access to COMMERCIAL and RESTRICTED information, a robust check of a person's identity is required. This may be done by way of checking valid official identification documentation, for example, a full UK passport and/or Photographic Driving licence (both parts). No formal security clearance is required, but the Need to Know Principle should be applied at all times.

Does your company have an auditable system for ID and employment checks?	Y <input type="checkbox"/>	N <input type="checkbox"/>
--	----------------------------	----------------------------

3. SECURITY DECLARATION

Section 79 Anti-terrorism Crime and Security Act 2001:

Section 79 of the Anti-terrorism Crime and Security Act 2001 prohibits the disclosure of any information or thing which might prejudice the security of a nuclear site or nuclear material, whether intentionally or recklessly.

Accordingly, anyone who holds information that might, if disclosed, prejudice the security of the Sellafield, Windscale or Capenhurst nuclear sites, any other nuclear site or any nuclear material, must ensure that it is appropriately secured.

Sellafield Limited ensures its compliance with section 79 of the Anti-terrorism Crime and Security Act 2001 by applying the "need to know" principle and by putting in place:

- Up to date Security Policy
- Security Procedures detailing the use of lockable office furniture or security furniture to protect sensitive information and assets, controls to keys for that furniture (ie: only those personnel who need to access the information/assets should have access to those keys), access control to rooms/offices/areas that house the lockable cabinets, security of offices overnight or out-of-hours.
- Enforcement of those procedures
- Promoting Security Awareness across the workforce

Commercial marking:

Sellafield Limited Invitations to Tender and contract documentation may also be marked as "Commercial" indicating that it contains commercially sensitive information disclosure of which would, for example, prejudice NDA, SL or the UK's economic interests or would breach a duty of confidentiality, or is otherwise prohibited or would be harmful to an important public interest.

As representative in security matters for the company named, I confirm that the information declared is current and correct at the date of signature.

By signing this document, I am confirming that:; (company name), at the declared location, will undertake appropriate controls to secure any Protectively Marked Information (PMI) and/or Sellafield Ltd COMMERCIAL information issued to us and Sellafield Ltd COMMERCIAL information that may be produced by us.

- We will only store documentation/information issued to us at the location declared on this form.
- We will not produce PMI as part of our tender submission.
- We understand the Anti-Terrorism, Crime and Security Act 2001 as outlined above and will disseminate this to all personnel with access to PMI and COMMERCIAL information issued to us by Sellafield Ltd.
- We will provide Sellafield Ltd with a copy of our security policy and procedures*.
- We will return, or confirm in writing the destruction of any PMI or COMMERCIAL documentation to Sellafield Ltd at the close of Invitation to Tender, or at contract completion should we be awarded a contract.
- We will not release any PMI to third-parties/sub-contractors based at other locations without prior permission of Sellafield Ltd. If permission is received, we will issue a Security Aspects Letter to all sub-contractors and supply copies of these to Sellafield Ltd Contract Security Team.
- We are aware that Sellafield Ltd and the Office for Civil Nuclear Security have the right to assess our premises at any time during the tender (and subsequent contract should it be awarded to us)

Failure to comply with the terms of this declaration may result in the named company not being considered for future sensitive Sellafield Ltd contracts.

Please note that should this declaration be approved by Sellafield Ltd that it is applicable only to physical security measures used to protect Sellafield Ltd information, and does not in any way give authorisation to produce or process PMI electronically as part of the tender submission, nor as part of the contract should it be awarded to you.

Signed:	
Name: (BLOCK CAPS)	
Appointment:	
Date:	

*If you have already submitted the Policy and relevant Procedures as part of a previous Declaration submission and been issued with a TAC, **and no changes have been made to either of the documents**, then you do not need to re-submit them.

4. IT SECURITY RISK ASSESSMENT

This information is gathered for use in an IT Security Risk Assessment prior to placement of contract. It forms no part of the above declaration, and as such NO PMI should be produced by the company as part of the Tender package – this includes using computers to access information on removable media such as CD, DVD, USB sticks etc.

This form should be completed in relation to the location the contract will be processed, that you have declared in Section 1.

COMPANY NAME:
If there is no requirement for your company to electronically process PMI, please mark this box: <input type="checkbox"/>

How many people will potentially have access to the information?		
How many people will be working on the information?		
Does your company at this location have a network or IT system that is Accredited to process Government Protectively Marked Information by a Regulator or Contracting Authority that can be used for this contract? (if Yes, please provide evidence)	Y <input type="checkbox"/>	N <input type="checkbox"/>
Is your company ISO27001:2005 accredited? (Information Security Management Standard) (if Yes, please provide evidence, no requirement to complete the IT Security Questionnaire) (if No, please complete the IT Security Questionnaire in full. ISO27001 principles are the minimum level required for processing Sellafield Ltd COMMERCIAL information)	Y <input type="checkbox"/>	N <input type="checkbox"/>

a. Security Management		
i. Does your company have an endorsed IT Security Policy?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ii. Does your company have a nominated/appointed IT Manager?	Y <input type="checkbox"/>	N <input type="checkbox"/>
iii. Are audits/assessments carried out on your IT system? (either internal or external)	Y <input type="checkbox"/>	N <input type="checkbox"/>
iv. Is your IT support and/or maintenance provided by a third party?	Y <input type="checkbox"/>	N <input type="checkbox"/>
v. Does your Company have an Anti-Virus process?	Y <input type="checkbox"/>	N <input type="checkbox"/>
vi. Does your Company have a Back-up process?	Y <input type="checkbox"/>	N <input type="checkbox"/>
vii. Is exchangeable media which may need to be re-used within your company overwritten using an authorised software package?	Y <input type="checkbox"/>	N <input type="checkbox"/>
viii. Does your Company have an information exchange policy (i.e. exchange of information via email)?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ix. Does your company provide security awareness, education and training to employees and contractors?	Y <input type="checkbox"/>	N <input type="checkbox"/>
b. Access Control		
i. Does your Company implement Access Control management (i.e. user access rights, access to applications etc)?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ii. Does your Company implement Password management?	Y <input type="checkbox"/>	N <input type="checkbox"/>
iii. Is your Company network connected to the internet?	Y <input type="checkbox"/>	N <input type="checkbox"/>
iv. Does your company have a firewall installed?	Y <input type="checkbox"/>	N <input type="checkbox"/>
c. Network security		
i. Is your Company network distributed across the UK?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ii. Will the network or IT System processing the information be connected to any other 3rd party network?	Y <input type="checkbox"/>	N <input type="checkbox"/>

iii. Will the information relevant to this contract be processed on your Company network?	Y <input type="checkbox"/>	N <input type="checkbox"/>
iv. Will the information relevant to this contract be processed on a standalone IT System (i.e. not connected the internet)?	Y <input type="checkbox"/>	N <input type="checkbox"/>
v. Does your company have a network connection into the Sellafield Ltd network?	Y <input type="checkbox"/>	N <input type="checkbox"/>
vi. Do you use wireless for processing information within your company?	Y <input type="checkbox"/>	N <input type="checkbox"/>
d. Media Management		
i. Does your Company implement exchangeable media management (i.e. removal, transfer, disposal, storage, document marking and labelling of media)?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ii. Do you have a formally Disposal process for your IT equipment and Exchangeable media?	Y <input type="checkbox"/>	N <input type="checkbox"/>
iii. Does your company encrypt removable media and laptops? If so, what encryption software is used?	Y <input type="checkbox"/>	N <input type="checkbox"/>
e. Mobile Computing		
i. Will laptops be used for the processing of Sellafield Ltd information as part of the contract?	Y <input type="checkbox"/>	N <input type="checkbox"/>
f. Change Control		
i. Does your Company have formal IT change control procedures?	Y <input type="checkbox"/>	N <input type="checkbox"/>
g. Security Incident Management		
i. Does your Company perform auditing and monitoring (event logging) across your network or IT system?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ii. Are information security events/incidents monitored and reported?	Y <input type="checkbox"/>	N <input type="checkbox"/>
h. Disaster Recovery		
i. Does your Company implement Disaster Recovery?	Y <input type="checkbox"/>	N <input type="checkbox"/>
ii. Are your back-ups stored at a different location from the location processed?	Y <input type="checkbox"/>	N <input type="checkbox"/>
i. Compliance		
i. Does your Company comply with all statutory, regulatory and contractual obligations (i.e. Data Protection Act, Computer Misuse Act etc.)?	Y <input type="checkbox"/>	N <input type="checkbox"/>

Signed:	
Name: (BLOCK CAPS)	
Appointment:	
Date:	