Rolls-Royce Plc
Supplier Security Handbook

This Security handbook provides information and guidance to safeguard the required contractual process and ensure the appropriate protective security controls are in place for the protection of assets against compromise.

01

Contractual Requirements

1.1 Security Aspects Letters (SALs)

Where work is to be carried out on the contractor's premises, we must clearly define to you, the contractor, what is defined in the condition as sensitive material associated with the contract. This must be done in the form of a Security Aspects Letter (SAL). The SAL flows down requirements from the MoD to Defence primes on how to manage and handle information in accordance with the current Government Security Classifications (GSC) guidance and other caveated information (NNPPI, PSA, ITAR etc.). For flow down of contracts at OFFICIAL-SENSITIVE, or above, to a subcontractor a SAL is required to be issued as well as the Security Conditions.

It is important that all employees connected with the planning and implementation of the security aspects fully understand the SAL and its implications. Where issues are unclear, or it imposes unacceptable or impracticable obligations on the contract, you should be encouraged to seek immediate clarification from the Rolls-Royce Security Controller. No data or assets are to be shared with the contractor until the aspects of the SAL have been accepted. Acceptance of a SAL is to be completed using the 'SAL response & assurance form'.

An example of Security requirements detailed in a SAL:

Table 1	
Scope of Work	
Highest Classification	E.g. Up to and including OFFICIAL-SENSITIVE
Personnel Security Clearance Required	A minimum of BPSS is required for access to OFFICIAL-SENSITIVE/ ·A minimum of SC is required for access to SECRET Sole UK Nationality required for access to UK EYES ONLY

1.2 Scope of Work

This details a high-level summary of the work to be undertaken and should reflect what information is to be shared. Please ensure that you are content with the summary.

The scope and Government Security Classified information that is referenced in the Security Aspects Letter should not be hosted or accessible from outside of the U.K. by any entity within your organisation or subcontracted element (e.g., outsourced I.T. service provider) without prior approval from Rolls-Royce Plc who will seek approval from the MoD.

The classification of information will be documented as the highest level of information that you will process, but you may also receive other information at a different classification which must be handled appropriately, this could also include caveated information e.g. UK Eyes Only

1.3 Information Release Approval Process

Please be aware that in order to be able to release any information publicly, you must first seek authorisation in writing from Rolls-Royce Plc by contacting the UK Defence Security Team: DefenceSecurityUK@Rolls-Royce.com

The result of your request will be communicated back to you as soon as possible.
In addition to this – Please note that we will not authorise the publication of any information which includes the following:

- A relationship with your business and Rolls-Royce Plc
- The scope of work you are completing on our behalf

The above information which is classified at OFFICIAL-SENSITIVE due to the sensitivity of the contracts you could be working on.

1.4 Government Security Classifications

His Majesty's Government has stated that all information needed to conduct government business services or programmes has intrinsic value and requires an appropriate degree of protection.

Security classifications indicate the sensitivity of information (in terms of the likely impact resulting in compromise, loss or misuse) and the need to defend against a broad profile of applicable threats.

There are three levels of classification: Official, Secret and Top Secret.

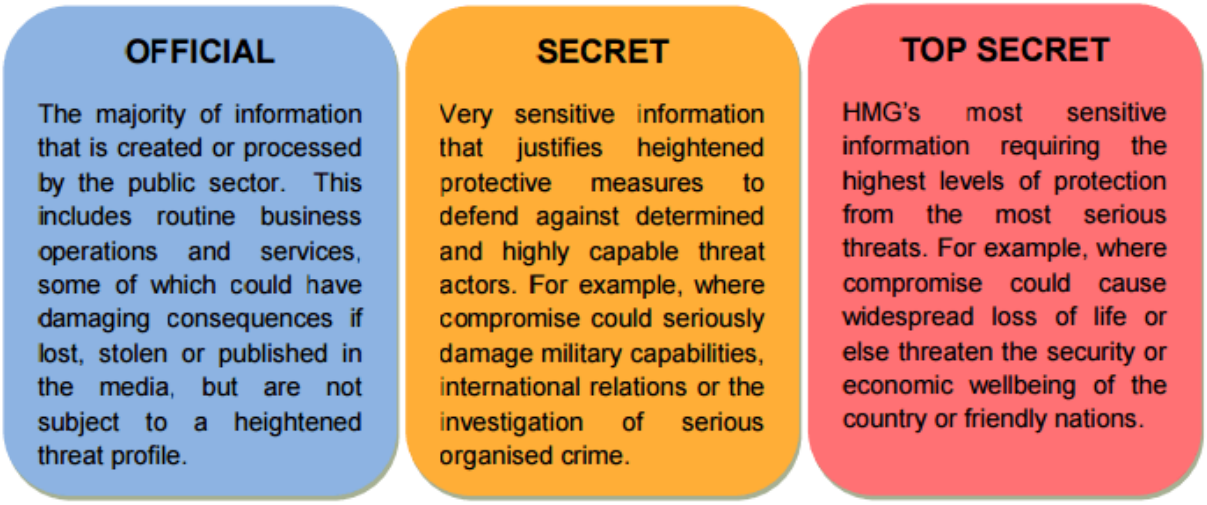
Further information can be found at:
https://www.gov.uk/government/publications/government-security-classifications

OFFICIAL information may have the handling caveat of SENSITIVE applied, which is then marked on documentation as OFFICIAL-SENSITIVE

OFFICIAL-SENSITIVE enforces the “Need to Know” principle – There are additional security controls necessary for this sub-set of information due to the sensitive nature. Nobody should access this information unless they have a genuine "Need to know" and are authorised.

A “UK” prefix is mandatory for overseas transmission of OFFICIAL-SENSITIVE information

Documentation Security Classified OFFICIAL-SENSITIVE does not have to be recorded in a Classified Document Register – but it must be kept under lock and key.



1.5 Subcontracting Requirements

For flow down of contracts at OFFICIAL-SENSITIVE to a subcontractor a SAL is required, a template is located within the cabinet office guidance Appendix 4 page 37 within Contractual Process.

All sub-contracted work must include and comply with the requirements of the SAL and the Security Classification of the work being carried out. A copy of each SAL which is issued to you in support of the scope of work must be sent to the company Security Controller via your Supply Chain point of contact.

For Non U.K. contracting a valid F1686 approval form signed by the MoD is required to be in place prior to contract placement and information release. Detailed information can be found within the cabinet office guidance Appendix 5 page 38 within the Contractual Process guidance which can be found here:
https://www.gov.uk/government/publications/contractual-process-personal-or-classified-data.

Consideration MUST be taken into account for additional sub-tiers of the supply chain. RR must be informed of any sub-contracted activities so that we are aware of what is being undertaken and by whom. Before entering into any discussions or placing sub-contracts for work, RR must be consulted.

02

Personnel Security

2.1 Screening and Vetting

The purpose of personnel security controls, such as pre-employment screening or national security vetting is to confirm the identity of individuals, employees and contractors, and provide a level of assurance as to their integrity and reliability. Whilst personnel security controls cannot provide guarantees, they are sensible precautions that provide for the identity of individuals to be properly established. In circumstances where risk assessments indicate that the necessary thresholds are met, they provide for checks to be made of official and other data sources that can indicate whether individuals may be susceptible to influence or pressure which might cause them to abuse their position or whether there are any other reasons why individuals should not have access to sensitive assets.

Baseline Personnel Security Standard (BPSS) is the minimum level of clearance required for all contracts which personnel handle OFFICIAL-SENSITIVE classified information.

Organisations are responsible for carrying out BPSS checks for their own employees. BPSS comprises verification of the following four main checks:

- Right to work – verification of nationality and immigration status;
- Identity check – verification of ID documentation i.e. passport;
- Criminal records – self declared and search for 'unspent' convictions (Basic Disclosure);
- Employment check – confirmation of 3 years (min.) employment history

Information collected at each stage of the process must be reviewed and assessed, and recorded on a BPSS Validation Record.

A copy of this record can be found in the Government guidance:
www.gov.uk/government/publications/government-baseline-personnel-security-standard

2.2 National Security Vetting (NSV)

NSV provides a level of assurance as to an individual's integrity and reliability to allow access to government classified data and assets at risk from a wide range of threats. These threats include terrorism, espionage, or other actions that could threaten the UK. NSV is delivered by the United Kingdom Vetting Service (UKSV), which is part of the Cabinet Office Government Security Group and the Government Security Function.

Levels of NSV:

There are 4 main levels of national security clearance:

- Accreditation Check/Level 1A (AC/L1A)
- Counter Terrorist Check/ Level 1B(CTC/L1B)
- Security Check (SC)
- Developed Vetting (DV)

SC & DV clearances are the most commonly applied within the Defence industry.

SC allows access up to and including data & assets classified at Secret, with occasional supervised access to Top Secret.

DV allows frequent uncontrolled access data & assets classified at Top Secret.

Should the contract that you are working on require NSV for your employees this will be specified within the Security Aspects Letter sent to you. Please refer directly to your Rolls-Royce UK Defence Security Team:
DefenceSecurityUK@Rolls-Royce.com

Further guidance on NSV can be found here:
https://www.gov.uk/government/organisations/united-kingdom-security-vetting

03

Physical & Procedural Security

3.1 Physical Security

Effective physical security of an asset is achieved through multi-layering of different mitigation measures, which is commonly referred to as ‘defence-in-depth’. The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single security layer. Each layer of security may be comprised of different elements, including for example:

- Access control and locking systems - Access control systems and locks are about controlling who can go where and when. These systems integrate with physical barriers to provide delay and detection against a multitude of attackers.
- Physical and active barriers to deny or delay the progress of adversaries. - The perimeter of a site is one of the key locations where physical security measures and controls can be applied to protect both users and facilities. Without proper thought, the perimeter can become a significant vulnerability.
- Measures to protect sensitive (e.g. classified) material or assets
- Command and control
- The response to an incident
- Security personnel (covered within the Personnel and People Security)

The above measures are interdependent and their effectiveness will be dictated by their ability to support one another.

Everyone with senior executive or Board level responsibility needs to have concise strategic information to guide their decision-making, risk management and governance activities. This is particularly important for the effective management of security at organisational level.

NPSA's PASSPORT TO GOOD SECURITY for Senior Executives sets out the key themes for best practice and provides relevant prompts for the actions you need to take as part of your strategy. It will help you to identify, assess and mitigate the threats to your organisation. Further guidance can be found here:
https://www.npsa.gov.uk/managing-my-asset/leadership-in-security/board-security-passport

3.2 Business Continuity

Additional security controls may impact current Business Continuity Plans (BCP), resilience against various unforeseen disruptions and continuity of operations and services. Regular BCP testing helps in identifying risks, preparing for emergencies, and improving recovery time.

ISO 22301:2019 Security and resilience; Business continuity management systems provides a framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.

3.3 Secure Destruction

Everyone has a responsibility to ensure that sensitive information and assets, whatever their form, are appropriately protected from the moment they are created until their verified destruction. Once there is no longer a need for the information or asset it must be destroyed in accordance with record retention requirements defined within the main contract.

What are the threats to the destruction process?

There are many potential threats to the destruction process. These can occur before, during or after the destruction process. These threats include:

- Accidental loss
- Emergency abandonment
- Espionage
- Insider attack
- Theft

Once the nature of the threat is understood, businesses should take a methodical and considered approach to determine the most appropriate and proportionate destruction procedures.

NPSA supports a programme certifying secure destruction service providers. As a minimum, confirm that secure destruction services have been subject to an independent assessment by a reputable organisation. Please refer to the NPSA website for additional guidance found here:
https://www.npsa.gov.uk/secure-destruction-0

3.4 Shipping of Assets

A Local Standard Operating Procedure (SOP) is required to be in place to outline how the movement of classified assets at a domestic level should be undertaken. The SOP aligns to client specific requirements whilst utilising the existing company process, contracts and shipping team

This can be be adopted to ensure that assets to be moved domestically are done so in an appropriate and complaint manner and that all aspects of the movements are auditable

All personnel have a responsibility to ensure that the assets which they have access to are always maintained with integrity and confidentiality and in the event of any concern arising they should report this to their line management immediately

There are many potential threats to the transportation process including:

- Opportunist theft
- Emergency abandonment
- Hijack or vehicle theft
- Insider attack
- Espionage

Once the nature of the threat is understood, practitioners should take a methodical and considered approach to determine the most appropriate and proportionate transportation procedures.

If overseas travel will occur, the Foreign & Commonwealth Office (FCO) provides advice for travelling abroad and specific country guides.

04

Cyber Security

4.1 Cyber Security

The MoD's vision is to work with Industry to build a cyber resilient defence to ensure that Defence can continue to deliver its purpose and support the national effort strengthening the UK in the cyber domain and cement its authority as a democratic and responsible cyber power.

The full Cyber Resilience Defence Strategy can be found here:
https://www.gov.uk/government/publications/cyber-resilience-strategy-for-defence

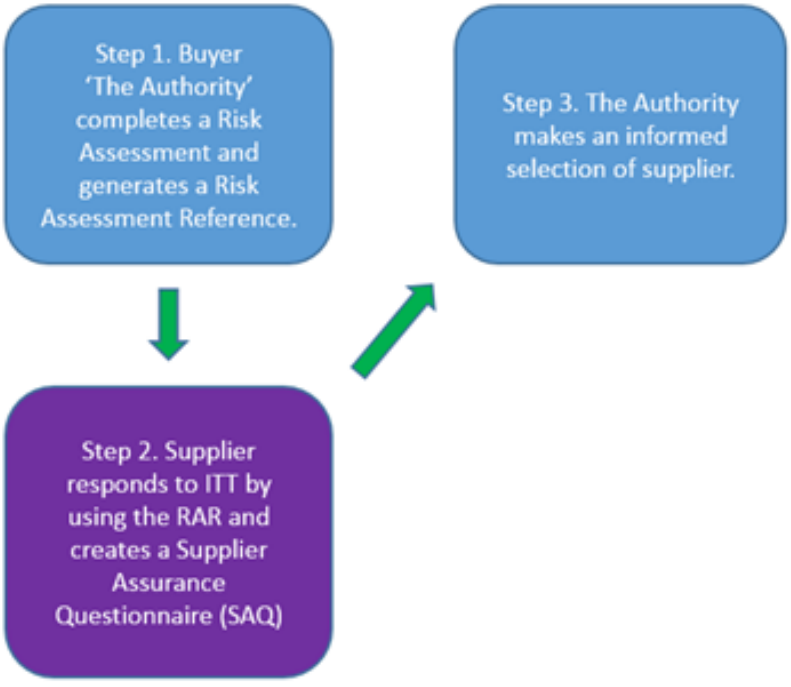
4.2 Defence Cyber Protection Partnership

The Defence Cyber Protection Partnership (DCPP) is a joint MoD / Industry initiative formed as part of the Defence Suppliers' Forum's directive to improve the protection of the defence supply chain from the cyber threat.

The DCPP acts in support of the UK's National Security Strategy and the National Cyber Security Strategy, which reaffirms the cyber threat as a Tier One risk to UK interests.

The Cyber Security Model is a risk-based, proportionate approach to protecting MoD information as it moves through, or is generated in, the supply chain.

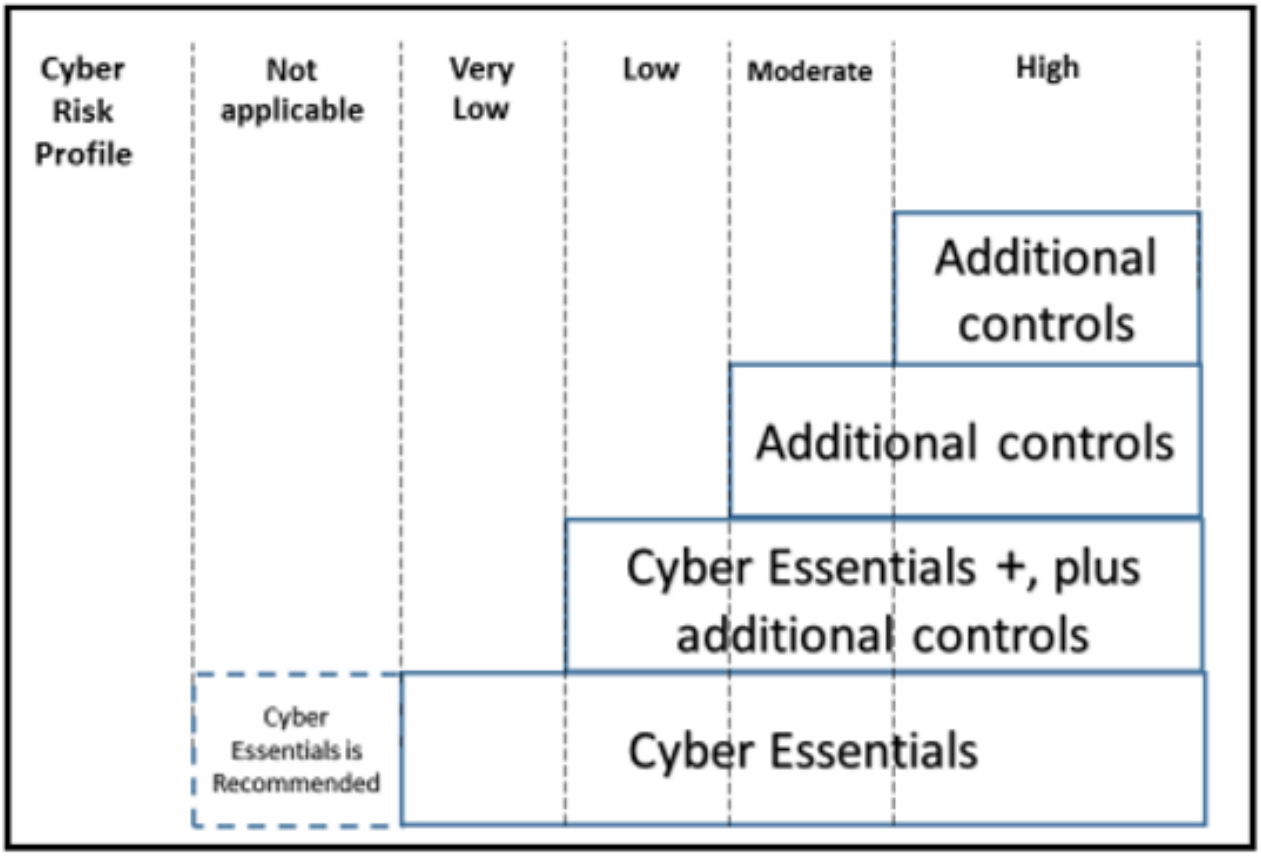
Defence Standards (DefStan) defines the MOD requirements in respect of the Cyber Security Model (CSM). The CSM starts with a Risk Assessment. This generates a Cyber Risk Profile and creates a Supplier Assurance Questionnaire (SAQ). The Authority makes an informed selection of supplier.



There are five outcomes from the Risk Assessment process.

Not Applicable, Very Low, Low, Moderate and High.

There is no specific correlation between the Risk Assessment outcome and the Government Security Classification Scheme although contracts involving Secret and Top-Secret information would be expected to carry a moderate or high level of cyber risk.



The full Defence Cyber Protection guide can be found here:
https://www.gov.uk/guidance/defence-cyber-protection-partnership

4.3 Cyber Essentials

The Government is taking steps to further reduce the levels of cyber security risk in its supply chain through the Cyber Essentials scheme. The scheme defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

There are 2 levels of certification:

- Cyber Essentials
- Cyber Essentials Plus

Cyber Essentials is for all organisations of all sizes, and in all sectors. The MoD have made the scheme mandatory for central government contracts advertised after 1st October 2014 which involve handling personal information and providing certain ICT products and services.

If a supplier is unable to achieve full compliance with the control measures associated with the relevant Risk Profile, a Cyber Implementation Plan (CIP) can be produced to demonstrate steps towards compliance. The CIP should detail what actions the supplier intends to take to put the control measures in place and should also clearly state dates for completion of each action.

The CIP may also be used where a contractor believes they have equivalent control measures in place. For example, Cyber Essentials Scheme is a British scheme so an overseas contractor may have accreditation from their national body.

Another reason that a contractor may produce a CIP would be if a sub-contractor is unable to comply with the control measures.

The CIP must be reviewed to determine whether the risk of not having the controls in place at contract start and the mitigations in the CIP are acceptable for the specific requirement. The CIP must be agreed before the contract start date and the level of approval depends on the Risk Profile. Although not responsible for accepting risk, your Major Business Unit, or Front-Line Command Senior Information Risk Owner, should also be informed of the acceptance of a CIP if the Risk Profile is Very Low, Low or Moderate.

The CIP process applies down the supply chain and at 'Very Low' and 'Low' the Higher Tier supplier can accept the CIP of their sub-contractor, although the Authority must still be notified. Any CIPs against a risk level of 'Moderate' or 'High' must be agreed by the MOD even down the supply chain.

Further Cyber Essentials information can be found here:
https://www.ncsc.gov.uk/cyberessentials/overview

Consectetur adipisici elit, sed eiusmod tempor incidunt ut labore etdolore magna aliqua. Excepteur sint obcaecat cupiditat non proident culpa. Plura mihi bona sunt, inclinet,amari petere vellent. Inmensae subtilitatis, obscuris et malesuada fames. Pellentesque habitant morbi tristiquesenectus et netus. Nihil hic munitissimus habendi senatus locus, nihil horum? At nos hinc posthac, sitientispiros Afros. Idque Caesaris facere voluntate liceret: sese habere. Nihilne te nocturnum praesidium Palati,nihil urbis vigiliae. Ambitioni dedisse scripsisse iudicaretur. Vivamus sagittis lacus vel augue laoreetrutrum faucibus. Lorem ipsum dolor sit amet.