Managing personnel security risks

Guidance to suppliers for meeting Rolls-Royce standards

Suppliers who manage employees or contractors with access to Rolls-Royce data need to keep that data protected, and operate in a manner consistent with Rolls-Royce personnel policies and procedures. This document provides specific guidance and resource information to suppliers to help mitigate the security risks involved in overseeing your workforce, while complying with Rolls-Royce standards.

All members of the Rolls-Royce supply chain have a role to play in keeping the company, its data, and customers safe. While these guidelines may seem demanding and potentially expensive to incorporate, they are mostly common sense steps you can follow without added costs. Thank you for doing your part.

Why these policies matter

Personnel security policies and procedures are important because they:

- Reduce the risk of recruiting staff who are likely to create a security concern
- Decrease the likelihood of existing employees becoming a concern
- Strengthen the protection of data assets
- Create standards for carrying out investigations to resolve suspicions and provide evidence for disciplinary procedures
- Support the implementation of security measures proportionate to risk

Rolls-Royce requires a personnel risk-reduction program

Rolls-Royce requires its suppliers to have an active workplace threat program to minimize employee-related risks. These requirements align with industry best practices (Reducing Insider Risk | NPSA, Defining Insider Threats | CISA) and comply with Rolls-Royce's Minimum Cyber Security Standard (MCSS). The minimum standard for compliance includes:

- Completing background checks on employees and contractors who have access to Rolls-Royce data assets or its IT systems.
- Having processes for new or departing employees/contractors, including managing their access to Rolls-Royce data and/or IT systems (i.e., applying least privileged principle). This also means ensuring employees/contractors return data or equipment and/or revoking access to systems when no longer required, or leaving employment.
- Delivering security training and ensuring employees/contractors maintain awareness of risks to Rolls-Royce data assets and/or IT systems.
- Ensuring employees/contractors know how to report breaches and incidents, and explaining how to follow procedures governing regulations and legal requirements (e.g., export controls, IP and/or government classified data).

Guidance on background checks

Suppliers must follow the same baseline standard Rolls-Royce uses to assess the potential risk posed by employees who have access to company IT systems or data. This **Baseline Personnel Security Standard** (BPSS) is a UK-based standard but is easily employed by companies worldwide. BPSS is used as a tool to prevent or deter a wide variety of insider attacks. Compliance with BPSS means you have confidence in the trustworthiness of your employees/contractors (i.e., those who have access to Rolls-Royce data assets and/or IT systems).

Personnel risk assessments can help you to identify employees/contractors who must undergo BPSS checks by determining the level of risk they pose to Rolls-Royce data assets and/or IT systems. You should maintain records of roles and responsibilities within your organization that are required to undertake BPSS checks — specifically those who have access to Rolls-Royce data assets and/or IT systems.

Your personnel risk assessment will guide you by ensuring you have implemented proportional and efficient personnel security, and only perform checks on employees/contractors who pose a risk to Rolls-Royce data assets and IT systems.

Important! Suppliers whose employees have access to defense data may require further checks. In the UK, the National Protective Security Authority (NPSA) provides further guidance: **Reducing Insider Risk | NPSA** and **https://www.npsa.gov.uk/resources/personnel-security-risk-assessment-guide-4th-edition**. In the U.S, the US Cybersecurity and Infrastructure Security Agency (CISA) provides guidance on **Insider Threat Mitigation**

Use this security checklist to vet your workforce

To maintain confidence that your employees/contractors are honest and have integrity, please assure that the checks outlined below are performed in a timely manner and you are completely satisfied with the information provided. Any inconsistencies or discrepancies should be verified to allow accidental errors to be corrected.

Identity — confirm an identity matches the information someone has provided (e.g., in an employment application or contractor profile)

- Verify identity documents have been issued by a government department/office.
- Photographs or identifying information should be compared with physical appearance.
- Confirm name, date of birth and address. Signatures should also be checked against other relevant documentation (e.g., other identity documents, a witnessed signature).

Nationality & Immigration status — confirm nationality and right to work in country where the role is located

- Check documentation verifying right to work (e.g., documents such as passports, verifying nationality and/or visas and immigration status).

Employment and Education History, including Professional Qualifications — verify employment and education history for past 3 years; verify any professional qualifications

- You may need employee/contractor's prior written permission to contact previous employers for references. Other commercial or professional services may provide evidence (e.g., from government agencies, financial institutions, attorneys, trade, or client references, etc.).
- If relevant to the role, verify professional qualification certificates. Many organizations offer online certification verification services (e.g., Institute of Accountants and Bookkeepers (iab.org.uk), Chartered Institute of IT Certificate Checker (bcs.org), etc.).
- Look for gaps in employment/education history of more than 12 weeks. Ask for additional information to check other events or circumstances occurring within that period.

Financial Checks — determine if someone is subject to any adverse financial circumstances

- Financial checks should only be performed if someone's role justifies an inquiry into their financial situation (e.g., financial roles, or roles include budget or asset management).
- Checks may be performed using information requested from the employee/contractor (i.e., self-declaration). The assessment should determine if employee/contractor financial circumstances could have a potential impact on their role (i.e., their access to company and customer assets). This means that employees/contractors could be more susceptible to being coerced or duped into causing harm to Rolls-Royce data assets and/or IT systems, for financial reward.

Criminal history checks (where law permits) — reveal any active criminal convictions held by the employee/contractor (including driving offences and convictions)

- Criminal history checks should be assessed on a case-by-case basis.
- Where it is not possible to perform checks or verify information provided (e.g., person lived or worked overseas) a proportional risk assessment approach should be taken, and/or consider alternative courses of action (e.g., Criminal records checks for overseas applicants (www.gov.uk)

A list of potential concerns

Several factors may separately or in combination raise concerns. In each case, you should consider personnel security risks before making an offer of employment or providing access to Rolls-Royce data assets or IT systems. These factors include:

- any involvement in illegal activities
- making false or unsubstantiated claims on a resume or application form
- unsubstantiated professional qualifications
- unexplained gaps in employment history
- receiving bad or false references
- questionable documentation (e.g., a lack of supporting paperwork or concern that documents are not genuine)
- evasiveness or unwillingness to participate and/or provide sufficient information

Managing personnel security risks

Personal data security

Personal information is very sensitive and must always be collected, handled, and stored securely, in accordance with your company security and privacy policies and laws. Access should only be provided to those with a genuine need-to-know.

If you are performing pre-employment checks and you reject a person's application, it is important to be clear about the reasons for rejection. Comprehensive records of decisions and the actions taken will be important if the individual is seeking feedback.

Data retention policies

Personal information collected for the purposes of BPSS checks must be retained or destroyed in accordance with your retention policies. Criminal conviction information must be destroyed, unless in exceptional circumstances the information is clearly relevant to the role and ongoing employment requirements (e.g., driving offenses).

Supporting information (e.g., copies of letters for proof of address) should be destroyed within 6 months.

NOTE FOR UK-BASED BUSINESSES

If you are UK-based, here are several links for further guidance:

- To confirm identities of new hires or contracts: **Home Office Guidance on examining identity documents** and **Guidance on examining identity documents (accessible) (www.gov.uk)**
- To confirm nationality, immigration status and right to work: **Performing basic passport checks (www.gov.uk)** and **Employers' right to work checklist (www.gov.uk)**

Additional note: There are several references in this document for suggested UK sources to seek out to provide guidance or information. For companies in other countries, we encourage you to find local sources to help you fulfill supplier requirements.

ANY QUESTIONS?

Please contact your Buyer or Business Point of Contact.

Reporting personnel security incident? Please contact your Rolls-Royce Buyer or Business Point of Contact.

Employment record-keeping and further monitoring

Maintain an employee human resources record to demonstrate information was verified and sufficient to confirm BPSS checks, and when they were completed. In some circumstances recheck is required (e.g., visa expiration) or after a long period of absence (e.g., re-employ contractor).

Create a culture in which security is important and accepted. Your managers and employees should discuss concerns and problems confidentially and informally, in particular:

- Ill health in the individual or family
- Financial difficulty
- Peer, family, or extended group pressure
- Perceptions of unfairness at work

The following observed behaviors require your immediate attention:

- Drug or alcohol abuse
- Expressions of support for extremist views, actions, or incidents, particularly when violence is advocated
- Major unexplained changes in lifestyle or expenditure
- Sudden loss of interest in work or overreaction or prolonged response to career changes or disappointments
- Unusual interest in security measures, or areas of work outside the normal remit
- Signs of stress, such as excessively emotional behaviors
- Changes in working patterns (e.g., frequently working alone or at unusual hours, and reluctance to take holidays)
- Frequent unexplained absences
- Repeated failure to follow recognised procedures
- Unusual travel abroad
- Relationships with or support for individuals or institutions that are generally regarded as professionally suspect or substandard
- Sudden or marked change of religious, political, or social affiliation or practice that has an adverse impact on the individual's performance of their job or attitude to security

You should have processes that provide appropriate data protection safeguards and restrict access based on concerns raised about an employee or contractor's behaviors. Information should only be shared with those who have a true need to know.