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 an overview to suppliers about how to mitigate workforce security risks according to Rolls-Royce standards. To see a full description of Rolls-Royce's standards for managing personnel risks, please click here.

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 and provide evidence for disciplinary procedures
- Support the implementation of proportional security measures

Common-sense approach: While these guidelines may seem demanding and potentially expensive to incorporate, they are mostly common sense steps you can follow without added costs.

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:

- Background checks on employees and contractors who have access to Rolls-Royce data or IT systems
- Processes for managing access to Rolls-Royce data and/or IT systems
- Protocol for ensuring employees/contractors return data or equipment when no longer required, or leaving employment
- Rules for reporting breaches and following government regulations
- Data security training

Managing personnel security risks

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. Compliance with BPSS means you have confidence in the trustworthiness of your employees/contractors.

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.

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 checklist to vet your workforce

To maintain confidence that your employees/contractors are honest and have integrity, perform the checks outlined below in a timely manner. Make certain you are completely satisfied with the information provided. Inconsistencies or discrepancies should be verified to correct accidental errors.

- **Identity:** Confirm the identity matches the information provided.
- **Nationality & Immigration status:** Confirm nationality and right to work in country where the role is located.
- **Employment and Education History:** Verify employment and education history for the past 3 years. Look for gaps in employment/education history of more than 12 weeks.
- **Financial Checks:** Determine if someone is subject to any adverse financial circumstances (if role justifies).
- **Criminal history checks (where law permits):** Criminal history checks should be assessed on a case-by-case basis.

A culture of security

It's important to create a culture in which security is important and accepted. Your managers and employees should discuss concerns and problems confidentially and informally. Some potential warning signs require immediate attention. These include:

- 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
- Unusual interest in security measures
- Signs of stress
- Changes in working patterns
- Repeated failure to follow recognised procedures
- Unusual travel abroad
- 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

Be aware of potential concerns

Several factors may separately or in combination raise concerns about employees or contractors. 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 or making false or unsubstantiated claims on a resume or application.

FOR MORE INFORMATION | Reminder: This document is a summary. Please see the fuller set of guidelines here. If you have any questions, please contact your Buyer or Business Point of Contact.