Rolls-Royce Supplier Baseline Cyber Security Standard

The purpose of this document is to specify the appropriate cyber security requirements Rolls-Royce requires its suppliers to implement, to protect the confidentiality, integrity and availability of Rolls-Royce Data.

Rolls-Royce Data is defined as any data provided to the supplier during the contract, including but not limited to; Proprietary Information, Technical Data, Intellectual Property, Personal Data, Export Controlled or Third Party Data, which may not without prior consent of Rolls-Royce be used or reproduced, in whole or in part, or communicated to any person not employed by Rolls-Royce.

Supplier will comply and procure the compliance of their employees, officers, directors, contractors, sub-contractors or other representatives of the supplier with the following minimum-security measures, which may be subject to change:

1. access to Rolls-Royce Data is provisioned on a least-privilege basis and restricted to only those who require access for the specific purposes of the exercise of the supplier's rights and the performance of its obligations under its contract(s) with Rolls-Royce;
2. do not store Rolls-Royce Data on any personal devices or personal removable media;
3. all portable devices including, laptops, tablets, phones, removable media, or any other portable computing devices that hold or have access to Rolls-Royce Data, are encrypted with commercial grade encryption;
4. any Data exchanged between Rolls-Royce and the supplier is transmitted securely via a Rolls-Royce approved mechanism suitable for the classification of the information (e.g., ForumPass);
5. all systems processing Rolls-Royce Data enforce a password policy that meets accepted good practice standards;
6. Rolls-Royce Data is not left unattended (clear desk and clear screen) and devices processing Rolls-Royce Data are locked immediately when not in use;
7. upon becoming aware of, or reasonably suspecting, an information security incident involving Rolls-Royce Data, the supplier shall notify Rolls-Royce (UK.SOC@rolls-royce.com) as soon as possible and no later than 48 hours from the time of initial discovery;
8. demonstrate, implement and maintain proactive defence measures against potential cyber-attacks, including, but not limited to:
    - applying a patch management procedure, ensuring all devices and services on their estate(s) are up-to-date;
    - installing industry standard hardware and software to protect and secure systems processing and/or storing Rolls-Royce Data, to include amongst others firewalls, anti-virus and malware protection software;
    - conducting independent annual penetration tests of external/internet facing services and applications; and
    - individuals with access to Rolls-Royce Data are trained on the requirements of this Standard and relevant internal security policies, and be aware of cyber security risks including how to identify security breaches, information security risks, and any regulation governing Export Control, Intellectual Property and Government classified data, that is stored, handled and processed by the supplier;
9. individuals with access to Rolls-Royce Data must be vetted and undergo security checks to ensure they are cleared to UK Government Baseline Protective Security Standard (BPSS) as a minimum or in-country equivalent checks;
10. maintain and implement appropriate onboarding and offboarding processes that involve revoking permissions upon the departure of an individual who has access to Rolls-Royce Data and the return of equipment to Rolls-Royce when no longer needed;

11. on termination or expiry of any agreement and/or contract with Rolls-Royce cease use of the Rolls-Royce Data and unless otherwise stated by Rolls-Royce or required by any legislative/regulatory requirement, permanently delete all Rolls-Royce Data in its possession and/or control so that no Rolls-Royce Data is recoverable once deleted;
12. security policies covering devices processing Rolls-Royce Data shall be assigned to an appropriately qualified owner, who oversees that they are maintained, monitored and reviewed on an annual basis, to ensure that they are adhered to and remain effective and updated and revised as necessary;
13. Access to certain Rolls-Royce IT Systems may require the provisioning of Rolls-Royce IT System access accounts. The third-party organisation must become a Third Party Approved entity via successfully passing the Third-Party Clearance Screening Process, before the provisioning of Rolls-Royce access accounts can be expedited;