Rolls-Royce Supplier Enhanced 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.

Where suppliers can demonstrate current certification to one (or more) of the following national Defence cyber security standards, and the certification scope covers the Rolls-Royce contractual scope, suppliers are not required to demonstrate compliance against the requirements detailed in this document:

- NIST 800-171
- CMMC Level 2 or higher
- Defence Standard 05-138 'Very Low' profile or higher

The supplier shall maintain certification to the national Defence cyber security standard throughout its contractual period(s) with Rolls-Royce.

In the event of a conflict, inconsistencies shall be resolved by giving precedence in the following order:

- In-country laws and regulations
- Contractual obligations as agreed to with Rolls-Royce
- This Standard

Rolls-Royce Data is defined as any data provided to the supplier during the contract(s), including but not limited to: Confidential 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 improperly.

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. Policy

1.1. 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.

2. Personnel Security

2.1. 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;

2.2. individuals with access to Rolls-Royce Data related to Defence products or services must undergo additional vetting procedures and maintain compliance with relevant Export Control obligations (e.g., permitted user nationality and location of access) as identified by Rolls-Royce;

2.3. 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;

2.4. 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.

3. Asset Management

3.1. implement, record and manage the scope and secure configuration of devices, laptops, servers and workstations that holds or has access to Rolls-Royce Data (including but not limited to, disabling unnecessary services, un-installing software no longer required/supported, disabling auto-run and maintaining inventories and baseline configurations);

3.2. do not store Rolls-Royce Data on any personal devices or personal removable media;

3.3. all portable devices including laptops, tablets, phones, removable media, or any other portable computing device that holds or has access to Rolls-Royce Data must be encrypted with commercial grade encryption;

3.4. 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.

4. **Access Control**

4.1. access to Rolls-Royce Data is via the supplier's corporate local area network (LAN) or Remote Access via a managed access control point using virtual private network technology with multi-factor authentication;

4.2. 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;

4.3. manage the standard-user and administrative account creation, modification, provision and withdrawal of access rights relating to systems holding or processing Rolls-Royce Data;

4.4. all access to Rolls-Royce Data is controlled by means of individual secure system logon identities and passwords;

4.5. passwords used to access systems that hold or process Rolls-Royce Data:

a) require use of upper and lower case alphabetic, numeric and special characters;
b) contain a minimum of 8 characters for standard user accounts;
c) contain a minimum of 15 characters for administrative accounts;
d) are not stored or transmitted in clear text on or over the network;

4.6. systems that hold or have access to Rolls-Royce Data shall limit the number of unsuccessful log-in attempts;

4.7. default passwords of systems that hold or have access to Rolls-Royce Data must be changed;

4.8. administrative accounts shall not be used for high-risk or day-to-day user activities, for example web browsing and email.

4.9. 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);

4.10. Rolls-Royce Data is not left unattended (e.g., clear desk and clear screen) and devices processing Rolls-Royce Data are locked immediately when not in use;

5. Physical Facilities

5.1. maintain physical security and access controls which meet industry best practice and are appropriate and proportionate for the protection of Rolls-Royce Data;

6. Operations Security

6.1. deploy and centrally manage end-point protection software on all systems that are connected to or capable of connecting to the Internet;

6.2. anti-virus software is updated for all systems in line with industry best practice and in accordance with advice from the applicable anti-virus software vendor;

6.3. deploy boundary protection on the boundary of the internal network(s);

6.4. appropriate patch management procedures are in place and centrally managed to remain current with platform security fixes, and to ensure adequate testing of these patches is carried out;

6.5. track, review (including security impact assessments), approve, or disapprove, and log changes to systems that holds or has access to Rolls-Royce Data;

6.6. maintain and regularly review logs which record account administration, user activities, faults and information security events, whilst ensuring that system clocks are synchronised to a single referenced time source

6.7. provide security controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

7. Communications

7.1. use encrypted sessions for the management of network devices;

7.2. implement as a minimum an industry standard encryption solution when transmitting or electronically accessing Rolls-Royce Data via a communications network (minimum Transport Layer Security v1.2 protocol or equivalent Virtual Private Network technology);

7.3. install and operate its wireless network connections in an appropriately secure manner (e.g., WPA2 encryption, complex administrative password and 802.1x authentication);

8. Incident Management

If the supplier discovers or is notified of any incident or reasonably suspected incident relating to the use of systems holding or processing Rolls-Royce Data, the supplier will:

8.1. notify the Rolls-Royce Security Operations Centre (UK.SOC@rolls-royce.com) within 48 hours of becoming aware of, or reasonably suspecting, an information security incident;

8.2. promptly take all reasonable steps necessary to contain the incident, mitigate the impact and prevent its reoccurrence, and shall notify Rolls-Royce of the remedial steps taken;

9. Disaster Recovery and Backup

9.1. disaster recovery plan and a backup solution are implemented, reviewed and tested to mitigate the risk of potential loss and/or compromise of Rolls-Royce Data;

10. Vulnerability Assessment

10.1. undertake a vulnerability assessment of systems holding or processing Rolls-Royce Data at least annually using industry standard tools, techniques and methodologies;

10.2. categorise and remediate in accordance with the supplier's security policy and a copy of the report shall be provided to Rolls-Royce upon request;

10.3. appoint an independent third party, to conduct a security penetration test of external/internet facing systems holding or processing Rolls-Royce Data at least annually and following any major technology systems or infrastructure change by the supplier;

10.4. provide a copy of the security penetration test results to Rolls-Royce upon request;

10.5. undertake and record regular security risk assessments of systems and components used to deliver the services to Rolls-Royce. Risks and mitigating actions shall be recorded in a risk register, stored in a securely controlled location;

11. Compliance and Audit

11.1. promptly respond to Rolls-Royce requests for information about compliance with this Standard;

The following requirements are only applicable where a supplier is developing Software on behalf of Rolls-Royce.

12. Software Development

12.1. adopt a software development lifecycle model that incorporates secure coding standards, including separation of access between non-production and production environments, segregation of duties, cryptographic controls, protections against malicious code and a peer review process;

12.2. maintain due diligence in reviewing source code for flaws, bugs or security issues that may impact integrity, availability or confidentiality of Rolls-Royce Data in the production environment;

12.3. take all reasonable steps to ensure that no unauthorised person is allowed physical or electronic access to any code created under the services agreed in the contract(s) with Rolls-Royce, regardless of the stage of development.