Rolls-Royce Supplier Minimum Cyber Security Standard

The purpose of this Rolls-Royce Supplier Minimum Cyber Security Standard is to set out the minimum security measures that Rolls-Royce's suppliers and/or its third parties ("**Supplier**") must implement and maintain during the provision of any services and/or goods to Rolls-Royce (as applicable), the latest version of which can be found at Rolls-Royce's website for suppliers (https://suppliers.rolls-royce.com).

- **Section A: Data, Systems and Resiliency**
  - protection of Rolls-Royce and its customer's data (i.e., confidentiality, integrity, and availability)
  - managing access to IT systems, and
  - ensuring resiliency in response to cyber threats.
- Section B: Cloud Security
- Section C: Connected devices
- Section D: Secure Software Development
- Section E: Offshoring data, systems, and services
- **Section F: AI Security**

The Supplier shall agree with Rolls-Royce those sections or specific measures of this Rolls-Royce Supplier Minimum Cyber Security Standard that do not apply to the provision of goods and/or services (as applicable) by them to Rolls-Royce.

Government Flow Down: Rolls-Royce has customers including governmental or other public bodies which may require, pursuant to their agreements and arrangements with Rolls-Royce and/or an Affiliate(s) of Rolls-Royce that Rolls-Royce and/or an Affiliate of Rolls-Royce (as applicable) comply with certain terms which may include compliance by a supplier to Rolls-Royce and/or an Affiliate of Rolls-Royce to such terms ("**Government Terms**"). If a Supplier is required to comply with any Government Terms, it shall do so in addition to those requirements contained herein.

Certification: Where a Supplier can present a valid certification/attestation to one (or more) of the following information and cyber security standards, and the scope covers the contractual requirements agreed in their agreements with Rolls-Royce, such Suppliers shall be deemed to comply with this Rolls-Royce Supplier Minimum Cyber Security Standard:

- NIST 800-171
- CMMC Level 2 or higher
- Defence Standard 05-138 'Very Low' profile or higher
- ISO/IEC 27001
- ISO/IEC 42001: 2023
- Cyber Essentials/Cyber Essentials Plus; and/or
- Other industry specific standards (e.g., IEC 62443)

If at any point during the term of its agreement with Rolls-Royce a Supplier ceases to hold a certification or attestation listed above the requirements contained in this Rolls-Royce Supplier Minimum Cyber Security Standard shall immediately apply to the provision of goods and/or services from such Supplier to Rolls-Royce.

In the event of any conflict or inconsistencies between provisions, the order of precedence shall be as follows:

- any Government Terms;
- local country laws and regulations;
- the terms and conditions of the relevant agreement between the Supplier and Rolls-Royce; and
- the terms of this Rolls-Royce Supplier Minimum Cyber Security Standard.

© 2025 Rolls-Royce
This information is provided by Rolls-Royce in good faith based upon the latest information available to it; no warranty or representation is given; no contractual or other binding commitment is implied.

Not Subject to Export Control

For the purposes of this Rolls-Royce Supplier Minimum Cyber Security Standard the following terms shall have the following meanings:

"**Cyber Security Incident**" means an adverse event or chain of events in or affecting an electronic information system that constitutes actual harm or the attempt to harm, including any events that compromises the confidentiality, integrity or availability of any confidential or sensitive business information to include a policy violation(s) of the system's security policy, unauthorised access attempts or usage, or changes made without the owner's (of the electronic information system or business information (as applicable)) knowledge, instruction or consent; and

"**Rolls-Royce Data**" shall be construed in its broadest sense and shall include any data, in any format or medium, provided to or accessed by a Supplier including but not limited to any information relating to Rolls-Royce, its Affiliates, its customers and/or any third party, confidential information, technical data, intellectual property, personal data and/or export controlled data, which shall not, without the prior consent of Rolls-Royce, be used or reproduced, in whole or in part, or miscommunicated.

"**Configuration Management Policy**" means a description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems, to ensure all assets are documented with their known configuration, interdependencies and relationships so that change management, impact analysis, and compliance activities can be executed.

Section A: Data, Systems and Resiliency

The scope of this section of the Rolls-Royce Supplier Minimum Cyber Security Standard covers:

- protection of Rolls-Royce and Rolls-Royce's customers' data (i.e., confidentiality, integrity, and availability);
- managing access to IT systems; and
- ensuring resiliency in response to cyber threats.

Rolls-Royce is committed to protecting the information it processes or stores according to its value, sensitivity, and the risks to which it is exposed, and in a manner consistent with Rolls-Royce's relevant legal, regulatory and contractual requirements. It is vital that all users of Rolls-Royce Data have a clear understanding of what is expected of them. This section sets out the information security controls and requirements required from Suppliers to protect Rolls-Royce and its customers' data from unauthorised access, theft and/or destruction and to ensure appropriate data protection in information systems, prevent common cyber-attacks, and assist the business recover in the event of a Cyber Security Incident.

1. The Supplier shall ensure:

   1.1 in relation to policy:

      (a) organisational leadership invests in a positive security culture. Security is considered and included from the outset, and given sufficient importance for protecting development, build and production environments;

      (b) security policies covering protection of Rolls-Royce Data, devices and physical/logical access to Rolls-Royce Data stored and processed on Supplier IT systems, shall be assigned to an appropriately qualified owner, who oversees that they are kept up to date, maintained, monitored, and reviewed at least on an annual basis, and to ensure they are communicated, adhered to, and remain effective at managing cyber risks to their systems and Rolls-Royce Data; and

      (c) their employees and contractors with authorised access to Rolls-Royce Data and IT systems comply with Rolls-Royce's current security policies;

   1.2 in relation to personnel security:

      (a) their employees and contractors with authorised access to Rolls-Royce Data and/or IT systems must be vetted and undergo security checks and aftercare to ensure they are cleared to UK Government Baseline Protective Security Standard (BPSS) as a minimum or in-country equivalent checks;

(b) if relevant, their employees and contractors with authorised access to Rolls-Royce Data and/or IT systems related to Rolls-Royce's Defence business' products and/or privileged access to services, must undergo additional vetting procedures and they shall comply with relevant Export Control obligations (e.g., permitted user nationality and location of access);

(c) onboarding and offboarding processes (i.e., Joiners, Movers and Leavers) manage risks of employees and contractors with access to Data and IT systems. Access or user permissions must be revoked when no longer required or upon the departure of an individual from the Supplier's employment and ensure any Rolls-Royce Data and equipment is returned when no longer required;

(d) their employees and contractors receive training and awareness that promotes and values positive contributions to security and that they have access to the necessary skills and security expertise to support them in their role; and

(e) their employees and contractors with access to Rolls-Royce Data and/or IT systems are trained on relevant security policies. Supplier shall ensure all staff are aware of cyber security risks to Rolls-Royce Data and IT systems and their responsibilities, including how to identify and report security breaches, handle information securely and follow regulation/legislation governing location, export control, intellectual property and Government classified data that is stored, handled, and processed by the Supplier;

1.3 in relation to asset management:

(a) Configuration Management Policy maintains an inventory and secure configuration of software and hardware devices that stores, processes, or manages access to Rolls-Royce Data or IT systems including but not limited to, procedures for disabling unnecessary services, un-installing software no longer required/supported, disabling auto-run, introduction, and removal of components to/from systems, etc.;

(b) Rolls-Royce Data shall not be stored, processed, or accessed on any personal devices or personal removable media;

(c) all portable devices including laptops, tablets, phones, removable media, or any other portable computing device that stores or manages access to Rolls-Royce Data shall be encrypted with commercial-grade encryption;

(d) any data exchanged between Rolls-Royce and the Supplier shall be transmitted securely, using a Rolls-Royce approved mechanism suitable for the classification of the information (e.g., ForumPass);

(e) maintains an asset inventory for Rolls-Royce Data stored, processed, and managed by the Supplier IT systems and any regulation/legislations that apply;

(f) Rolls-Royce Data is not left unattended (e.g., clear desk and clear screen) and user devices used to access or store Rolls-Royce Data are physically secured when not in use, with authentication access tokens secured in a separate storage location; and

(g) on termination or expiry of any agreement and/or contract with Rolls-Royce, cease use of the Rolls-Royce Data and unless stated by Rolls-Royce, or required by any legislative/regulatory requirement, permanently delete or destroy (so that it is no longer retrievable) all copies of Rolls-Royce Data;

1.4 in relation to identity and access control:

(a) authorised Supplier employees and contractors use a corporate-controlled and managed device to remotely access Rolls-Royce Data stored on the Rolls-Royce IT system. Least privileged access is granted by Rolls-Royce for authorised individuals, with a legitimate business purpose. Suppliers and/or third parties shall review or audit user accounts of employees and contractors regularly, and when no longer required (e.g., user changes role or leaves the organisation) shall notify Rolls-Royce immediately;

(b) access to Rolls-Royce Data on Supplier IT systems is provisioned on a least-privilege basis and restricted to such Supplier employees and contractors requiring access for the specific purposes of performing the Supplier's obligations under its agreements with Rolls-Royce. Suppliers shall maintain control of user accounts and access privileges, and remove or disable accounts or privileges when no longer required;

(c) maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Rolls-Royce Data. Safeguards shall include, but will not be limited to, measures designed to prevent unauthorised access to or disclosure of Rolls-Royce Data;

(d) Supplier IT systems use industry best practices for identity and authentication controls (e.g., username and passwords, multi-factor authentication (MFA) hardware/software token or 'one-time' passcode, passwords not stored or transmitted in clear text over insecure networks, etc.) and employees and contractors receive training on creating good passwords and protecting system access credentials;

(e) Supplier IT systems storing, processing, or managing access to Rolls-Royce Data shall limit the number of unsuccessful log-in attempts; and

(f) administrative user accounts of Supplier IT systems should be used for system administration and management purposes only;

1.5 in relation to physical facilities:

(a) maintain industry best practice physical security and access controls, processes, and procedures for locations where Supplier operates its business and stores and processes Rolls-Royce Data;

(b) monitor and regularly review the effectiveness of physical access controls protecting Supplier's facilities and systems storing and processing Rolls-Royce Data; and

(c) approve sites from where Supplier employees and contractors access Rolls-Royce IT systems, details of the site, location, protection mechanisms, controls and processes must be maintained in a Rolls-Royce Architecture and Information Assurance (AIA) document.

1.6 in relation to system security:

(a) Supplier IT systems are designed to identify and mitigate threats through:

(i) end-point protection software on all devices and servers that are connected to or capable of connecting to the Internet;

(ii) boundary protection (e.g., application firewalls or firewall services) for web services and internal network(s);

(iii) changing system or software default vendor-supplied passwords;

(iv) keeping software and hardware up to date, following industry best practices, and patching critical vulnerabilities within 14 days of release;

(v) logging user and privileged access and activities, exceptions, faults, and information security events covering IT Systems used by the Supplier in the performance of its obligations under the relevant agreement with Rolls-Royce. Logs should be kept secure and regularly reviewed, and any anomalies investigated and reported to the Rolls-Royce Security Operations Centre (see Section 1.7); and

(vi) system clocks are synchronised to a single referenced time source;

(b) firewalls and routers on the edge of the Supplier's IT systems are managed from inside the network not from the Internet;

(c) unnecessary software (including applications, system utilities and network services) are removed or disabled;

Not Subject to Export Control

(d) changes to Supplier IT systems and services are assessed and improved with mitigations against new and evolving threats and vulnerabilities;

(e) all forms of sensitive communications within the scope of the Supplier's agreement with Rolls-Royce, including but not limited to web browsing, email, secure shell, remote desktop, etc., are encrypted using industry-standard encryption (e.g., minimum Transport Layer Security v1.2 (TLS v1.2) protocol) to prevent eavesdropping; and

(f) wireless devices used to deliver services that can connect to the Internet should be configured securely and protected by a correctly configured firewall or equivalent network device (e.g., Wi-Fi router);

1.7 in relation to incident management, if the Supplier identifies, detects, is notified, or reasonably suspects a Cyber Security Incident relating to services within the scope of the goods and/or services provided to Rolls-Royce or the Supplier IT systems storing or processing Rolls-Royce Data, the Supplier shall:

(a) track, document and notify the Rolls-Royce Security Operations Centre (sec.reporting@rolls-royce.com within 48 hours of becoming aware of, or reasonably suspecting, a Cyber Security Incident has occurred;

(b) provide Rolls-Royce SOC with report(s) of the investigation undertaken and findings including, if relevant, any Indicators of Compromise (IoCs). Promptly reply to requests for further information and support Rolls-Royce in meeting its notification and breach reporting obligations, within the required time limits, to Supervisory Authorities; and

(c) promptly take all steps necessary to contain the incident, mitigate the impact and prevent its reoccurrence, and inform Rolls-Royce of the corrective actions taken and provide a plan of further remedial action and timescales, with any joint actions to be agreed upon between the Supplier and Rolls-Royce;

1.8 in relation to resilient networks and systems:

(a) a disaster recovery plan that describes the Supplier's actions in the event of a severe incident, impacting the availability and safe operation of IT resources and tested regularly to ensure it works in practice;

(b) a business continuity plan that describes how the Supplier's business will continue operating in the event of a severe incident impacting IT resources, and tested regularly to ensure it works in practice;

(c) data backups should be taken regularly and protected appropriately (e.g., through encryption, offsite storage, physical controls, etc.) to ensure that in the event of a failure, Supplier systems and Rolls-Royce Data can be restored and services resume in a timely manner; and

(d) is ready to exercise plans with Rolls-Royce to ensure alignment and assess preparedness in response to common cyber-attacks;

1.9 in relation to vulnerability management:

(a) maintain awareness of vulnerabilities and cyber threats;

(b) undertake vulnerability assessments to ensure ongoing resilience of Supplier IT systems storing or processing Rolls-Royce Data at least annually using industry standard tools, techniques, and methodologies;

(c) identify, triage, and mitigate vulnerabilities following the Supplier's security policy and, upon request, share the remediation plans with Rolls-Royce;

(d) regularly run vulnerability scanning tools against networked devices to check software and hardware patches and security fixes have been kept up to date; and

(e) perform regular security risk assessments of systems and components that store, process, or manage access to Rolls-Royce Data. Embed an appropriate risk management regime, actively

Not Subject to Export Control

supported by the board and senior managers, and maintain a record of security risks and mitigating actions in a securely controlled location;

1.10 in relation to supply chain management:

(a) maintain an inventory of all third-party goods and services, including records on supplier's contact details, and for software/hardware components the details of the support lifecycle and update schedule, how updates are obtained, and the level of testing performed on supplied components (i.e., before installation into Rolls-Royce systems, after significant configuration changes, etc.); and

(b) security risks of third-party components and support services are well understood, documented, owned, and managed by stakeholders; and

1.11 in relation to security assurance and reporting:

(a) regularly review and inform Rolls-Royce of the compliance status with this Rolls-Royce Supplier Minimum Cyber Security Standard and share information on security risks to Supplier IT systems and services within the scope of the relevant agreement with Rolls-Royce; and

(b) when requested, respond to requests for information and assist Rolls-Royce, or its assigned independent third party, to contribute to assurance activities within the scope of the relevant agreement with Rolls-Royce.

Section B: Cloud Security

This section of the Rolls-Royce Supplier Minimum Cyber Security Standard covers Rolls-Royce Data stored and processed by, and services supporting business and operational processes hosted in the Cloud (SaaS, IaaS, PaaS). Suppliers may use Cloud services as part of their contracted service offering (e.g., access to Cloud-hosted software/web-based application for data processing, delivering a PaaS service providing both software and hardware connected to machines on Rolls-Royce factory floor, etc.).

There is increasing use of Cloud computing to deliver services to Rolls-Royce, or storage and processing of Rolls-Royce Data. Cloud creates an agile environment for delivering infrastructure and application services, however incorrect configuration and poor security measures may impact the security of Rolls-Royce Data. This may lead to unauthorised access, theft of data, storage of Rolls-Royce Data in unknown locations, breach of export controls and customer data, disruption to access or services, account takeover, etc., A good service using a secure design and default configuration will ensure the Cloud service can defend against common cyber-attacks. The purpose of this section is to describe the measures required by Rolls-Royce in relation to the use of Cloud by Suppliers.

For the purposes of this section of the Rolls-Royce Supplier Minimum Cyber Security Standard "**Cloud Services**" are shared computing and storage resources accessed as an online service instead of locally on-premises.

1. in relation to cloud security principles the Supplier shall ensure that:

(a) data in transit, between networks and external to the Cloud environment, shall be protected against tampering and eavesdropping, using a combination of encryption, service authentication and network-level protections;

(b) data and assets storing, or processing Rolls-Royce Data are protected against physical tampering, loss, and damage or seizure. Protections shall include encryption, physical security of data centres and locations the Supplier operates from, secure data erasure and service resiliency;

(c) it maintains separation between customer data and/or its tenants/Cloud Services. Effective boundaries are implemented to ensure networks and customer services are managed separately, preventing leakage of data and code between different environments;

(d) it carefully coordinates and controls its management of Cloud Services and the data handled within it, and can demonstrate secure operations, services and security measures are effective throughout the contract lifetime. The administrative systems, services and processes are designed, implemented, and managed to maintain a secure environment and follow best industry practices;

(e) it can detect, respond to, impede and/or prevent attacks on Cloud Services. This can be achieved through regular vulnerability scanning and patch management, proactive monitoring, configuration and change management, and effective incident management plans that are regularly tested;

(f) employees with access to stored Rolls-Royce Data and Cloud Services are vetted or undergo security checks and aftercare to ensure they are cleared to UK Government Baseline Protective Security Standard (BPSS) as a minimum (or in-country equivalent checks), receive security awareness training, and have the necessary skills to competently administrate and manage the Cloud Services;

(g) Cloud Services are designed and developed to minimise and mitigate security threats. Suppliers shall regularly assess the threats and risks to the Cloud environment and use a robust software development lifecycle (including automated and audited integration and deployment techniques). When code repositories are used, they shall be supported by good security practices for managing access and code configuration changes (e.g., protecting access credentials, and removing access when no longer required, maintaining records and reviewing all code changes before upload, backup code and ensure have an effective plan to recover in the event of an incident to the repository);

(h) subcontracted Cloud service providers follow and maintain good security standards and practices. The supplier shall notify Rolls-Royce if subcontracted third parties have access to Rolls-Royce Data or Cloud Services. During the lifetime of the contract, the Supplier shall provide ongoing assurance of any third-party procured hardware or software connected to its Cloud Services before installation and throughout the lifecycle of the assets;

(i) access to Rolls-Royce Data and Cloud Services is only provided to securely authenticated and authorised identities on a least privileged basis and removed when no longer required. Privileged Access Management (PAM) shall apply to all administrator accounts and, if applicable, tools shall be made available for Rolls-Royce to administer, manage, and monitor its staff and third-party access to Rolls-Royce Data and Cloud Services;

(j) Internet connected interfaces shall be continuously tested to ensure external interfaces remain secure and defences are implemented to protect Internet connected interfaces from common attacks, e.g., denial of service (DoS) attacks, authentication attacks (e.g., password spraying) and application-based attacks (e.g., SQL injection), etc.; and

(k) logging and auditing are available to identify security issues and incidents. Incident management plans shall be exercised regularly to test response to common cyber-attacks.

Section C: Connected devices

This section of the Rolls-Royce Supplier Minimum Cyber Security Standard covers any connected devices installed, integrated with, or connected to Rolls-Royce IT/OT systems, facilities, or products, and combined with associated supporting services to deliver an end-to-end business solution.

For the purposes of this section:

"**Connected Device**" means any device embedded with technology connected to a network infrastructure or Internet and interacts or communicates with other devices (including without limitation, the Internet of Things (IoT)) and associated services, which are also connected to the network. (Note: associated services are out of scope and covered by other sections of the Rolls-Royce Supplier Minimum Cyber Security Standard); and

"**The Internet of Things" (IoT)** means the interconnection of devices allowing them to interact with the surrounding environment and collect and share data without human interaction.

Risk statement: following an initial compromise, connected devices may be used as an attack vector or pivot point to enable cyber actors to steal data or gain access to connected networks and systems for espionage purposes, cause disruption to the device operations or associated services, or for financial gain (e.g., ransomware attacks).

1. The Supplier shall ensure:

1.1 in relation to asset management:

Not Subject to Export Control

(a) an inventory of installed Connected Devices and associated services hardware and software (including software components and sub-components) is maintained, including details of manufacturer and contact details, period of support, unique identifiers and description of the device's physical location and network connectivity, etc.;

(b) sensitive data handled by Connected Devices is stored and transported securely over insecure networks, using appropriate cryptographic mechanisms;

(c) Connected Device stored data, including build configuration shall be securely backed up regularly;

(d) hard-coded unique security parameters (e.g., device identity) shall be implemented to resist tampering by physical, electrical or software, and critical security parameters in software source code (e.g., hard-coded usernames and passwords) shall not be used; and

(e) data and configuration settings shall be securely removed or deleted from decommissioned Connected Devices and associated services, or alternatively, secure disposal methods are used that prevent recovery of data;

1.2 in relation to access control:

(a) where pre-installed passwords are used, they shall be unique per Connected Device and generated using a mechanism that reduces the risk of automated attacks, or can be changed by the user on first use or during initialisation;

(b) authentication mechanisms used to authenticate users shall use best practice cryptography, appropriate to the properties of the technology, risks to system and usage, and the authentication value (e.g., certificate, token, ONP, etc.) is changeable;

(c) limitations on the number of authentication attempts within a defined time interval, and brute-force attacks on the authentication mechanism via network interfaces are detected and prevented;

(d) access to Connected Device functionality via the network interface should only be available to authorised and authenticated users and devices; and

(e) least privileged and secure management processes follow industry best security practices for user, administrative and management access (e.g., Privileged Access Management);

1.3 in relation to software security:

(a) software is developed using industry best practice secure development processes;

(b) software has mechanisms to validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networked Connected Devices and associated services;

(c) software is kept up to date, following industry best security practices, and critical vulnerabilities are patched within 14 days of release. The Supplier shall maintain records of Connected Devices or associated services that cannot have their software updated, and details shared with Rolls-Royce on request, including patch status, the rationale for the absence of software updates, period of software update support and method of hardware replacement and/or software upgrade support, etc.;

(d) mechanisms for Connected Devices and associated services to check after initialisation, and then periodically, if software security updates are available. These mechanisms shall support the authenticity and integrity of software updates, approved automatic updates and update notifications, or enable the controlled release, installation, and verification of security updates; and

(e) security updates are distributed to Connected Devices and associated services using an appropriate secure transport mechanism or application layer protocol;

1.4 in relation to vulnerability management:

(a) maintain awareness of vulnerabilities and cyber threats to Connected Devices;

(b) undertake vulnerability assessments to ensure unused network and logical interfaces are disabled and the security of Rolls-Royce Data collected and handled by Connected Devices, using industry-standard tools, techniques, and methodologies;

(c) network interfaces of Connected Devices in initialised or offline state are minimised to prevent unauthenticated disclosure or security-relevant information and stored Rolls-Royce Data;

(d) Connected Device hardware shall not unnecessarily expose physical interfaces;

(e) software installed and used by Connected Devices and associated services are required for the intended use or operation of the Connected Device, and shall run with the least necessary privileges for security and functionality purposes;

(f) regularly run vulnerability scanning tools against networked Connected Devices to check software and hardware patches and security fixes have been kept up to date;

(g) identify, triage, and mitigate vulnerabilities promptly and following the Supplier's security policy and, upon request, share the remediation plans with Rolls-Royce;

(h) for Connected Devices operating within or connected to high-risk or critical systems and services, appoint an independent third party to conduct a security penetration test of external/Internet facing interfaces at least annually and following any major technology systems or infrastructure changes;

(i) perform regular security risk assessments of connected devices collecting, storing, or processing Rolls-Royce Data. Embed an appropriate risk management regime, actively supported by the board and senior managers and maintain a record of security risks and mitigating actions in a securely controlled location; and

(j) details of the manufacturer's vulnerability disclosure policy shall be maintained, including contact details for reporting issues and information on timelines for responding to reported issues;

1.5 in relation to resilient devices and services:

(a) disruptions to Connected Device basic functionality shall be kept to a minimum:

(i) Rolls-Royce shall be informed with sufficient notice of any planned outages to Connected Devices and associated services;

(ii) seek prior-approval from Rolls-Royce for planned outages of Connected Devices providing safety-relevant functions or services; and

(iii) Connected Devices remain operating and locally functional during a loss of network access or outages of data networks and power. Connected Devices shall reconnect to networks in an expected, operational, and stable state, taking into consideration the capability of the infrastructure (i.e., preventing signalling storms or Distributed Denial of Service (DDoS) events);

(b) Connected Devices shall verify installed software using secure boot mechanisms, and if unauthorised changes are identified, the Connected Device shall issue an alert to an appropriate monitoring system/service; and

(c) Connected Device telemetry data (e.g., usage and measurement data, security logs recording access, configuration changes and system functions, etc.) shall be collected and examined by an appropriate monitoring system/service for security anomalies; and

1.6 in relation to incident management, if the Supplier identifies, detects, is notified, or reasonably suspects a Cyber Security Incident relating to Connected Devices and associated services within the scope of

the relevant agreement with Rolls-Royce or Supplier IT systems storing or processing Rolls-Royce Data, the Supplier shall:

(a) track, document and notify the Rolls-Royce Security Operations Centre (sec.reporting@rolls-royce.com within 48 hours of becoming aware of, or reasonably suspects, a Cyber Security Incident has occurred;

(b) take into consideration the safety aspects of Connected Devices, and identify any consequences of misuse, misconfiguration and/or failure;

(c) provide Rolls-Royce SOC with the report(s) of the investigation undertaken and findings including, if relevant, Connected Device telemetry data (depicting security anomalies) any Indicators of Compromise (IoCs); and

(d) promptly take all reasonable steps necessary to contain the incident, mitigate the impact and prevent its reoccurrence, and inform Rolls-Royce of the corrective actions taken and provide a plan of further remedial action and timescales, with any joint actions agreed between the Supplier and Rolls-Royce.

Section D: Secure Software Development

The scope of this section of the Rolls-Royce Supplier Minimum Cyber Security Standard covers the development of software for Rolls-Royce use. It considers security implications of modern code development and risk management during the development process.

For the purposes of this section "**software**" means those software assets that are necessary to conduct Rolls-Royce business, including but not limited to application software, system software, development tools and utilities.

Risk statement: malicious interference in code, changes to the intended function of the software, causing damage to, exploits or disables the devices, systems and/or networks it is installed, or is used to steal data, bypass access controls and cause harm or damage as a consequence of its malfunction or failure.

1. The Supplier shall ensure:

1.1 in relation to secure development environment:

(a) it complies with security requirements in Section A for IT environments used for software development (where applicable, non-confirming controls leading to a less constrained environment should be documented, and risks understood and managed);

(b) the development environment is segregated (at least logically) from corporate/business services and production (live) systems;

(c) access to the development environment is restricted to authorised developers and system administrators who shall be provided with the least privileged access and authenticate using multi-factor authentication (MFA);

(d) developers follow secure coding standards and practices (i.e., Software Development Lifecycle);

(e) tool choice is based on a balanced consideration of usability and functionality, and configuration settings should be the most secure possible;

(f) sensitive information (such as IP, encryption and access keys, passwords, and knowledge of security controls) is protected;

(g) appropriate protections are provided for code throughout its lifecycle (build, deployment, production, and development);

(h) user/system logging and protective monitoring are used to help detect compromise and facilitate effective remediation of security incidents;

1.2 in relation to code repository:

Not Subject to Export Control

(a) access to the code repository is controlled using MFA and revoked when no longer required and regular access reviews are performed;

(b) least privileged access for those with permission to make changes to the code repository. All user activity is logged, and changes to master versions are reviewed and independently verified; and

(c) version control and reviews are regularly performed, and code is backed up, securely; and

1.3 in relation to security testing and vulnerability management:

(a) security testing is aligned with the development lifecycle, and provides confidence that vulnerabilities are resolved before technology releases;

(b) maintain records of the coverage of tests and remediation plans, and track unresolved issues; and

(c) maintain vulnerability disclosure scheme for users and researchers to responsibly disclose security issues, and processes to review and resolve reported security issues.

Section E: Offshoring data, systems, and services

Rolls Royce, like many organisations, is reliant on suppliers to develop and deliver its products and services. Global supply chains and a shortage of essential skills lead many organisations to outsource and offshore their systems and services. Managed service providers and engineering partners are no exception to the trend. Rolls-Royce is facing increasing pressure from suppliers to accommodate changes in the geolocation of data, systems and services and third-party employees engaged on Rolls-Royce contracts. This increases the risk for Rolls-Royce, and the location data is stored and processed is of particular and specific concern.

For the purposes of this section, "offshoring" means the contracting of any work to a third-party and/or where this work is carried out and data is stored and processed in a geographically separate region from Rolls-Royce's base of operations.

Risk Statement: the risks of offshoring data, systems and services to geographical locations Rolls-Royce does not operate in, include (without limitation): (i) access to data to sanctioned countries; (ii) theft and egress of data and services to unmanaged locations; (iii) bypassing managed service providers security controls to access and compromise Rolls-Royce IT systems; and (iv) breach of regulatory or customer contract.

1. The Supplier shall ensure:

1.1 in relation to location of data, systems, and services:

(a) provides locations where all data shall be stored/processed, systems accessed, or services delivered from. The supplier shall not offshore Rolls-Royce data, systems, or services without Rolls-Royce's prior written approval; and

(b) connectivity, operating model and staff access to Rolls-Royce Data and systems shall be reviewed regularly and reports provided to Rolls-Royce to provide assurance that the controls are effectively managing the risks. Any changes shall be submitted to Rolls-Royce for approval prior to implementing such changes;

1.2 in relation to physical security:

(a) physical security protections are implemented to prevent unauthorised access to Rolls-Royce Data, systems, and services, including but not limited to:

(i) secure working areas with a door access control system for authorised personnel only and access logs shall be reviewed regularly;

(ii) staffed reception area (control of visitors and goods-in/goods-out); and

(iii) 24x7 monitoring (Intruder alarms and CCTV);

1.3 in relation to network security:

(a) boundary firewall or equivalent device controls connectivity to and from Supplier's networks, to:

(i) permit outbound connections from the network as defined by business requirements;

(ii) permit inbound connections only to approve networks/services as defined by business requirements; and

(iii) block access to unapproved services;

(b) network segregation controls connectivity within the network(s) based on information criticality and business requirements (e.g., internet-facing services should be segregated with controlled access to internal networks and resources);

(c) following security hygiene checks (e.g., patch status, anti-virus checks, etc.) and authentication, devices are permitted access to the Supplier's networks; and

(d) remote access to Supplier's networks is controlled by multi-factor authentication ("**MFA**") via, for example, cloud broker services or secure web gateways;

1.4 in relation to device security:

(a) only corporate managed devices are connected to Rolls-Royce systems and services, using approved remote access solutions and MFA for device and user. Personal devices are not permitted to access Rolls-Royce systems or store/process Rolls-Royce Data;

(b) devices have a hardened security build, with only approved applications installed, hard drive encryption and secure boot. Security agents installed on devices (e.g., malware protection, software firewall, end-point protection, etc.) and configured to apply automatic security updates;

(c) devices are regularly scanned for vulnerabilities; and

(d) mobile device management (MDM) is used for device provisioning, enrolment, application management and remote wipe; and

1.5 in relation to personnel security:

(a) their employees and contractors with authorised access to Rolls-Royce Data, systems and services are vetted and undergo security checks and aftercare to ensure they are cleared to UK Government Baseline Protective Security Standard (BPSS) as a minimum or in-country equivalent checks;

(b) onboarding and offboarding processes manage risks of employees and contractors with access to Rolls-Royce Data and IT systems. Access or user permissions shall be revoked when no longer required or upon the departure of an individual from the Supplier's employment and ensure any Rolls-Royce Data and equipment is returned when no longer required;

(c) their employees and contractors receive training and awareness that promotes and values positive contributions to security and that they have access to the necessary skills and security expertise to support them in their role; and

(d) their employees and contractors with access to data and systems are trained on relevant security policies. Supplier shall ensure all staff are aware of cyber security risks to Rolls-Royce Data and IT systems and their responsibilities, including how to identify and report security breaches, handle information securely and in accordance with regulation/legislation governing location, export control, intellectual property and Government classified data that is stored, handled, and processed by the Supplier.

Section F: Artificial Intelligence (AI) security

This section of the Rolls-Royce Supplier Minimum Cyber Security Standard covers the minimum security measures that Rolls-Royce's Suppliers must implement and maintain during the provision of any Artificial Intelligence (AI) related systems, services and technologies to the Rolls-Royce group of companies.

As the integration of Artificial Intelligence (AI) into products and services accelerates, the associated security risks, such as threats to data confidentiality, integrity, and system resilience, are also contributing to significant security risks. AI-specific security risks can be exploited by model manipulation, data poisoning, or misuse of generative capabilities, resulting in significant legal, reputational, and operational challenges. The controls in this section of this Rolls-Royce Supplier Minimum Cyber Security Standard are designed to mitigate AI-related security risks and ensure responsible deployment and use of AI technologies. The aim is to maintain a high level of security, trust, and regulatory compliance across Rolls-Royce's AI systems and Rolls-Royce's supply chain's AI systems.

This section of the Rolls-Royce Supplier Minimum Cyber Security Standard provides a set of AI security controls that must be adhered to by all suppliers using AI within services or goods it supplies to Rolls-Royce. These controls are aligned with the UK Cyber Security for AI Code of Practice and ETSI TS 104 223 Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems, thereby supporting compliance with the EU AI Act.

Secure Design

1. The Supplier shall ensure:

    1.1 in relation to the awareness of AI security threats and risks that:

        (a) its cyber security training programme shall include AI security content which shall be regularly reviewed and updated, to include:

            (i) training on the emergence of any new substantial AI-related security threats; and

            (ii) awareness of the latest security threats and vulnerabilities related to AI models, applications, and systems;

        (b) its AI security training shall be tailored to the specific roles and responsibilities of its own staff members;

        (c) updates should be communicated through multiple channels, such as security bulletins, newsletters, or internal knowledge-sharing platforms; and

        (d) AI developers (being those individuals who are responsible for coding, testing and integrating AI models into applications and AI systems), and other specialist roles, shall train and be competent in secure coding and system design techniques specific to AI development, and preventing and/or mitigating security vulnerabilities in AI algorithms, models, and associated software;

    1.2 in relation to the design of the Supplier's AI system for security, as well as functionality and performance, the Supplier will:

        (a) conduct a thorough risk assessment that determines and documents the AI security risks and mitigation strategies, including any interfacing systems or data sources;

        (b) involve the relevant Rolls-Royce data owner who has authority and accountability for the quality, security, and usage of data, when appropriate, in internal discussions when determining the requirements and data needs of the AI system, particularly when discussing risks determined in (e) below;

        (c) ensure that AI systems are designed and implemented to withstand adversarial AI attacks, unexpected inputs, and AI system failures;

        (d) support the process of preparing data, security auditing and incident response for an AI system and AI developers shall document and create an audit trail in relation to the AI system, to include. This shall include the operation, and lifecycle management of models, datasets and prompts incorporated into the system;

        (e) assess the security risks of any external components used and perform due diligence in line with existing software development processes;

        (f) ensure that the Supplier's employees proactively identify and report internally on any potential security risks in AI systems and processes and if such risks impact or may impact Rolls-Royce the

Not Subject to Export Control

Supplier will report such security risks to their Rolls-Royce point of contact as soon as reasonably practicable;

(g) inform the Supplier's Rolls-Royce procurement or business point of contact if external vendor(s) or provider(s) are involved in delivering the relevant services or goods to Rolls-Royce and perform due diligence assessments to ensure such sub-contractor is adhering to this section F (AI Security); and

(h) ensure permissions granted to the AI system, service or technology, or other systems or data sources (be they internal or external) are provided as at least privileged, and/or for functionality of the AI system;

1.3 in relation to threats and managing risks to the Supplier's AI system, service and/or technology, the Supplier will:

(a) analyse threats and manage security risks, including when changing a setting, implementing a new configuration, and/or replacing components, through the lifecycle of the AI system, service, and technology;

(b) use threat modelling, or similar approach, to perform regular reviews, and to understand AI-specific attacks to their systems, services and/or technology (e.g., data poisoning, model inversion, and membership inference);

(c) where applicable:

(i) in relation to developers of AI systems, services, and technologies, that such developers shall manage the security risks associated with their respective AI models; and

(ii) where increased functionality leads to increased risk, apply controls to risks identified through the analysis to reduce risk to an acceptable level;

(d) when identified AI security threats cannot be resolved by developers:

(i) inform system operators, so they can threat model their systems;

(ii) inform Rolls-Royce, and identify how they should be detected, so Rolls-Royce is made aware of these threats; and

(iii) ensure all communications include detailed descriptions of the risks, potential impacts, and recommended actions to address or monitor these threats;

(e) if sub-contractors have responsibility for managing AI security risks, identified within the AI system, service or technology, then Suppliers should obtain assurance that such sub-contractors have appropriate mitigations to address such risks; and

(f) continuously monitor and review the risks to AI system, services, and technologies, and inform Rolls-Royce of risks above the Supplier's appetite; and

1.4 in relation to responsibilities for development and use of AI systems, services, and technologies the Supplier will:

(a) incorporate and maintain capabilities to enable human oversight of AI systems, services, and technologies:

(b) design systems for humans to assess outputs they are responsible for, by ensuring that models outputs are explainable or interpretable;

(c) when human oversight is a risk control, design, develop, verify, and maintain technical measures to reduce the risk through such oversight;

(d) verify security controls specified by Rolls-Royce have been built into the system; and

(e) make Rolls-Royce aware of any prohibited use cases of the AI system, services, and technologies.

Secure Development

2. The Supplier shall ensure that:

2.1. in relation to the identification, tracking and protection of assets, the Supplier will:

(a) maintain a comprehensive inventory of Supplier's assets (including any interdependencies/connectivity);

(b) as part of broader software security practices, have processes and tools to track, authenticate, manage version control, and secure the Supplier's assets due to the increased complexities of AI specific assets;

(c) develop and tailor disaster recovery plans to account for specific attacks aimed at AI systems;

(d) ensure that a known good state can be restored;

(e) protect sensitive data, such as training or test data, against unauthorised access;

(f) sanitise and check the quality of data and inputs when designing models, based on the access and storage of data and inputs. Repeat data and input checks when models are revised in response to feedback from Rolls-Royce or continuous learning; and

(g) any training data or model weights are confidential, and developers put appropriate protections in place to protect them;

2.2. in relation to securing the Supplier's infrastructure, the Supplier will:

(a) evaluate access control frameworks and identify appropriate measures to secure APIs, models, data, and training and processing pipelines;

(b) secure APIs to external customers or collaborators and apply controls that mitigate attacks on the AI system via the API;

(c) use dedicated environments for creation, development, and model tuning activities and back dedicated environments by technical controls to ensure separation and principle of least privilege;

(d) implement and publish a clear and accessible vulnerability disclosure policy;

(e) create, test, and maintain an AI system incident management plan and AI system recovery plan; and

(f) ensure any cloud service operators secure its capability, and any contractual agreements with them support compliance with this Section F (AI Security) of the Supplier's AI systems, services, and technologies;

2.3. in relation to securing the Supplier's supply chain, the Supplier will:

(a) ensure developers and system operators follow secure software supply chain processes for AI model and system development;

(b) document the security and use and/or adaption of any sub-contractor AI models, or components and agree with Rolls-Royce the use and/or adaption of such AI models or components and will also ensure:

(i) mitigating controls are in place and undertake a risk assessment linked to such models or components;

(ii) the sharing of this documentation with Rolls-Royce in an accessible way; and

(iii) regularly re-run test evaluations on released models; and

(c) communicate to Rolls-Royce, in an accessible way, their intention to update models before the models are updated;

Not Subject to Export Control

2.4. in relation to documenting the data, models, and prompts, developers of AI models and prompts will:

(a) document, and maintain a clear audit trail of their system design and post-deployment maintenance plans;

(b) make documentation available to system operators and Rolls-Royce, and include security-relevant information such as:

(i) sources of training data (including fine-tuning data and human or other operational feedback);

(ii) intended scope and limitations;

(iii) guardrails;

(iv) data retention time;

(v) suggested review frequency; and

(vi) potential failure modes;

(c) release cryptographic hashes for model components and make them available, for Rolls-Royce to verify the authenticity of the components;

(d) maintain documentation of training data, including:

(i) source of the data (including publicly available sources);

(ii) URL of scraped pages;

(iii) Data/time data obtained; and

(iv) how the data is used in the model; and

(e) maintain an audit log of changes to system prompts or other model configurations (including prompts) that affect the underlying working of the AI systems and make such audit log available to Rolls-Royce on request; and

2.5. in relation to testing and evaluation, developers of AI models, applications and systems will:

(a) ensure all components are tested as part of a security assessment process;

(b) conduct security testing with support from developers and using independent security testers with relevant technical skills, prior to the system being deployed and at least once annually;

(c) share findings from the testing and evaluation, with supplier or supplier sub-contractor system operators to inform their own testing and evaluation assessments; and

(d) evaluate model outputs regularly to ensure they do not allow system operators or end-users to reverse engineer non-public aspects of the model or the training data, or to have unintended influence over the system.

Secure Deployment

3. The Supplier shall ensure:

3.1. in relation to communication and processes associated with Rolls-Royce end users, developers of AI models, applications and systems, the Supplier will:

(a) communicate where and how their personal data will be used, accessed, and stored;

(b) provide guidance to support secure and safe use, management, integration, and configuration of AI systems. This guidance shall include information on the appropriate use of models or systems, highlighting their limitations and potential failure modes;

(c) inform Rolls-Royce of any security relevant updates and provide clear explanations in an accessible way; and

(d) comply with Section 1.7 of Section A (Data, Systems and Resiliency) if affected by a Cyber Security Incident and take appropriate action to contain and mitigate the impacts of an incident on Rolls-Royce data or its use of the AI systems, services and technologies.

Secure Maintenance

4. The Supplier shall ensure:

4.1. in relation to maintaining regular security updates, patches, and mitigations, that the Supplier will:

(a) provide security updates and patches, where possible, and notify Rolls-Royce of the security updates;

(b) treat major AI system updates as a new version of a model and undertake security testing and evaluation process prior to deployment; and

(c) respond to model changes by providing Rolls-Royce preview access (e.g., via beta testing and versioned APIs, etc.); and

4.2. in relation to monitoring AI system's behaviour, the Supplier will:

(a) log system and user actions to support security compliance, incident investigations and vulnerability remediation;

(b) analyse logs to ensure AI models continue to produce desired outputs, and to detect anomalies, security breaches, or unexpected behaviour over time (e.g., data drift or data poisoning, etc.); and

(c) monitor internal states and performance of AI models and systems over time, to detect sudden or gradual changes in behaviour that could affect its security.

Secure End of Life

5. The Supplier shall ensure that:

5.1. in relation to proper data and model disposal it may with Rolls-Royce's prior written consent transfer or share ownership of Rolls-Royce data, training data and/or AI models to another entity; and

5.2. when decommissioning an AI model and/or system, the Supplier will:

(a) notify Rolls-Royce of its intention to decommission a model;

(b) securely return or delete Rolls-Royce data and all applicable data, and configuration details; and

(c) securely dispose of Rolls-Royce data, training data and AI models, and/or system components.