BlackBerry Security Requirements (BBSR)

This BlackBerry Security Requirements document (the **"Document**") details specific minimum-security requirements that BlackBerry expects of any third-party supplier, consultant, service provider or Supplier ("**Supplier**") processing, storing or transmitting BlackBerry Materials. The Supplier shall ensure that any third party that it uses, which will have access to BlackBerry Materials shall also comply with the requirements. Where a Service Provider or Partner is incapable or unwilling to implement these controls, alternate compensating controls may be used with the approval of BlackBerry Information Security Management.

The following sections detail the security requirements that apply to a Supplier.

All definitions and expressions in this Document shall have the same meaning as the definitions and expressions used in the agreement to which this Document is attached or in which this Document is referenced (the **"Agreement**"), unless otherwise defined herein.

If there is a direct conflict between any requirement in this Document and in the Agreement, the terms of this Document will prevail to the extent of such conflict.

The most recent version of the BlackBerry Security Requirements Document is available here:
https://blackberry.com/bbsrd

Definitions:

"BlackBerry Materials" means BlackBerry products, data, plans, specifications, reports, designs, source code, object code, customer information, documentation, BlackBerry Confidential Information, Personal Information, and any other information or materials provided by BlackBerry, or to which Supplier has had indirect or direct access during performing its obligations hereunder.

"BlackBerry Confidential Information" is as defined in a Non-Disclosure Agreement ("NDA") between the parties and includes without limitation (or, if no NDA exists means) all information (including BlackBerry Materials and personal information), drawings, specifications, data, other engineering and manufacturing information, software, source code, business plans, or other property furnished by BlackBerry, or prepared by Supplier in connection with the Agreement.

"Business Continuity Plan" means Supplier's business continuity and disaster recovery plan.

"Personal Information" means any information or data of any kind that personally identifies or that can be used in conjunction with other information or data, to personally identify an individual that is collected, used, transferred or disclosed by or to Supplier in the course of providing the products or Services.

"Services" means the services to be provided by Supplier to BlackBerry as set out in a statement of work or other order document.

"Term" means the term of the Agreement including any renewal periods thereto.

1 Security requirements

1.1 Access Control (AC)

AC1 Access to Supplier's applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by the Supplier's management to ensure access is restricted to the minimum level necessary for individual role responsibilities to be discharged, before access is granted.

AC2 The Supplier must use a secure method to convey authentication credentials and authentication mechanisms. Multi-factor authentication must be used where feasible.

AC3 The Supplier must assign unique and non-recycled user identifiers to individual users. The use of shared accounts must be prohibited except where there are technical limitations.

AC4 Timely deprovisioning, revocation, or modification of user access to the Supplier's systems information assets, and data shall be implemented upon any change in status of employees, contractors, customers, business partners, or third parties.

AC5 The Supplier will implement and enforce (through automation) user credential and password controls for applications, databases, and server and network infrastructure in accordance with industry best practices.

AC6 The Supplier shall ensure that multi-factor authentication is required for all remote user access.

AC7 The Supplier restricts the use of privileged accounts on the information system to only those necessary for the performance of authorized tasks and documents the rationale for such access

1.2 Compliance (CP)

CP1 The Supplier will engage a reputable and independent third party to conduct reviews of the Supplier's implementation of their cyber security program and applicable regulatory requirements as necessary (for example, SOC2 or ISO27001.

The Supplier will provide, upon request from BlackBerry, a formal report from the auditor detailing the scope, period, and the results of the assessment, including any deficiencies or areas of non-compliance, and the Suppliers risk remediation activities, and timelines for implementation.

CP2 The Supplier's systems performing Services under the Agreement, or those systems interconnected to such key systems not separated by a firewall, must be scanned for vulnerabilities based on industry best practices.

CP3 The Supplier's systems performing Services under the Agreement, or those systems interconnected to such key systems not separated by a firewall or otherwise reasonably segregated, must be subject to a penetration test, completed by an independent and qualified third party on an annual basis.

CP4 The Supplier shall allow BlackBerry, upon thirty (30) days prior written notice and subject to the Supplier's reasonable security requirements, to attend the Supplier location to inspect BlackBerry Materials and the Supplier's compliance with these BlackBerry Information Security Requirements.

Control deficiencies and areas of non-compliance will be remediated using industry standard processes and tools within a reasonable period, the timeframe of remediation being subject to negotiation between BlackBerry and the Supplier. This includes, but should not be considered limited to, areas of concern identified by BlackBerry prior to the commencement of the Agreement.

1.3 Change/Release Management (CR)

CR1 All changes to the production environment must follow a formal and documented procedure in accordance with industry best practices and be tested and approved before implementation.

CR2 The Supplier must undertake an independent third-party security code review and scan of any internally developed software to identify, detect and remediate security vulnerabilities. The Supplier must perform quality assurance testing of the application security components to validate and maintain the confidentiality and integrity of the system resources and data. Any such third party must be reviewed and deemed acceptable to BlackBerry.

CR3 Material planned changes that may impact the security of BlackBerry Materials must be communicated in writing to by notifying security@blackberry.com a minimum of 2 business days before implementing the changes. Material unplanned changes should be considered Security Incidents.

1.4 Data Governance (DG)

DG1 The Supplier shall at all times maintain policies and procedures for acceptable use of information assets. The Supplier's management shall review these policies and procedures at planned intervals, or because of changes to the organization, in order to ensure their continuing effectiveness and accuracy.

DG2 The Supplier shall ensure that the system containing BlackBerry Confidential Information shall be assigned a classification, taking into consideration data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, value, sensitivity, criticality, and any other obligations for retention and prevention of unauthorized disclosure or misuse.

DG3 The Supplier shall at all times maintain policies and procedures for labelling and handling data and objects that contain BlackBerry Confidential Information.

DG4 The Supplier shall at all times maintain policies and procedures for data retention and storage, and backup or redundancy mechanisms to ensure availability of BlackBerry Confidential Information, and compliance with regulatory, statutory, contractual, or service availability where applicable. Testing the recovery of backups must be implemented at planned intervals and annually at a minimum. The Supplier shall inform BlackBerry of deficiencies noted during testing.

DG5 The Supplier shall at all times maintain mechanisms for the secure disposal and complete removal of BlackBerry Confidential Information from all storage media, ensuring that data is not recoverable, by any computer forensic means as per the NIST 800-88 standard. Secure disposal shall be restricted to authorized personnel to prevent unintentional or malicious data loss.

1.5 Human Resources (HR)

HR1 The Supplier shall ensure that all persons that will have access to BlackBerry Confidential Information and systems will be subject to background verification screening, pursuant to local laws, regulations, ethics, and contractual constraints. Such background screening to be completed prior to any person being granted access to BlackBerry Confidential Information and systems.

HR2 The Supplier shall ensure that before granting physical or logical access to BlackBerry Confidential Information or systems, employees, contractors, third-party users and tenants, and customers shall contractually agree and sign equivalent terms and conditions regarding information security responsibilities in employment or service contracts. The individuals who will access BlackBerry systems will be required to complete the BlackBerry Contractor Code of Conduct training and attest to compliance before being granted access.

HR3 The Supplier shall implement a security awareness training program for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to BlackBerry Confidential Information shall receive appropriate awareness training, including for the threat of social engineering.

HR4 The Supplier shall implement and maintain a formal disciplinary or sanction policy for employees who have violated security policies and procedures.

1.6 Incident Response (IR)

IR1 The Supplier shall at all times maintain policies and procedures to triage and respond to security-related events. These policies and procedures shall include proper forensic procedures, including chain of custody, to support potential legal action subject to the relevant jurisdiction.

IR2 Immediately following the Supplier's reasonable suspicion of a security incident that may impact BlackBerry Materials or BlackBerry systems, the Supplier must notify BlackBerry at security@blackberry.com, 1-877-746-5831 x79997 or, 1-519-888-7465 x79997

The Supplier will provide BlackBerry with a mechanism to report security incidents.

The Supplier shall communicate with BlackBerry designated individuals and will promptly provide updates regarding steps taken by the Supplier to rectify or address the security breach or security incident. The Supplier must support BlackBerry's efforts to perform an audit of the Supplier's physical, logical, and information security controls commensurate with the Services being provided under the Agreement.

IR3 The Supplier shall ensure that a comprehensive Business Continuity Plan is in place to include how business operations shall be restored as quickly as possible following an interruption to or failure of business process.

1.7 Operational Controls (OC)

OC1 The Supplier shall at all times maintain policies, processes, procedures, or technical controls to enforce and assure proper segregation of duties.

OC2 The Supplier shall at all times maintain policies and procedures and a mechanism for vulnerability and patch management. Applicable patches must be tested and applied in a timely manner taking a risk-based approach for prioritizing critical patches. If patching is not possible, alternate risk treatment must be used as approved by Supplier's management. The Supplier will inform BlackBerry about Common Vulnerabilities and Exposures (CVE) rated vulnerabilities of High or Critical, that are not able to be patched.

OC3 The Supplier will deploy and maintain an effective antivirus solution that can detect, remove, and protect against all known types of malicious or unauthorized software within a maximum of 24 hours of its release.

OC4 User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications. Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.

OC5 Information classified as BlackBerry Confidential or higher must be prohibited from being stored on removable media except where;

- Using corporate managed laptops utilizing full disk encryption
- Mobile devices under the control of a MDM solution with appropriate encryption and secure access enabled.

If BlackBerry Confidential Information is required to be transferred to removable media, such activities must be approved in advance by BlackBerry, and then only to meet a specific business need of BlackBerry.

OC6 The Supplier shall establish baseline security requirements to be applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements.

Compliance with security baseline requirements must be reassessed at least annually or when significant changes occur. Applications shall be designed in accordance with industry accepted security standards (for example, OWASP for web applications) and shall comply with applicable regulatory and business requirements.

OC7 During the Term and Sunset period, the Supplier represents and warrants to BlackBerry that any supplied software, tool, or code does not contain: (i) any security vulnerability, virus, Trojan horse, worm, backdoor, shutdown mechanism, malicious code, sniffer, bot, drop dead mechanism, or spyware, and (ii) any other undocumented software, code, or program.

If the Supplier becomes aware of the existence of any malware or undocumented feature in or relating to the Licensed Software, the Supplier shall promptly notify BlackBerry.

OC8 Where the Supplier uses wireless environments within their organization, the Supplier will implement industry best practices and controls to detect and prevent unauthorized access.

OC9 Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and security events shall be retained for a period of 3 months and reviewed at least daily.

OC10 Network segregation must be used between trusted and non-trusted zones.

OC11 The Supplier will implement and operate file integrity (host), next generation firewalls, network intrusion detection, (IDS), network intrusion prevention (IPS), and advanced persistent threat (APT) detection and remediation tools to help facilitate timely detection, and to investigate the root cause analysis and response to incidents.

OC12 The Supplier shall implement industry standard encryption mechanisms when storing or transmitting BlackBerry Confidential Information. Publicly verifiable certificates from reputable vendors must be used.

OC13 The Supplier must use strong encryption technologies with ciphers approved by BlackBerry for the transfer of BlackBerry Confidential Information outside the Suppliers' controlled facilities and/or network, including without limitation, screen captures, voice recordings, and file transfers.

Advanced ciphers as defined by OWASP are approved, others must be reviewed. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/TLS_Cipher_String_Cheat_Sheet.md

For the transmission of email communications between BlackBerry and the Supplier, the Supplier will utilize a secure transport mechanism, for example, Transport Layer Security (TLS) with valid certificates, or a suitable, agreed upon alternative mechanism. BlackBerry and the Supplier will agree upon TLS failing to plain text (TLS Preferred) or failing to non-delivery (TLS Required).

OC14 The Supplier shall use an external, accurate time source to synchronize the system clocks of all relevant information processing systems within the organization or an explicitly defined security domain to facilitate tracing and reconstitution of activity timelines.

OC15 The Suppliers availability, quality, capacity, and resources shall be planned, prepared, and measured to deliver the required system performance to BlackBerry, in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.

OC16 Where information classified as BlackBerry Confidential or higher is retained in a database, the Supplier must have database transaction logging features enabled.

OC17 The Supplier must restrict access to security logs to authorized individuals. The Supplier must regularly review security logs for anomalies and must document and resolve all logged security problems in a timely manner. A SEIM (Security Event and Incident Management) platform is an expected control for log analysis and alerting.

OC18 Supplier may process BlackBerry Confidential Information only at locations agreed by BlackBerry in writing. The locations where Supplier will process BlackBerry Confidential Information cannot be changed without BlackBerry's written consent. Supplier shall not disclose or transfer any Blackberry Confidential Information to any person or entity located in a jurisdiction not previously agreed with BlackBerry.

OC19 The Supplier will check, assure and ensure originality and quality of the work outputs provided to BlackBerry as part of the Services. The Supplier will remain liable for any infringements that may occur as a result of the use of Generative AI.

OC20 The Supplier will disclose any use of Generative AI technology in delivering the Services. The Supplier will protect the confidentiality of BlackBerry Materials by not sharing them with a Generative AI system

1.8 Physical Security (PS)

PS1 Appropriate physical security perimeters, barriers, badge identification and access controls, and monitoring shall be implemented to safeguard sensitive data and information systems hosting BlackBerry Materials. Video monitoring should be used where deemed necessary.

PS2 Where systems have stored, processed, or transmitted BlackBerry Materials, policies, and procedures shall be established and maintained for secure disposal of equipment. Such procedures shall include a complete inventory of critical assets.

1.9 Risk Assessment (RA)

RA1 Where Supplier is given remote access to any BlackBerry systems, the Supplier will use this access solely to perform work within the scope of the Agreement. The Supplier will not access, or attempt to access, any other BlackBerry system other than those specifically required to perform the services.

The Supplier's access to services may be limited at BlackBerry's sole discretion and may be terminated at any time by BlackBerry. The Supplier will limit such access to those Supplier personnel who are qualified and required to have such access. The Supplier agrees to cooperate with BlackBerry in the investigation of any apparent unauthorized access by Supplier personnel to BlackBerry systems or unauthorized release of Confidential Information by the Supplier or Supplier's personnel.

1.10 Security Program (SP)

SP1 The Supplier shall ensure that an effective cyber security management program has been developed, documented, management approved, and implemented. The program shall include safeguards to protect BlackBerry assets from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

SP2 The Supplier shall develop and maintain an enterprise risk management framework in accordance to industry best practices. The risk framework shall have executive support and assessments must be completed at planned intervals, and at a minimum completed annually.

SP3 Risks shall be mitigated to a reasonable and acceptable level in accordance with industry best practices. Acceptance levels based on risk criteria shall be established and documented in accordance to industry best practices and must have executive approval.

1.11 Supplementary Measures for the Processing of Personal Data (PD)

PD1 Technical Measures

PD1.1 The Supplier shall provide the following measures related to Data Encryption:

- Encrypts data in transport using industry-standard ciphers supported by endpoint / client and the service provided to the customer.
- Encryption algorithms are implemented according to best practices and properly maintained using software without known cryptographic vulnerabilities.
- Encryption keys are reliably managed, including the methods used to generate, administer, store and revoke when necessary.
- In cases where transport encryption is not sufficient to prevent attacks, sensitive data is also encrypted end-to-end on the application layer using industry standard encryption methods.
- Encryption of data backups from operational systems.

PD 1.2 The Supplier shall provide the following measures related to Key Management Systems Monitoring:

- Performs logging and monitoring of key management activity, such as key generation, key renewal, key archive, key distribution, key destruction.

PD 1.3 The Supplier shall provide the following measures related to Network Protection:

- Implements network firewalls on external points of connectivity in Data Importer's network.
- Performs logging and monitoring of network activity for potential security events, including intrusion.

PD2 Contractual Measures

PD 2.1 The Supplier shall provide the following commitments on handling requests from public authorities:

- Ensures all requests from public authorities are reviewed to determine applicability, legality and proper jurisdiction.
- Ensures the Data Importer will use available legal mechanisms to scrutinize and limit demands from public authorities including the use of local counsel, international agreements and available judicial remedies.
- Ensures that any responsive information provided to a public authority is provided all confidentiality protections afforded under applicable law, including any non-disclosure provisions or orders.
- Ensures the Data Importer will object to requests which seek information outside the scope of the statutory limits or beyond the specific legal order and endeavor to minimize the scope of information requested.

PD 2.2 The Supplier shall provide assistance in conducting a transfer impact assessment:

- Provides product and service privacy notices and security documentation mentation to support privacy risk assessments and Article 46 GDPR transfer impact assessments by Data Exporters.
- Cooperates with exporters to ensure a timely and thorough review of the specific circumstances of the data transfer.

PD3 Organizational Measures

PD 3.1 The Supplier shall provide the following Information Security practices based on International Standards:

- Maintains information security and privacy polices based on ISO, NIST and AICPA standards and international best practices.
- Maintains ISO/IEC 27001 or equivalent certifications and at minimum annually audits its practices.

PD 3.2 The Supplier shall provide the following measures related to Transparency:

- Provides descriptions of personal data collected by BlackBerry Solutions in product privacy notices which are available on Data Importer's external web site.

PD 3.3 The Supplier shall provide the following Data Minimization Measures:

- Conducts privacy reviews of products and services throughout the software development lifecycle.
- Data collected and processed by BlackBerry is accessible only to authorized personnel.

PD 3.4 The Supplier shall provide the following measures related to Training:

- Requires personnel responsible for managing access requests from public authorities receive specific training that is updated periodically to align with corporate policies, new legislative and jurisprudential developments.
- Requires role-based training privacy training of personnel based on the privacy risks inherent in their roles and their access to personal data.