Black Duck Cybersecurity Requirements for Vendors

PURPOSE: The purpose of the requirements set forth herein ("Requirements") is to establish cybersecurity standards and data privacy requirements for products and services delivered to Black Duck by a person or entity ("Vendor"), or where Vendor otherwise has access to Black Duck Data. Vendor must handle, treat, and otherwise protect Black Duck Data in accordance with these Requirements and any contractual agreement between Vendor and Black Duck.

Defined terms used are found in Section 4 (Definitions) below.

SECTION 1: ACCESS TO BLACK DUCK NETWORKS AND/OR BLACK DUCK DATA PROCESSED WITHIN BLACK DUCK CONTROLLED ENVIRONMENT

1.1 Compliance: Vendor shall comply with all applicable privacy and security laws to which it is subject and shall not, by act or omission, place Black Duck in violation of any applicable privacy or security law including, without limitation, HIPAA. Vendor policies and practices must comply with all applicable laws, regulations, and contractual obligations under its agreements with Black Duck.

1.2 Third Party Disclosure: Vendor shall not disclose Black Duck Data to any third party unless with respect to each such disclosure: (A) the disclosure is necessary in order to carry out Vendor's obligations under its agreements with Black Duck; (B) such third party is bound by the same provisions and obligations as set forth in these Requirements; and (C) Vendor has received Black Duck's prior written consent.

1.3 Breach and Security Threat Notification: Vendor shall notify Black Duck Cybersecurity at csirt@blackduck.com without undue delay, but in no event should notification occur later than 48 hours from having actual knowledge of any Data Security Breach, security threat, or security incident (such as any security attack or hack allowing unauthorized access to Vendor's or its Customer's network) that impacts Black Duck Data or Black Duck information assets. At Vendor's cost and expense, Vendor shall assist and cooperate with Black Duck concerning any investigation, disclosures to affected parties, and other remedial measures reasonably requested by Black Duck or required under applicable law. Vendor shall respond within three (3) business days to Black Duck's request to complete a security assessment/questionnaire concerning the level of impact to Black Duck and/or Black Duck Data associated with a Data Security Breach.

1.4 Remote Access Control: If Vendor requires remote access to Black Duck Data, Vendor must use a Black Duck-approved method when connecting. Vendor must not install technology that provides remote access to any Black Duck Data on the Black Duck network, including, but not limited to, wireless access points, modems, Virtual Private Networks, remote access software, etc. Black Duck reserves the right to monitor all systems used by Vendor to connect to Black Duck networks or access Black Duck Data.

1.5 Data Owner: Black Duck Data shall at all times remain the sole property of Black Duck and nothing in these Requirements will be interpreted or construed as granting Vendor any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right to Black Duck Data other than the limited right to use the Black Duck Data for the purposes of fulfilling any Vendor contractual obligations to Black Duck.

1.6 Derivative Data: Vendor shall not create, use, retain, or maintain data that are derivative of Black Duck Data, except for the purpose of performing its obligations under its agreements with Black Duck or as otherwise expressly authorized in writing by Black Duck. Any derivative of Black Duck Data, regardless of how created, shall be deemed Black Duck Data.

1.7 Background and Screening Checks: To the extent permitted by local law, Vendor shall conduct appropriate background and screening checks prior to permitting any Vendor employee or contractor to access Black Duck Data, systems or premises. Vendor shall, in no event, expose Black Duck to a level of risk that is commercially unreasonable, or which is higher than that to which Vendor would be comfortable exposing itself. Black Duck may at its sole option require the Vendor, at Vendor's expense, to conduct more extensive background checks for any employee or contractor of Vendor who will have access to Personal Data or other information deemed highly sensitive by Black Duck.

1.8 Security Awareness and Education: Vendor shall have a defined security awareness program to provide periodic cybersecurity awareness training to Vendor's employees and contractors. If Vendor will have access to Black Duck Data while fulfilling the services, those Vendor employees and contractors shall also be subject to Black Duck's cybersecurity awareness training and shall comply with Black Duck's security policies and standards. Education and awareness training shall address, at a minimum, Vendor's security policies and standards for the secure handling of Black Duck Data, including annual security awareness training, privacy training, and regular phishing simulations. Vendor shall ensure that all relevant employees and contractors complete such training. If Vendor's services include software development, Vendor's training program must also include secure application development training to ensure Vendor is developing software is developed in accordance with secure coding techniques and principles.

1.9 Security Assessments and Audits: At Black Duck's request, Vendor shall submit to periodic security assessments to validate Vendor's compliance with industry standards and best practices, such as ISO 27001 and SOC 2. Vendor shall, at Vendor's expense, submit to reasonable data security and privacy compliance audits by Black Duck, or by an independent third party, upon reasonable evidence that Vendor is in violation of these Requirements, applicable law, and any applicable contractual undertakings.

SECTION 2: ACCESS TO BLACK DUCK DATA PROCESSED EXTERNAL TO BLACK DUCK CONTROLLED ENVIRONMENT

If Vendor (A) provides Cloud or SaaS services, or (B) provides outsourced software development services, or (C) Processes Black Duck Data external to a Black Duck controlled environment, the following provisions shall apply in addition to the provisions in Section 1 above:

2.1 Technical and Organizational Security Measures: Vendor shall have in place appropriate and reasonable Technical and Organizational Security Measures to protect the security of Black Duck Data and prevent a Data Security Breach. Upon Black Duck's written request, Vendor shall provide access to evidence that it has established and maintains Technical and Organizational Security Measures governing the Processing of Black Duck Data.

2.2 Cryptographic Controls: Vendor shall employ encryption to protect Black Duck Data during transmission across public or wireless networks. Vendor shall use Transport Layer Security (TLS) version 1.2 or higher, or substantially equivalent industry-accepted secure protocols to encrypt Black Duck Data during transmission. Vendor shall encrypt all Black Duck Data, including but not limited to, authentication credentials and cryptographic keys, at rest using AES-256 or a comparable industry-standard encryption algorithm. Vendor shall maintain up-to-date TLS certificates on all software applications that store, process, or have access to Black Duck Data or products. Vendor shall implement secure encryption key management practices,

including restricted access to keys and periodic rotation of encryption keys in accordance with industry best practices.

2.3 Access Control: Vendor shall restrict access to Black Duck Data to authorized personnel only, based on the principle of least privilege. Implement role-based access controls and ensure that access rights are reviewed regularly. Maintain logs of access to systems containing Black Duck Data and review them periodically for suspicious activity. These logs must provide an indication of system access changes and data processing activities.

2.4 Network, Operating System, and Application Control: Vendor must deploy firewalls to protect the network perimeter and internal systems that store or process Black Duck Data. Utilize intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and block malicious activity. Ensure all devices and systems are securely configured in accordance with industry best practices. Ensure that Black Duck Data is logically and physically segregated from other data to prevent unauthorized access.

2.5 Malware Protection: Where technically feasible, Vendor must deploy malware protection on all IT systems that access Black Duck Data. Vendor must ensure malware protection technology has the latest and up-to-date manufacturer's signatures, definition files, software, and patches.

2.6 Asset Management and Equipment: Vendor must have processes in place to inspect all Vendor-supplied computing or data storage equipment used in providing services to Black Duck to ensure that data is securely overwritten prior to disposal. Vendor must physically destroy storage media or overwrite information using industry standard techniques to make the original information unrecoverable (e.g., "wiped" or degaussed). Vendor shall ensure accurate and timely inventory for computing assets that perform or are connected to assets that store or have access to information associated with Black Duck.

2.7 Physical Security: Vendor must implement safeguards and controls that restrict unauthorized physical access to areas containing equipment used to access, store, or process Black Duck Data. Vendor personnel shall be required to submit a Visit Authorization Request (VAR) and obtain written approval from Black Duck prior to arriving at any Black Duck location. Only preauthorized Vendor personnel may be permitted onsite. All tools, equipment, laptops, diagnostic devices, or other materials intended to be brought onsite must be disclosed in advance as part of the VAR and approved by Black Duck prior to the visit. Vendor must implement clear desk procedures to ensure that any printed Black Duck Data is secured and protected from unauthorized access at all times.**2.8 Information Security Risk Management:** Vendor must have an established process that periodically assesses risk within the organization with respect to the possession and Processing of Black Duck Data. Vendor shall designate a security compliance officer for overseeing the implementation of Technical and Organizational Security Measures.

2.9 Password Management and Authentication Controls: Vendor must ensure that systems that Process Black Duck Data employ strong password complexity rules, including the following configurations: Passwords must be configured in a manner that is consistent with NIST guidelines or better, systems must enable system lockout after failed login attempts, and systems must enable operating system screen saver locks after a period of inactivity, and require multi-factor authentication for all systems and accounts accessing Black Duck Data. Vendor must encrypt authentication credentials during storage and transmission. Vendor must prohibit its users from sharing passwords.

2.10 System Security: Vendor must establish and maintain configuration standards to address currently known security vulnerabilities and industry standard practices for all network devices and hosts. These standards must address configuration with all applicable security parameters to prevent misuse, including but not limited to unauthorized access to data. Vendor must remove or disable non-essential functionality (i.e., hardening each system) such as scripts, drivers, features, subsystems, or file systems (e.g., unnecessary web servers, default, or sample files, etc.). Vendor must ensure that software used in operational systems maintains up-to-date patching support by its supplier.

Vendor will implement policies and procedures to apply security patches promptly to software following a change management process, including operational and regression testing.

2.11 Backup and Recovery / Disaster Recovery: Vendor must back up Black Duck Data regularly and implement a disaster recovery plan to restore systems and data in the event of a security incident or system failure. Vendor must regularly test data restoration process to ensure reliability.

2.12 Return of Black Duck Data: Unless otherwise prohibited by applicable law, Vendor shall return, delete, or destroy (at Black Duck's written election), or cause or arrange for, the return, deletion, or destruction of, all Black Duck Data subject to these Requirements, including all originals and copies of such Black Duck Data in any medium and any materials derived from or incorporating such Black Duck Data, upon the expiration or earlier termination of the agreement between Black Duck and Vendor, or when there is no longer any legitimate business need (as determined by Black Duck) to retain such Black Duck Data, or otherwise on the written instruction of Black Duck, but in no event later than ten (10) days from the date of such expiration, earlier termination, expiration of the legitimate business need, or instruction. If applicable law prevents or precludes the return or destruction of any Black Duck Data, Vendor shall notify Black Duck of such reason for not returning or destroying such Black Duck Data and shall not Process such Black Duck Data thereafter without Black Duck's express prior written consent. Vendor's obligations under these Requirements to protect the security of Black Duck Data shall survive termination of its business relationship with Black Duck.

SECTION 3: ACCESS TO CARDHOLDER DATA

If Vendor has access to Cardholder Data, whether processed in Vendor's environment or a Black Duck-controlled environment, the following provisions will apply in addition to the provisions in Sections 1 and 2 above.

3.1 Attestation of Compliance, PCI DSS: Vendor represents that it is presently in compliance, and will remain in compliance, with the current PCI DSS for protecting individual credit and debit card account numbers. Upon written request from Black Duck, Vendor agrees to provide Black Duck with a copy of its PCI DSS Attestation of Compliance.

3.2 Attestation of Compliance, PA-DSS: If Vendor provides to Black Duck software that processes any payments via a Payment Application, Vendor represents that software provided to Black Duck has been assessed and complies with the current PA-DSS and agrees to provide Black Duck with all documentation, including the PA-DSS Implementation Guide, necessary for Black Duck to deploy the software in a manner consistent with the PCI DSS. Vendor agrees to re-assess software following any changes determined to impact payment application security in accordance with the PA-DSS, provide updated documentation as necessary, and immediately notify Black Duck of any change in its PA-DSS compliance status.

SECTION 4: DEFINITIONS

For purposes of these Requirements, the following definitions shall apply:

"Black Duck Data" means any non-public information which is commercially valuable, proprietary, privileged, or personal, the unauthorized disclosure of which could adversely affect Black Duck and/or its employees (e.g., competitively, by waiver of legal privilege, monetary loss, or violation of law or right of privacy). Black Duck Data includes Personal Data of employees, contractors, customers, or potential customers of Black Duck, any classified information Black Duck receives in connection with participation in government programs, and any data the unauthorized disclosure of which could cause significant harm to Black Duck or the individual to whom the information pertains.

"Cardholder Data" has the same meaning as defined by the PCI DSS.

"Data Security Breach" means: (A) the loss or misuse arising out of Vendor's internal use, Processing or other transmission (by any means) of Black Duck Data, including, without limitation any unauthorized access or disclosure to unauthorized individuals; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Black Duck Data; or (C) any other act or omission that compromises the confidentiality, integrity, or availability of Black Duck Data. Data Security Breach includes, without limitation, a breach resulting from or arising out of Vendor's internal use, Processing or other transmission of Black Duck Data, whether between or among Vendor's subsidiaries and affiliates or any other person or entity acting on behalf of Vendor.

"PA-DSS" means Payment Application Data Security Standard 2.0, its supporting documentation and any subsequent version(s) of said standard published by the PCI Security Standards Council or its successor(s).

"Payment Application" means any application that stores, processes, or transmits cardholder data as part of authorization or settlement.

"**PCI-DSS**" means the current version of the Payment Card Industry (PCI) Data Security Standard (DSS), its supporting documentation and any subsequent version(s) of said standard published by the PCI Security Standards Council or its successor(s).

"Processing" or "**Process**" means any operation or set of operations that is performed upon Black Duck Data, whether by automatic means or not, including without limitation collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, blocking, deletion, erasure, or destruction.

"Technical and Organizational Security Measures" means security measures, consistent with the sensitivity of the Black Duck Data being Processed and the services being provided by Black Duck, to protect Black Duck Data, which measures shall implement industry recognized protections and may include, as applicable, physical, electronic and procedural safeguards to protect Black Duck Data supplied to Black Duck against any Data Security Breach, and any security requirements, obligations, specifications, or event reporting procedures set forth in any agreement between Vendor and Black Duck.