Bitdefender

COMPLIANCE, CONFIDENTIALITY AND INFORMATION SECURITY REQUIREMENTS

These requirements shall apply to all Bitdefender Clients, Providers and Partners ("Partners")

COMPLIANCE

Partner represents, warrants and agrees that it shall comply with all applicable international, national, governmental, quasi-governmental and local law and regulations including, without limitation, data protection, privacy and import and export, anti-bribery compliance laws and regulations ("Law") in performing its duties or exercising its rights hereunder and also assure that, in connection with the performance of its obligations pursuant to this Agreement.

The Partner shall indemnify and hold harmless Bitdefender from and against any claim, proceeding, action, fine, loss, cost and damages arising out of or in relation to any noncompliance.

Bitdefender is committed to the principle of equal employment opportunity and value diversity among its employees. Consistent with Bitdefender's values and in accordance with applicable law, Bitdefender is committed to create and maintain a work environment in which all employees are treated with dignity and respect and which is free from all forms of harassment. Bitdefender expects Partners to share its commitment to these principles.

Therefore, Partners shall:

- Not engage in discrimination in hiring, compensation, access to training, promotion, termination or retirement based on race, religion, color, national origin, ancestry, physical or mental disability, medical condition, marital status, veteran status, age, sex or sexual orientation, gender identity or any other protected criteria in any employment decision.
- Provide a safe and healthy work environment and fully comply with all applicable safety and health laws, regulations and practices. Adequate steps shall be taken to minimize the causes of hazards inherent in the working environment.
- Use only voluntary labor. The use of forced labor whether in the form of indentured labor, bonded labor, or prison labor by a Partner and/or its subcontractors is strictly prohibited.

- Comply with all local minimum working age laws and requirements and not utilize child labor. Employees shall not be under the legal minimum working age of the respective region or shall not be less than 16 years of age (whichever is higher).
- Not require workers to work more than the maximum hours of daily labor set by local laws; ensure that overtime is voluntary and paid in accordance with local laws and regulations.
- Keep employee records in accordance to local and/or national regulations.

Partner represents and warrants that in connection with the Agreement with Bitdefender, it has not and will not make any payments or gifts or any offers or promises of payments or gifts of any kind, directly or indirectly, to any official of any foreign government or any agency or instrumentality thereof and (ii) it will comply in all respects with the with all applicable laws, statutes, regulations, and codes relating to anti-bribery and anti-corruption.

CONFIDENTIALITY

Partner shall not disclose any confidential and/or proprietary information belonging to the Bitdefender unless agreed in writing by Bitdefender. This obligation shall not apply to information received which: (i) is or becomes known by the Partner without an obligation to maintain its confidentiality; (ii) is or becomes generally known to the public through no act or omission on the part of the Partner; or (iii) is independently developed by the Partner without the use of confidential or proprietary information. In the event that Partner is required to disclose confidential and proprietary information pursuant to law, it shall notify the other Party of the required disclosure.

Bitdefender's Confidential and/or Proprietary Information includes, without limitation: (i) any and all information, whether in oral, written or other tangible form, disclosed by Bitdefender to Provider whether or not such Confidential and / or Proprietary Information is designated as confidential or proprietary or would reasonably be understood to be confidential or proprietary; (ii) any of Bitdefender's Product, Modules, Source Code, software, know how, methodologies, business strategies, trade secrets, know-how, protocols, pricing information, processes, technologies, tools, support manuals; (iii) Bitdefender Customer personal information and any compilations thereof and (vi) the terms, conditions and existence of an agreement or a potential agreement with Bitdefender.

These provisions shall be considered replaced by any obligation of confidentiality that is more restrictive and subject to a separate agreement with Bitdefender.

Bitdefender

BITDEFENDER INFORMATION SECURITY

I. Security

I.1 The Partner shall guarantee appropriate technical and organizational measures to ensure standard industry security measures and best practices or procure applicable certifications such as ISO 27001 and SOC 2 Type II, unless otherwise agreed by Bitdefender.

I.2 In assessing the appropriate level of security, the Partner shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing data as well as the risk of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed for Bitdefender. The Partner shall be liable for any person natural or legal acting under its authority and with access to Bitdefender data, and shall take steps to ensure that any such person is bound by enforceable contractual or statutory confidentiality obligation.

A. Personnel

(A1.1) Upon hire, employees that have access to Bitdefender data and information systems must acknowledge that they read and agree to a code of conduct that describes their responsibilities and expected behaviour regarding data and information system usage. Employees are required to sign a confidentiality agreement upon hire. This agreement prohibits any disclosure of information and other data to which the employee has been granted access.

New personnel offered employment are subject to background checks or equivalent internal screening prior to their start date.

(A1.2) Management has established defined roles and responsibilities to oversee implementation of security and the control environment and report any issues to the board of directors.

(A1.3) Partner shall implement controls reasonably necessary to prevent unauthorized use, disclosure, loss, acquisition of, or access to the company data. This includes, but is not limited to personnel security measures, such as background checks and clear job description for employees managing Bitdefender's data, as well as providing evidence upon request of its employees completing an annual Information Security Awareness course.

(A1.4) The Partner security responsible subscribes to industry security bulletins and email alerts and uses them in order to monitor the impact of emerging technologies and security on the in-scope production systems.

B. Physical Security

(B1.1) The Partner shall implement appropriate physical controls to prevent unauthorized physical access, damage, or interference to the working environment and the information processing facilities used by the Partner, its affiliates, and subcontractors to access, process, transmit, or store Bitdefender Data, including badge access requirements, visitor and access logs, security alarm system(s), CCTVs, and other measures.

C. Logical and Information Security

(C1.1) Authentication to the Partner's systems require unique usernames and passwords with MFA or authorized Secure Shell (SSH) keys, with privileged access to the production systems restricted only to authorized users with a clear business need and if it's part of their job description.

The network must be segmented to prevent unauthorized access to customer data, with access to firewalls restricted only to authorized network administrators and with periodic firewall rules review. No port must be allowed to be exposed directly on the public internet without a documented justification, and any remote access must use Multi Factor Authentication.

(C1.2) Antimalware and Intrusion Detection and Prevention systems must be used to provide continuous monitoring of the Partner's network and early detection of potential security breaches, together with a file integrity monitoring (FIM) tool that is used to notify system administrators of potential unauthorized changes to the production systems.

(C1.3) All of Bitdefender's data managed by the Partner must be encrypted while at rest (on systems or on portable and removable media) or in transit by industry standard mechanisms and algorithms, with periodic key rotations, and a clear inventory of all systems where such data is kept or processed must exist.

The Partner shall identify all the datacenters or locations where the data at rest or backups will reside and all datacenters or locations must be guaranteed to reside within the contracted regions.

(C1.4) Configuration of Partner's systems should not be manual but rather through a configuration management tool to ensure that system configurations are deployed consistently throughout the environment and to further mitigate the risk of human errors.

The Partner's network and system hardening standards must be documented, should be based on industry's best practices and must be reviewed at least annually.

In addition, a formal systems development life cycle (SDLC) methodology must be in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. All systems must be updated to the latest available versions, with Critical and High patches being applied no longer than one week since release.

(C1.5) The Partner must have annually reviewed documented formal procedures that outline the process its staff follows to perform access control functions like adding of new users, modifying an existing user's access and removing an existing user's access.

Termination checklists must be completed to track employee terminations, and access must be revoked for employees within 24 hours at most as part of the termination process.

Documented user access reviews are conducted by management for systems or system components managing Bitdefender's data to help ensure that access is restricted appropriately, with tickets being created to add, remove or modify access as necessary in a timely manner.

D. Vulnerability and Incident Management

(D1.1) The Partner must establish and maintain a vulnerability management and penetration testing program for all information systems that process, transmit, or store Bitdefender data. The program must be designed to prevent exploitation of vulnerabilities by continuous monitoring and mitigation of vulnerabilities.

(D1.2) The program must include periodic security audits of these systems via vulnerability scanning, penetration testing, vulnerability assessments and vulnerability remediation coupled with system and application patching.

(D1.3) Internal and external network vulnerability scans must be performed quarterly and remediation plans with required changes will be implemented to remediate all critical and high vulnerabilities at a minimum.

The Partner shall have the final form of their software reviewed for security flaws, ideally by an independent organization that specializes in application security, prior to delivery. The Partner warrants that the system is free of and does not contain any code or mechanism that collects personal information or asserts control of the system without Bitdefender's consent, or which may restrict Bitdefender's access to or use of its data. Partner further warrants that it will not introduce, via any means, spyware, adware, ransomware, rootkits, keyloggers, viruses, trojans, worms, or other code or mechanisms designed to

permit unauthorized access to Bitdefender's data, or which may restrict Bitdefender's access to or use of its data.

(D1.4) The Partner must ensure that security events are logged, tracked, resolved, and communicated to affected parties by management according to the Partner's security incident response policies and procedures. All events must be evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.

The Partner shall notify Bitdefender's designated contact of any known Security Vulnerability involving Bitdefender's data or in scope solutions managed by the Partner immediately after it becomes aware but no later than 48 hours after discovery. The Partner agrees to cooperate with Bitdefender in the investigation and analysis of the vulnerabilities, and to further take appropriate remedial action with respect to the integrity of its security systems and processes.

(D1.5) The Partner must have an incident response plan that must be tested by at least annually. Security incident response policies and procedures must be documented and communicated to authorized users by the Partner.

E. Risk Management

(E1.1) A risk assessment must be performed by the Partner at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to the in-scope service commitments are identified and the risks are formally assessed. The risk assessment should also include a consideration of the potential for fraud and how fraud may impact the service.

(E1.2) A Partner management program must also be in place, with components that must include maintaining a list of critical third-party Partners, requirements for third-party Partners to maintain their own security practices and procedures and annually reviewing critical third-party attestation reports or performing a Partner risk assessment.

II. Availability

II.1 The Partner must have a documented business continuity/disaster recovery (BC/DR) plan that is tested annually. Upon request the Partner shall provide the results of the latest BC/DR test results. To further ensure availability, the Partner must have daily incremental and weekly full backups for data stores housing Bitdefender's data. Formal procedures that outline the process the Partner's staff follows to back up and recover customer data must be documented.

II.2 It is highly recommended that the Partner's production systems utilize cloud hosted virtualized infrastructure to allow for increased capacity upon demand.

II.3 The Partner must continuously evaluate the capacity and ensure system changes are implemented to help ensure processing capacity can meet demand and that availability is ensured. To this end, a log management tool must be utilized to log access and identify trends that may have a potential impact on the Partner's ability to achieve its availability and security objectives.

III. Processing Integrity

III.1 The Partner must have policies or procedures which ensure that Bitdefender's data is prohibited from being used or stored in non-production systems or environments and must also ensure that data containing confidential information is purged or removed from the application environment in accordance with best practices when the contract ends.

IV. Confidentiality & Security Breaches

IV.1 If the Partner becomes aware our data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms herein or the contract with Bitdefender, then the Partner must alert us of any data breach within a maximum of 24 hours, and shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the data breach.

IV.2 The Partner must immediately correct any data breach and shall devote such resources as may be required to accomplish that goal, while providing Bitdefender with updates every 6 hours at most. After resuming normal operations, the Partner shall provide a full report about the breach to allow Bitdefender to fully understand the nature and scope of the data breach.