Bitdefender

Bitdefender Supplier Information Security Requirements

I. Security

I.1 The Supplier 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.

I.2 In assessing the appropriate level of security, the Supplier 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 Supplier 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 behavior 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) Supplier 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 Supplier 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 Supplier 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 Supplier, 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 Supplier'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 Supplier'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 Supplier 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 Supplier 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 Supplier'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 Supplier'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 Supplier 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 Supplier 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 Supplier 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 Supplier 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. Supplier 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 Supplier must ensure that security events are logged, tracked, resolved, and communicated to affected parties by management according to the Supplier'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 Supplier shall notify Bitdefender's designated contact of any known Security Vulnerability involving Bitdefender's data or in scope solutions managed by the Supplier immediately after it becomes aware but no later than 48 hours after discovery. The Supplier 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 Supplier 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 Supplier.

E. Risk Management

(E1.1) A risk assessment must be performed by the Supplier 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 Supplier management program must also be in place, with components that must include maintaining a list of critical third-party Suppliers, requirements for third-party Suppliers to maintain their own security practices and procedures and annually reviewing critical third-party attestation reports or performing a Supplier risk assessment.

II. Availability

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

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

1.3 The Supplier 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 Supplier's ability to achieve its availability and security objectives.

III. Processing Integrity

1.1 The Supplier 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.

Bitdefender

IV. Confidentiality & Security Breaches

1.1 If the Supplier becomes aware our data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this agreement or the contract, then the Supplier 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.

1.2 The Supplier 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 Supplier shall provide a full report about the breach to allow Bitdefender to fully understand the nature and scope of the data breach.