KASPERSKY SECURITY NETWORK (KSN) STATEMENT - Kaspersky Endpoint Security 11 for Windows Kaspersky Security Network Statement (hereinafter “KSN Statement”) relates to the computer program Kaspersky Endpoint Security (hereinafter “Software”). KSN Statement along with the End User License Agreement for Software, in particular in the Section “Conditions regarding Data Processing” specifies the conditions, responsibilities and procedures relating to transmission and processing of the data, indicated in the KSN Statement. Carefully read the terms of the KSN Statement, as well as all documents referred to in the KSN Statement, before accepting it. When the End User activates the using of the KSN, the End User is fully responsible for ensuring that the processing of personal data of Data Subjects is lawful, particularly, within the meaning of Article 6 (1) (a) to (1) (f) of Regulation (EU) 2016/679 (General Data Protection Regulation, “GDPR”) if Data Subject is in the European Union, or applicable laws on confidential information, personal data, data protection, or similar thereto. Data Protection and Processing Data received by the Rightholder from the End User during use of the KSN are handled in accordance with the Rightholder’s Privacy Policy published at: www.kaspersky.com/Products-and-Services-Privacy-Policy. Purpose of Using the KSN Use of the KSN could lead to increase the effectiveness of protection provided by the Software, against information and network security threats. The declared purpose is achieved by: - determining the reputation of scanned objects; - identifying information security threats that are new and challenging to detect, and their sources; - taking prompt measures to increase the protection of the data stored and processed by the End User with the Computer; - reducing the likelihood of false positives; - increasing the efficiency of Software components; - preventing information security incidents and investigating incidents that did occur; - improving the performance of the Rightholder’s products; - receiving reference information about the number of objects with known reputation. Processed Data During use of the KSN, the Rightholder will automatically receive and process the following data: - information about files and URL addresses to be scanned: checksums of the scanned file (MD5, SHA2-256, SHA1) and file patterns (MD5), the size of the pattern, type of the detected threat and its name according to Rightholder’s classification, identifier for the anti-virus databases, URL address for which the reputation is being requested, as well as the referrer URL address, the connection’s protocol identifier and the number of the port being used; - information about the results of categorization of the requested web-resources, which contains the processed URL and IP address of the host, the version of the Software’s component that performed the categorization, the method of categorization and set of the categories defined for the web-resource; - the identifier of the scan task which detected the threat; - information about digital certificates being used needed to verify their authenticity: the checksums

(SHA2-256) of the certificate used to sign the scanned object and the certificate's public key; - information about the software installed on the Computer: name of the software applications and software vendors, registry keys and their values, information about files of the installed software components (checksums (MD5, SHA2-256, SHA1), name, path to the file on the Computer, size, version and the digital signature), information about kernel objects, drivers, services, Microsoft Internet Explorer extensions, printing system extension, Windows Explorer extensions, Active Setup elements, control panel applets, entries in the hosts file and system registry, versions of browsers and mail clients; - information about the state of the Computer's anti-virus protection: the versions and the release timestamps of the anti-virus databases being used, statistics about updates and connections with Rightholder's services, job identifier and the identifier of the Software component performing scanning; - information about files being downloaded by the End User: the URL and IP addresses of the download and the download pages, download protocol identifier and connection port number, the status of the URLs as malicious or not, file's attributes, size and checksums (MD5, SHA2-256, SHA1), information about the process that downloaded the file (checksums (MD5, SHA2-256, SHA1), creation/build date and time, autoplay status, attributes, names of packers, information about signatures, executable file flag, format identifier, and entropy), file name and its path on the Computer, the file's digital signature and timestamp of its generation, the URL address where detection occurred, the script's number on the page that appears to be suspicious or harmful, information about HTTP requests generated and the response to them; - information about the running applications and their modules: data about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the sign of trusted program or process, the full path to the process's files, and the starting command line, level of the process's integrity, a description of the product that the process belongs to (the name of the product and information about the publisher), as well as digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes (their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them on the Computer), PE-file header information, names of packers (if the file was packed); - information about all potentially malicious objects and actions: the name of the detected object and the full path to the object on the Computer, checksums (MD5, SHA2-256, SHA1) of the files being processed, detection date and time, names and size of infected files and paths to them, code of the path template, the flag indicating whether the object is a container, names of packers (if the file was packed), file

type code, file format identifier, list of the activities of malicious applications and associated decisions made by the Software and the End User, identifiers for the anti-virus databases the Software used to make a decision, name of the detected threat according to the Rightholder's classification, level of the danger, the status and method of the detection, reason for including a file in the analyzed context and the file's serial number in the context, checksums (MD5, SHA2-256, SHA1), name and attributes of the executable file for the application that passed the infected message or link, anonymized IP address (IPv4 and IPv6) of the blocked object's host, the file's entropy, autoplay status, time of the file's first detection in the system, number of times the file has been run since the last time statistics were sent, information about the name, checksums (MD5, SHA2-256, SHA1) and size of the mail client used to receive the malicious object, job identifier of the software that performed the scan, flag of the reputation verification or file signature verification, result of processing the file, checksum (MD5) of the pattern collected on the object and pattern size in bytes, technical parameters of the applicable detection technologies; - information about scanned objects: the assigned trust group to which and/or from which the file has been placed, the reason the file was placed in that category, category identifier, information about the source of the categories and the version of the category database, the file's trusted certificate flag, name of the file's vendor, file version, name and version of the software application which includes the file; - information about vulnerabilities detected: the vulnerability ID in the database of vulnerabilities, the vulnerability danger class, and the status of detection; - information about emulation of the executable file: file size and its checksums (MD5, SHA2-256, SHA1), the version of the emulation component, emulation depth, an array of properties of logical blocks and functions within logical blocks obtained during the emulation, data from the executable file's PE headers; - information about network attacks: the IP addresses of the attacking computer (IPv4 and IPv6), the number of the port on the Computer that the network attack is directed at, identifier of the protocol of the IP packet containing the attack, the attack's target (organization name, website), flag for the reaction to the attack, the attack's weight, trust level; - information about attacks associated with spoofed network resources, the DNS and IP addresses (IPv4 and IPv6) of visited websites; - DNS and IP addresses (IPv4 or IPv6) of the requested web-resource, information about the file and web-client requesting the web-resource, name, size, checksums (MD5, SHA-256, SHA1) of the file, its full path and the code of the template of the path, the result of the digital signature verification and its status according to the KSN; - information about the rolling back of malware's activities: data about the file whose activities are being rolled back (file name, full path to the file, its size and checksums (MD5, SHA2-256, SHA1)), data about successful and unsuccessful actions to delete, rename, and

copy files and restore values in the registry (names of registry keys and their values), information about system files changed by malware, before and after the roll back; - information about the modules loaded by the Software: name, size and checksums (MD5, SHA2-256, SHA1) of the module file, its full path and template code of the file path, parameters of the module file's digital signature, timestamp of the signature generation, names of the subject and the organization that signed the module file, identifier of the process, in which the module was loaded, name of the module vendor, index number of the module in the load queue; - service information about the Software's operation: the compiler version, flag for the potential maliciousness of the scanned object, version of the set of statistics being sent, information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent, flag indicating whether the software is operating in interactive mode; - if a potentially malicious object is detected, information is provided about data in the processes' memory: elements of the system object hierarchy (ObjectManager), data in UEFI BIOS memory, names of registry keys and their values; - information about events in the systems logs: the event's timestamp, the name of the log in which the event was found, type and category of the event, name of the event's source and the event's description; - information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening; - information about the date of installation and activation of the Software on the Computer: type of the installed license and its expiration date, identifier of the partner from whom the license was purchased, license serial number, type of the Software installation on the Computer (initial installation, updating, etc.) and an installation success flag or the installation error number, a unique identifier for the installation of the Software on the Computer, type and identifier of the application that is being updated, identifier of the update job; - information about the set of all installed updates, and the set of most recently installed/removed updates, the type of event that caused the update information to be sent, duration since the installation of last update, information about any currently installed anti-virus databases; - information about the Software operation on the Computer: CPU usage data, memory usage data (Private Bytes, Non-Paged Pool), the number of the Software's active threads and threads in wait state, the duration of the Software operation before the error occurred; - number of software dumps and system dumps (BSOD) since the Software was installed and since the time of the last update, the identifier and version of the Software module that crashed, the memory stack in the Software's process, and information about the anti-virus databases at the time of the

crash; - data on the system dump (BSOD): a flag indicating the occurrence of the BSOD on the Computer, the name of the driver that caused the BSOD, the address and memory stack in the driver, a flag indicating the duration of the OS session before the BSOD occurred, memory stack of driver that crashed, type of stored memory dump, flag for the OS session before BSOD lasted more than 10 minutes, unique identifier of the dump, timestamp of the BSOD; - information about errors that occurred during operation of the Software components: the status ID of the Software, the error type, code and time of occurrence, the IDs of the component, module and process of the product in which the error occurred, the ID of the task or update category during which the error occurred, logs of drivers used by the Software (error code, module name, name of the source file and the line where the error occurred), identifier of the method to identify an error in the Software operation, name of the process that initiated interception or traffic exchange which led to an error in the Software operation; - information about updates of anti-virus databases and Software components: the name, date and time of index files downloaded during the last update and being downloaded during the current update, as well as the date and time of completion of the last update, names of the files of updated categories and its checksums (MD5, SHA2-256, SHA1); - information about abnormal termination of the Software operation: the creation timestamp of the dump, its type, the name of the process linked to the dump, the version and send time of the statistics dump, type of event that caused the abnormal termination of the Software operation (unexpected power-off, third-party application crash, errors of interception processing), date and time of the unexpected power-off; - information about third-party applications that caused the error: their name, version and localization, the error code and information about the error from the system log of applications, the address of the error and memory stack of the third-party application, a flag indicating the occurrence of the error in the Software component, the length of time the third-party application was in operation before the error occurred, checksums (MD5, SHA2-256, SHA1) of the application process image, in which the error occurred, path to the application process image and template code of the path, information from the system log with a description of the error associated with the application, information about the application module, in which an error occurred (exception identifier, crash memory address as an offset in the application module, name and version of the module, identifier of the application crash in the Rightholder’s plugin and memory stack of the crash, duration of the application session before crash); - version of the Software updater component, number of crashes of the updater component while running update tasks over the lifetime of the component, ID of the update task type, number of failed attempts of the updater component to complete update tasks; - information about operation of the Software system

monitoring components: full versions of the components, code of the event that overflowed the event queue and number of such events, the total number of queue overflow events, information about the file of the process of the initiator of the event (file name and its path on the Computer, template code of the file path, checksums (MD5, SHA2-256, SHA1) of the process associated with the file, file version), identifier of the event interception that occurred, the full version of the interception filter, identifier of the type of the intercepted event, size of the event queue and the number of events between the first event in the queue and the current event, number of overdue events in the queue, information about the file of the process of the initiator of the current event (file name and its path on the Computer, template code of the file path, checksums (MD5, SHA2-256, SHA1) of the process associated with the file), duration of the event processing, maximum duration of the event processing, probability of sending statistics; - information about the last unsuccessful OS restart: the number of unsuccessful restarts since OS installation, data on the system dump (code and parameters of an error, name, version and checksum (CRC32) of the module that caused an error in the OS operation, error address as an offset in the module, checksums (MD5, SHA2-256, SHA1) of the system dump); - information to verify authenticity of digital certificates being used to sign files: the certificate's fingerprint, the checksum algorithm, the certificate's public key and serial number, the name of the issuer of the certificate, the result of certificate validation and the certificate's database identifier; - information about the process executing the attack on the Software's self-defense: the name and size of the process file, its checksums (MD5, SHA2-256, SHA1), the full path to the process file and the template code of the file path, the creation/build timestamps, executable file flag, attributes of the process file, information about the certificate used to sign the process file, code of the account used to launch the process, ID of operations performed to access the process, type of resource with which the operation is performed (process, file, registry object, FindWindow search function), name of resource with which the operation is performed, flag indicating success of the operation, the status of the file of the process and its signature according to the KSN; - information about the Rightholder's Software: its full version, type, locale language and operation state, version of the installed Software components and their operation state, information about the installed updates, the value of the TARGET filter, the version of the protocol used to connect with the Rightholder's services; - information about hardware installed on the Computer: type, name, model name, firmware version, parameters of built-in and connected devices, the unique identifier of the Computer with the installed Software; - information about the versions of the operating system and installed updates, the word size, edition and parameters of the OS run mode, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file. Also, in order to achieve the

declared purpose of increasing the effectiveness of protection provided by the Software, the Rightholder may receive objects that could be exploited by intruders to harm the Computer and create information security threats. Such objects include: - executable and non-executable files or their parts; - portions of the Computer's RAM; - sectors involved in the process of booting the OS; - network traffic data packets; - web pages and emails containing suspicious and malicious objects; - description of the classes and instances of classes of the WMI repository; - application activity reports. Such application activity reports contain the following data about files and processes: - the name, size and version of the file being sent, its description and checksums (MD5, SHA2-256, SHA1), file format identifier, the name of the file's vendor, the product name to which the file belongs, full path on the Computer, template code of the file path, the creation and modification timestamps of the file; - start and end date/time of the validity period of the certificate (if the file has a digital signature), the date and the time of the signature, the name of the issuer of the certificate, information about the certificate holder, the fingerprint, the certificate's public key and appropriate algorithms, and the certificate's serial number; - the name of the account from which the process is running; - checksums (MD5, SHA2-256, SHA1) of the name of the Computer on which the process is running; - titles of the process windows; - identifier for the anti-virus databases, name of the detected threat according to Rightholder's classification; - data about the installed license, its identifier, type and expiration date; - local time of the Computer at the moment of the provision of information; - names and paths of the files that were accessed by the process; - names of registry keys and their values that were accessed by the process; - URL and IP addresses that were accessed by the process; - URL and IP addresses from which the running file was downloaded. Also, in order to achieve the declared purpose with respect to preventing false positives, the Rightholder may receive trusted executable and non-executable files or their parts. Providing the above information to the KSN is voluntary. After installing the Software, the End User can at any time enable or disable the use of the KSN in the Software settings as described in the User Manual. 