Kaspersky Labs Limited (the "Company"), a private company limited by shares, and its subsidiaries (together referred to as the "Group" or "Kaspersky") comprise of private limited companies in accordance with The Companies Act 2006 located in the UK, as well as companies located in Russia, Switzerland, Germany, France, United States of America (the "US"), China, Germany, France and other countries.

Kaspersky is one of the world's largest privately-owned cybersecurity companies, with the company registered in the United Kingdom.

The Group was founded in 1997 and today it is an international group operating in almost 200 countries and territories worldwide. It has 34 representative territory offices in more than 30 countries. Kaspersky has a corporate client base of more than 250,000 companies located around the globe, ranging from small and medium-sized businesses to large governmental and commercial organizations. Over 400 million people worldwide are protected by Kaspersky products and technologies. Kaspersky currently employs more than 4,000 qualified specialists. Approximately, forty six percent of Kaspersky's employees are R&D specialists.

The Group's portfolio encompasses solutions to suit a wide range of customers, protecting consumers, small companies, medium-sized businesses and enterprises from different types of threats and provides them with convenient tools to control and manage their security.

Kaspersky empowers consumers with a range of products to protect all corners of their lives from cybercrime. It understands the needs of small businesses and has a unique multi-layered solution especially for them, which unites ease of management and effective protection. The Group covers all the cybersecurity needs of large enterprises with its full enterprise platform that helps to prevent all types of cyberthreats, detects even the most sophisticated attacks, responds to security incidents and predicts the evolution of the threat landscape. The Group's comprehensive portfolio of solutions achieves all of this thanks to the combination of our expertise, threat intelligence and machine learning that enables us to develop robust technologies to detect, block and prevent cyberattacks. The business focus of Kaspersky is continuing to evolve from "cybersecurity" towards the wider concept of "cyber-immunity".

The Group's most valuable asset is the wealth of expertise it has gained in its years of combating major IT threats. Kaspersky's Global Research and Analysis Team (GReAT) is an elite group of more than forty leading security experts who operate all over the world and provide leading anti-threat intelligence and research. The team is well-known for the discovery and dissection of some of the world's most sophisticated threats, including cyber-espionage and cyber-sabotage threats.

To record the groundbreaking malicious cyber-campaigns that have been investigated by GReAT, Kaspersky launched a Targeted Cyberattack Logbook. Although our key expertise is related to cyberthreats, we fight against them not only to ensure that our customers are protected now, but so that our solutions are also ready for new challenges in the future.

The Group's commitment to its customers as well as advanced technology ensure its competitiveness. The Group has been named a Leader in the evaluation of Wave Endpoint Security and a Strong Performer in an evaluation of Cloud Security Solutions by analyst firm Forrester. Kaspersky is also firmly positioned as one of the top five leading endpoint security vendors. For the third time in a row, the company was recognized as a Gartner Peer Insights Customers' Choice for the Endpoint Protection Platforms in 2019.

Management believes that a joint effort is the most effective way to fight cybercriminals. To this end, the Group shares its expertise, knowledge and technical findings with the world's security community. It takes part in joint cyberthreat investigations with such companies as Adobe, AlienVault Labs, Novetta, CrowdStrike, OpenDNS and others. Kaspersky was included in the list of Vulnerability Top Contributors by Microsoft.

Kaspersky cooperates with INTERPOL in the joint fight against cybercrime. The company provides the organization with human resources support, training, and threat intelligence data on the latest cybercriminal activities. Other partners in the field of law enforcement include, but are not limited to, Europol, The City of London Police, The National High Tech Crime Unit (NHTCU) of the Netherlands' National Police Corps, and the Microsoft Digital Crimes Unit, as well as Computer Emergency Response Teams (CERTs) and many other police authorities worldwide.

By joining forces, the Group helped fighting cybercrime (such as the Carbanak case), disrupt criminal botnets (for example, Simda), and launch new initiatives (such as No More Ransom, with more than 100 supporting partners from the public and private sector). The Group takes part in joint cyberthreat investigations and conducts trainings for cybersecurity specialists. Collaboration between the Dutch police and Kaspersky led to the arrest of suspects behind the CoinVault ransomware attacks.

Kaspersky is involved in the discussion and development of cybersecurity initiatives and standards through its advisory group memberships (i.e. the Anti-Malware Testing Standards Organization). Aiming to solve the cyber security challenges faced by the modern world today, Kaspersky is also a member of initiatives and organizations such as Securing Smart Cities and the Industrial Internet Consortium.

The key market in which the Group operates is endpoint security. It encompasses products that are designed to protect endpoints from attack or to protect information residing on endpoints, both physical and virtual, regardless of operating system type — including Windows, Linux, Mac OS, iOS, and Android. Endpoint security products provide security using or leveraging an endpoint agent or client as a core or fundamental component. Functionality includes client antimalware software, file/storage server antimalware, personal firewall software, host intrusion prevention software, file/disk encryption, whitelisting, patch management, desktop URL filtering and endpoint data loss prevention. The endpoint security category covers both corporate and consumer products. Global corporate and consumer markets are growing approximately at 8% and 2% per year.

Key drivers of the endpoint security market include the following:

- The continual growth in the sophistication of cyberattacks, the growth in the volume of cyberattacks, and the corresponding press associated with such attacks continue to fuel awareness in the minds of consumers. As threats and awareness grow, the likelihood of moderate increases in penetration and/or average selling price increases for consumer security software grows.

- The drive to a single agent. Agents have become an acute problem for many organizations, as many report endpoints with seven or eight security agents and 25-30 agents total, which can bring system performance to a crawl. The security industry has responded with minimization / consolidation of agents – an improvement in which IT security departments are willing to invest.

- Modern endpoint security adoption - technology is finding its way from corporate solutions to consumer solutions. Leveraging specialized threat analysis and protection of intellectual property in consumer offerings allows vendors to further monetize their intellectual property investments. In parallel, larger expenditures on the business side are being driven by heightened adoption of sophisticated EDR solutions and security services tightly integrated therein.

- As vendors look to differentiate their offerings, the endpoint security product definition is expanding. Rather than focus on the narrow definition of stopping malware, market messages and product features increasingly focus on concepts of "safety" and "performance," thus attracting more consumer spend.

Endpoint security market inhibitors include the following:

- Organizational expenses related to IT security continue to increase and often constitute a serious financial burden for businesses.

- A decrease in the global consumer PC install base effectively reduces the addressable consumer market.

- Lack of metrics by which endpoint products can be differentiated continues to be an inhibitor to the industry. Endpoint vendors are challenged to quantify "safe" in a manner from which consumers can

make informed cost/benefit analyses. While enterprise buyers are challenged, consumers can be lost at times.

The other key markets where Kaspersky is present are:

- Web security – web security products are deployed on software, appliance, SaaS, and virtual platforms. The submarkets of the web security products include URL filtering, web antimalware, web application firewall, and web content filtering products. Selected data loss prevention technologies can be included in web security as well. Web security products protect against both inbound (malware) and outbound (data leakage) threats. This market grows at 8% per year.
- Messaging security – messaging security solutions are deployed on all security platforms. This market includes three submarkets: antispam, antimalware, and content filtering. Messaging security can also contain selected data loss prevention, alongside selected information protection and control technologies. These products are designed to work with applications, including email, instant messaging (IM), and other collaborative applications. This market grows at 6% per year.
- Threat Intelligence Services – services for provision of information about potential cyber threats, including existing and emerging threats, cybercrime actors, tools and methods. This information can be used to inform decisions regarding the client's response to those menaces / hazards. Threat intelligence is made available through portals, online delivered feeds, subscription-based analyst personnel support and platform software. This market grows at 10% per year.
- Hybrid Cloud Security (Cloud Workload Protection) – workload-centric security protection solutions addressing the unique requirements of server workload protection in modern hybrid datacenter architectures that span on-premises, physical and virtual machines (VMs) and multiple public cloud infrastructure-as-a-service (IaaS) environments. This market grows at 15% per year.
- Industrial Cybsersecurity – Security solutions (and accompanying services) for industrial control systems' networks and nodes. This market grows at 14% per year.

The Group also extends its product portfolio in Security Services (Managed Detection and Response, Threat Hunting, Security Assessment), Anti-DDoS Protection, Online Fraud Prevention, Anti-Targeted Attacks, EDR (Endpoint Detection & Response), and Embedded Systems Security).

The Company operates in a market where technology plays a key role. The Company's fellow subsidiaries manages this risk by investing substantial resources in research and development activities, including those, which are related to ensuring product quality, as well as in legal substantiation of its intellectual property rights.

Statement by the Directors in performance of their statutory duties in accordance with s172 Companies Act 2006

The Directors consider the following issues, factors and stakeholders relevant in complying with section 172 (1) (a) to (f):

Regard to the likely consequences of decisions in the long term

The 2020 budget which was approved in 2019 places focus on the Company's profitability, which is meant to be achieved through a combination of revenue growth and efficient spending in strategically important directions.

No dividends were declared during 2019, which is aimed at building the retained earnings for implementing the Company's strategy.

Regard to the interests of the company's employees

Employee remuneration is reviewed on an annual basis to ensure that it is at a fair market level. Employee remuneration amounted in 2019 to 49% of the Group's operating expenses (2018: 48%). Employee involvement and commitment to the success of the business is an important element of the Company's culture. Management conducts regular communications and consultations with employees on key aspects

of the Company's activities in the form of e-mail communications, annual meetings and informal events. A significant portion of employees bonuses depend on the financial performance of the business unit that they belong to and/or Kaspersky Group as a whole. An annual review of employee compensation is performed to support the business strategy of profitable revenue growth, which should in turn provide interesting and fulfilling work and the prospect of a higher future remuneration if the strategy is successfully achieved. The Group hiring policies stipulate full and fair consideration to applications for employment made by disabled persons, having regard to their particular aptitudes and abilities. We provide continuing employment to those employees who become disabled during their employment with the Group, and provide training, career development and promotion to disabled employees, where appropriate.

Regard to the need to foster the company's business relationships with suppliers, customers and others

The Board is committed to ensure that Kaspersky Group strictly comply with its obligations to its suppliers and customers by the Company's commitment to its customers through providing them top quality products. The Group undertakes research and development in connection with its principal activity. The Group's research and development expenses increased by 2% from USD 147,667 thousand in 2018 to USD 150,619 thousand in 2019.

Regards to the impact of the company's operations on the community and the environment

The Company operates in the industry whose primary goal is fighting cybercrime, which benefits communities worldwide. The Company is conscious of its environmental responsibilities and aims at reducing any damage to the environment that might be caused by its activities, primarily by reducing energy consumption.

Regards to the desirability of the company maintaining a reputation for high standards of business conduct

The Board considers that the reputation for high standards of business conduct derives primarily from meeting its obligations to its customers and suppliers, involving employees in the relevant areas of its business activity and promoting cybersecurity to make the world safer.

Regards to the need to act fairly as between members of the company

The Group treats all its shareholders fairly and no preferences are made to some shareholders at the expense of the others. During 2019 the Group did not declare any dividend and did not enter in material transactions with any of its members, apart from the fact that some of the Group's shareholders are part of the management and/or are employed by the Group.

The effect of COVID-19 on the Company's business

The directors have considered the impact of the COVID-19 pandemic on the financial and operational functions of the Company. The directors have commissioned market intelligence research on the potential impact of the pandemic on the sector and have assessed the business systems including the robustness of the internal and external supply chains for operational continuity. Based on these assessments and considerable financial resources of the Company together with long-standing relationships with a number of customers and suppliers across different geographic areas and industries, the directors believe that the Company is well placed to manage its business risks successfully.

The effect of COVID-19 on the security industry in general is complex and goes in opposite directions:

- General slow-down of economy worldwide, which negatively affects the budgets of businesses and households.
- Growth of interest to IT security because of a wider spread of working from home worldwide.

Corporate Governance Report

The Group does not apply a formal corporate governance code. All the entities inside the Group are governed in accordance with the relevant laws and constitution and by-laws that apply in their country.

The key members of the Company are the Company's Board of Directors. The nature and functions of the Board and the manner in which it is conducted is aligned with the Articles and Memorandum of Association of the Company. All the Company's Directors are equally involved in managing all sides of the Company's activities and interact with the members of the Company in accordance with the laws of the UK.

There is no governance code required because the management of the Company and the Group management on the highest level is executed by the same permanent group of chief managers, headed by major beneficial owners (members) of the Group, in the form of the Company's Board of Directors. In this respect the Company has no practical need for any special governance code or supplementary arrangements for corporate governance as the Board and the shareholders are structurally aligned.

DETAILED FINANCE AND LEGAL INFORMATION ABOUT KASPERSKY LABS LIMITED CAN BE FOUND AT HTTPS://WWW.GOV.UK/GOVERNMENT/ORGANISATIONS/COMPANIES-HOUSE