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.

The Company's registered office is: 2 Kingdom Street, London, W2 6BD.

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 240,000 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. More than a third of the highly qualified specialists working at Kaspersky are research and development (R&D) specialists developing and maintaining all of our solutions in-house, which is key to providing a holistic approach to security.

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".

More than a third of the highly qualified specialists working at Kaspersky are research and development (R&D) specialists developing and maintaining all of our solutions in-house, which is key to providing a holistic approach to security. An elite group of more than 40 security experts from our Global Research and Analysis Team (GReAT) operate all around the world and provide leading 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 CyberattackAPT 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. Today, it is more important for us to use this accumulated expertise to create technologies that will make cyberthreats lose their relevance.

Kaspersky is focused on innovation and believes in the collaboration with brilliant minds to accelerate the development of new solutions for a digitally safe today and tomorrow. The Kaspersky Innovation Hub is a core element in our growth strategy, with the main mission to discover new frontiers and identify new trends, understanding market needs, security challenges and demands across industries. It promotes knowledge sharing and disruptive thinking, while providing a stable infrastructure to develop in-house ideas

or external advanced projects into businesses, validate them on the market, enhance them, conduct pilots for the final goal to add meaningful value to our customers.

The Group's commitment to its customers as well as advanced technology ensure its competitiveness. Based on the results of the 2020 Global Industrial (OT/ICS) Cyber Security market, Kaspersky has been recognized a Global Company of the Year by analyst firm Frost and Sullivan. The Group is also firmly positioned as one of the top five leading endpoint security vendors. Kaspersky has been recognized as a 2020 Customers' Choice for Endpoint Detection & Response Solutions by Gartner Peer Insights. Kaspersky was also recognized as a highly rated vendor in the Gartner Peer Insights 'Voice of the Customer' Security Awareness Computer-Based Training, 2021 report.

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, the Industrial Internet Consortium and AUTOSAR.

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. Endpoint security products protect against both file-based and fileless exploits. In the corporate segment, the endpoint security market is also increasingly associated with the Endpoint Detection & Response (EDR) market. EDR products facilitate incident investigation and remediation on endpoints in cases where threats successfully evade prevention controls. The endpoint security category covers both corporate and consumer products. Global corporate and consumer markets are growing approx. at 8% and 1% per year, respectively.

Key drivers of the endpoint security market include the following:

- Cloud-native endpoint security offerings are rapidly gaining traction among companies of all sizes, as SaaS-delivered solutions allow companies to shift the administrative burden from product maintenance to more productive threat mitigation and risk reduction activities. Cloud products'

nimble architecture also appeals to organizations that support an increasingly remote, distributed workforce, and must spend to secure it.

- The trend of vendor/agent consolidation continues, as organizations increasingly demonstrate a preference for buying fully integrated endpoint prevention / EDR offerings over best-of-breed point solutions.
- A growing availability of and appetite for managed detection and response (MDR) services are lowering the barrier to entry small and midsize companies wishing to buy EDR solutions, thus increasing the addressable market for providers.
- As everyday life becomes more digitalized, consumers encounter increasing exposure to threats to their online security and privacy. The adoption of smart home devices and growing spend on technology services and subscriptions (e.g. wireless, internet, video content services, gaming) will only serve to broaden consumers' digital footprint, and thus their attack surface. Consumers stuck at home during the coronavirus are increasingly aware of this exposure and are taking steps to enhance their cybersecurity posture.
- Although the penetration of consumer antivirus is high, the penetration of other consumer security technologies that are frequently bundled with antivirus, such as consumer VPN or password managers, remains much lower. Providers offering these features/functionalities will actively market their benefits to attract new customers.

Endpoint security market inhibitors include the following:

- The COVID-19 pandemic has forced many companies out of business and caused survivors to become more conservative with budgets. Corporate endpoint security vendors, accordingly, have fewer companies to sell to, and heightened cost and time pressure resulting from the pandemic makes selling in general more difficult.

- Many types of end-user devices, operating systems and applications include an increasing amount of "built-in" security capabilities. As such, providers of commercial consumer security products must devote more time, money and energy to educating consumers that their paid products are sufficiently differentiated from "built-in" or free offerings.

- The rise of free alternatives in the consumer space will force vendors away from direct B2C sales in favor of other consumer channels, such as network carriers and internet service providers. The shift towards selling through these channels will put downward pressure on providers' margins.

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 11% 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 8% 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 17% 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 33% 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.

During 2020 the Group acquired 100% in Nexway Group AG, a leading e-commerce and payment platform, to strengthen its position and increase opportunities for the company's online sales channel. The market realities of 2020 have demonstrated the importance of having an effective online sales channel that is fast in management and reliable in terms of the safety of customer data. The extended integration of the two companies will enable more effective management of the Kaspersky online sales channel and further expansion of Nexway's growth as the leading e-commerce platform for security solutions.

Despite rising competition on the market, Nexway stands out with its technologically advanced e-commerce solution that keeps businesses compliant with all local and global regulations as they operate in multiple currencies, languages and payment methods. The Group and Nexway have a long and successful history of working together, and the companies have decided to start a mutually beneficial partnership - bringing together their expertise and further strengthening their businesses. Nexway has launched its Open kitchen project where it will continue demonstrating the security of users' data via advanced data storage and processing practices, with the data only being available to vendors and not to the owner of the platform.

The Group measures its progress against goals using the following key performance indicators ("KPIs"): billings, revenue, results from operating activity and net profit before tax.

The main short-term KPI the Group uses to track the progress of the business within a year as well as year-on-year growth is billings. Billings represent the total monetary value of products and services sold and delivered to its customers during a reporting period measured by the monetary amounts of invoices issued to its partners and customers. Billings are the most accurate measure of the sales volumes and growth of business. International Financial Reporting Standards ("IFRS") and the Group's accounting policy require that some software license revenue is recognised rateably over the license term, which therefore has the effect of deferring a portion of billings to future periods. This ensures a future guaranteed revenue stream in the amount of the deferred revenue as at the end of a reporting period.

The Group's performance in 2020 was significantly influenced by the changes of the foreign currency exchange rates. USD weakened during 2020 against the EUR by 9% and strengthened against the RUB by 19%, the main currencies affecting the Group's operations.

The Group's billings increased in 2020 by 7% from USD 699 million in 2019 to USD 747 million. Billings expressed in local currencies of the countries, in which the sales are made, increased by 10% in 2020 compared to 2019. In addition to its core business revenues, the Group earned USD 4 million (2019: USD 5 million) of lease income from letting out office premises.

The Group's revenue increased by 3% from USD 690 million in 2019 to USD 713 million in the current reporting period. Revenue in constant currency terms increased in 2020 by 6.2% compared to 2019. Similar factors affect the dynamics of the Group's revenue and billings.
The Group's profit from operating activities increased by 51% from USD 73 million in 2019 to USD 110 million in 2020, the growth mainly being due to increase of revenue and decrease of distribution expenses.
The Group's EBITDA1 increased from USD 119 million in 2019 to USD 154 million in 2020. Its dynamics corresponds to the change in operating profit.
The Group's net finance income of USD 3 million (2019: USD 17 million) is formed primarily by investment gain and interest income.
The Group's profit before income tax increased by 28% from USD 90 million in 2019 to USD 115 million in the current reporting period.
The Group's effective tax rate increased from 17% to 42% mainly due to the effect of reduction of tax rates in Russia upon deferred tax asset balances.
As a result of factors described above, the Group's net profit for 2020 amounted to USD 66 million (2019: USD 75 million), a decrease of 12% compared to the previous year.

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 2021 budget which was approved in 2020 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 2020, 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 amounted in 2020 to 57% of the Group's operating expenses (2019: 52%). Employee involvement and commitment to the success of the business is an important element of the Group's culture. Management conducts regular communications and consultations with employees on key aspects of the Group's activities in the form of e-mail communications, annual meetings and informal events. Bonuses of aA significant portion of employees bonuses depend on the financial performance of the business unit that they belong to and/or the 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.

[1] EBITDA for twelve months ended 31 December 2020 includes IFRS operating profit of USD 110 million (2019: USD 73 million) plus depreciation and amortisation USD 41 million (2019: USD 45 million).

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

The Board is committed to ensure that the Group strictly comply with its obligations to its suppliers and customers.

The Group conducts operations on different national markets and can be significantly affected by geopolitical situations in the world. As a result of the tensions the Group used to receive negative publicity in some countries. To cope with these geopolitical challenges the Group abides by the highest ethical business practices, and through its Global Transparency Initiative launched in 2017, it is exemplifying its ongoing commitment to assuring the integrity and trustworthiness of its products.

Global Transparency Initiative includes customer detection data storage and processing. In November 2018, the Group started relocation of data processing for European customers and a year after, in November 2019, announced moving data of customers from the U.S. and Canada. This process was completed by November 2020. In addition to Europe, the United States, and Canada, Kaspersky has also relocated data storage and processing for a number of Asia-Pacific countries. The Group have opened four Transparency Centers: in Zurich, Switzerland, in Madrid, Spain, in Kuala Lumpur, Malaysia and São Paulo, Brazil. These are facilities for our trusted partners to review the company's source-code. In addition to that, they serve as briefing centers to learn more about company's engineering and data processing practices. As part of the Global Transparency Initiative, the Group has already increased its bug bounty program.

The Group operates in a market where technology plays a key role. Maintaining industry leadership positions is subject to a number of risks. Specifically, the Group may lack financial and other resources to maintain its positions. Products in the Group's target market are technologically complex and vulnerable to defects and error. Additionally, a possible infringement of the Group's intellectual property rights may negatively affect the Group's competitiveness in the market. The Group 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.

Endpoint security has historically been the core of the Group's business; this security market is close to maturity and the growth is minimal. This may negatively affect the Group's financial performance and position in the future. To manage this risk we are constantly expanding our product portfolio with solutions in the non-endpoint security area, such as critical infrastructure IT protection, cybersecurity intelligence and Secure Web / E-Mail Gateway services.

Some of the third-party products in the endpoint security market (especially the consumer segment) are free. The trend of moving to free products is especially apparent in the Asian markets. In most cases, the free products are only providing basic antivirus protection but customers are looking for a complete suite of security capability. The Group believes that free endpoint security software is not a detriment to the market but recognises that it has to manage the risk of market share loss to free endpoint security solutions by ensuring the quality of its products and by introducing a freemium software model.

The Group's policy in working with customers is focused on market penetration. As such, extended credit terms are granted to some of the Groups' major distributors. In addition, the Group invests in resellers' incentives offering them volume rebates and other similar discounts. This results in a credit risk which the Group incurs on its trade accounts receivable. The Group manages this risk by developing a network of long-term reliable distributors and by day-to-day monitoring of exposure to individual customers. Credit risk management activities are led by a Credit Committee including representatives of top management. Note 23(c)(iii) of the consolidated financial statements sets out a description of this risk.

The Group is exposed to foreign currency risk, because some entities of the Group need to carry out sales and purchases and make lending and borrowings in currencies different from the functional currencies of these entities. This risk is mitigated by the day-to-day monitoring of the Group's open foreign currency position and the currency structure of its financial resources. Note 23(f) of the consolidated financial statements sets out a description of this risk.

The Group's operating margins remain healthy (15% in 2020 and 11% in 2019) and its operating cash flow has been considerable in recent years (USD 126 million in 2020 and USD 47 million in 2019). The Group's net current monetary assets position remains stable. The Group's most significant assets as at the reporting date are non-monetary deferred income of USD 586 million (2019: USD 542 million) due to the Group's revenue recognition policy. The Group's monetary current assets at 31 December 2020 are USD 434 million (2019: USD 384 million). These monetary current assets exceed the Group's monetary current liabilities of USD 142 million (2019: USD 138 million).

On a regular basis the cash position of the Group is monitored to ensure sufficient cash resources are available to settle liabilities as they fall due – both in aggregate and in each individual currency. Management carries out a thorough analysis of the Group's cash position before making any significant investment or financing decisions.

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

The Group operates in the industry whose primary goal is fighting cybercrime which benefits communities worldwide. The Group 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 2020 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 Group. 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 Group and Company together with long-standing relationships with a number of customers and suppliers across different geographic areas and industries, the directors believe that the Group is well placed to manage its business risks successfully.

Subsequent to the end of the reporting year the COVID-19 pandemic outbroke around the world. As of the date of this report, the effect of the pandemic has not been significant for the Group, the largest impact being related to the devaluation of most currencies against the USD, which negatively affects the Group's revenues in the USD terms. Management cannot currently reliably estimate the influence of COVID-19 on the Group's future performance, but are confident that the outbreak of the virus does not raise a going concern question for Kaspersky.

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