Copyleaks Technologies LTD.

Copyleaks platform

ISAE 3000 - SOC 3

Service Auditor’s Assurance Report

For the period

January 1, 2024, to December 31, 2024

Contents

Section I - Management Assertion Provided by Copyleaks Technologies LTD.

We have prepared the attached description of Copyleaks Technologies LTD. platform ('The System') for the time period of January 1, 2024, to December 31, 2024 (the 'Description') based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.34 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality and Privacy (the 'Description criteria'). The Description is intended to provide with information about Copyleaks platform and to meet the criteria for "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy" issued by the Association of International Certified Professional Accountants (AICPA).

We confirm, to the best of our knowledge and belief, that:

A. The Description fairly presents The System for the period January 1, 2024, to December 31, 2024, based on the following Description criteria:
   i) The Description contains the following information:
      1. The types of services provided.
      2. The components of the system used to provide the services:
         a) Infrastructure: the physical and hardware components of a system (facilities, equipment, and networks);
         b) Software: the programs and operating software of a system (systems, applications, and utilities);
         c) People: the personnel involved in the operation and use of a system (developers, operators, users, and managers);
         d) Procedures: the automated and manual procedures involved in the operation of a system; and
         e) Data: the information used and supported by a system (transaction streams, files, databases, and tables).
      3. The boundaries or aspects of the system covered by the Description;
      4. How the system captures and addresses significant events and conditions;
      5. The process used to prepare and deliver reports and other information to customers and other related parties;
      6. If information is provided to, or received from, subservice organizations or other parties; how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance and storage are subject to appropriate controls;
      7. For each principle being reported on, the applicable trust services criteria and the related controls that must be designed and operated effectively to meet those criteria, including as applicable:
         a) Complementary user-entity controls contemplated in the design and operation of the service organization's system.
      8. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
      9. Any applicable trust services criteria that are not addressed by a control and the reasons; and

10. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

ii) The Description does not omit or distort information relevant to the service organization's system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

B. Subject to the information outlined in point c) below, the controls stated in the Description were suitably designed and operated effectively for the period January 1, 2024, to December 31, 2024, to meet the applicable trust services criteria. This assumes that the subservice organizations applied, for the specified period, the types of controls expected to be implemented and operated at the subservice organization and incorporated in the design of the system.

Copyleaks Technologies LTD.

Nir Saban

March 12, 2025

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

Tel +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Section II – Independent Service Auditor's Assurance Report Provided by KPMG

Private and confidential

The Board of Directors

Copyleaks Technologies LTD.

Israel

March 12, 2025

Dear Directors,

ISAE 3000 (SOC 3) Type II Independent Service Auditor's Assurance Report.

In accordance with our engagement letter, we have examined the accompanying Description in Section III of the controls in place at the service organization called Copyleaks Technologies LTD. (Copyleaks or The Company) and carried out procedures to enable us to form an independent opinion on whether The Company's management has fairly described Copyleaks Technologies LTD. platform('The Platform') throughout the specified period of January 1, 2024, to December 31, 2024 (the 'Description'), and on the design and operation of controls stated in the Description to meet criteria for the Security, Confidentiality, Privacy and Availability Principles set forth in the TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Technical Practice Aids) ('applicable trust services criteria'). Our opinion is set out below and should be read and considered in conjunction with this report in full.

Copyleaks Technologies LTD. Management's responsibilities

In this report, references to Copyleaks Technologies LTD.'s "management" means the directors of Copyleaks Technologies LTD. and those employees to whom the directors of Copyleaks Technologies LTD. have properly delegated day-to-day conduct over matters for which the directors of Copyleaks Technologies LTD. retain ultimate responsibility.

Management of Copyleaks Technologies LTD. is responsible for (1) preparing its statement and the system description, (2) having a reasonable basis for its statement, (3) selecting the criteria to be used and stating them in the statement, (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description, and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the applicable trust services criteria will be achieved.

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

Tel +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Service Auditor's responsibilities

Our responsibility is to express an independent opinion to Copyleaks Technologies LTD. based on the procedures performed and evidence obtained, as to whether (1) Copyleaks Technologies LTD.'s management Description fairly presents the controls that were designed and implemented throughout the specified period, and the aspects of the controls that may be relevant to a user organization's internal control, as it relates to an audit of the Security Principle within Copyleaks Technologies LTD.'s statement, (2) the controls included in the Description were suitably designed throughout the specified period to provide reasonable assurance that the required trust services criteria would be met if the described controls were complied with satisfactorily, and (3) such controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the required trust services criteria were achieved during the specified period.

Framework Applied

Our work was performed based on the framework set out by the International Auditing and Assurance Standards Board (IAASB) and International Standard on Assurance Engagements (ISAE 3000).

Our Independence and Quality Control

We comply with the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants. Accordingly, we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements and professional standards (including independence, and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior) as well as applicable legal and regulatory requirements.

Scope of work

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's Description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description based on the Description criteria and the suitability of design and operating effectiveness of those controls to meet the applicable trust services criteria.

We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Copyleaks platform uses Google Cloud Platform (GCP) as a sub-organization to provide infrastructure management services. The description indicates the need for additional controls from the sub-organization, appropriately designed and operating effectively, along with Copyleaks platform controls, to meet in the platform's service obligations and system requirements, in accordance with the relevant Trust Services criteria. Our testing only included Copyleaks platform and its controls, and there was no extension of our testing to the specific services of Google Cloud Platform (GCP) throughout the period January 1, 2024, to December 31, 2024.

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

Tel +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Limitations of Controls at a Service Organization

Copyleaks Technologies LTD. management's Description is prepared to meet the needs of their auditors. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in service operations or related reporting. Also, the projection of any evaluation of the effectiveness of the controls to meet the applicable trust services criteria to future periods is subject to the risk that the system may change or that controls at a service organization may become inadequate or fail.

The relative effectiveness and significance of specific controls at Copyleaks Technologies LTD., and their effect on assessments of control risk at the user organization is dependent on their interaction with the controls and other factors present at the user organization. We have performed no procedures to evaluate the effectiveness of controls at the user organization.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In all material respects, based on the criteria identified in Copyleaks Technologies LTD.'s statement on Section II and III and the applicable trust services criteria:

A. The Description fairly presents The System that was designed and implemented throughout the period of January 1, 2024, to December 31, 2024.
B. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the described controls were complied with satisfactorily throughout the period of January 1, 2024, to December 31, 2024; and
C. The controls tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were achieved, operated effectively throughout the period of January 1, 2024, to December 31, 2024.

About this report including disclosure

This report is made to and has been prepared solely for the management of Copyleaks Technologies LTD. as a body, on the terms agreed and recorded in our Engagement Letter. In this report, by "management" we mean the directors of Copyleaks Technologies LTD. and those employees to whom the directors of Copyleaks Technologies LTD. have properly delegated day-to-day conduct over matters for which the directors of Copyleaks Technologies LTD. retain ultimate responsibility.

This report was designed to meet the agreed requirements of Copyleaks Technologies LTD. and particular features of our engagement determined by Copyleaks Technologies LTD.'s needs at the time.

The information contained in this report is confidential and shall not be released, duplicated, published, or disclosed in whole or in part, or used for other purposes, without our prior written consent or as permitted by our engagement letter.

Intended users and purpose

This report and Description of tests of controls and results on section IV are only to be disclosed to User Entities who have a sufficient understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, and other parties;

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

- Internal control and its limitations;
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

The above understanding is necessary to enable the User Entities to consider the matters stated including the basis of our consent to disclosure and their ability to rely on this report, along with other information including information about controls implemented by customers themselves, when assessing the risks in relation to User Entities' operational systems. This report is not to be used by anyone other than these specified parties.

Any party other than Copyleaks Technologies LTD. or its management, as a body, who obtains access to this report or a copy and chooses to use and rely on this report (or any part of it) will therefore do so at its own risk. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than Copyleaks Technologies LTD. and its management, as a body, for our work, for this report, or for the opinions we have formed.

Yours faithfully,

Somekh Chaikin

KPMG

Tel Aviv, Israel

March 12, 2025

Section III - Description of Copyleaks Technologies LTD. system

Company Overview and Background

Copyleaks platform is an AI based content authentication platform that is focused on detection of originality in textual content.

Key Features of Copyleaks platform

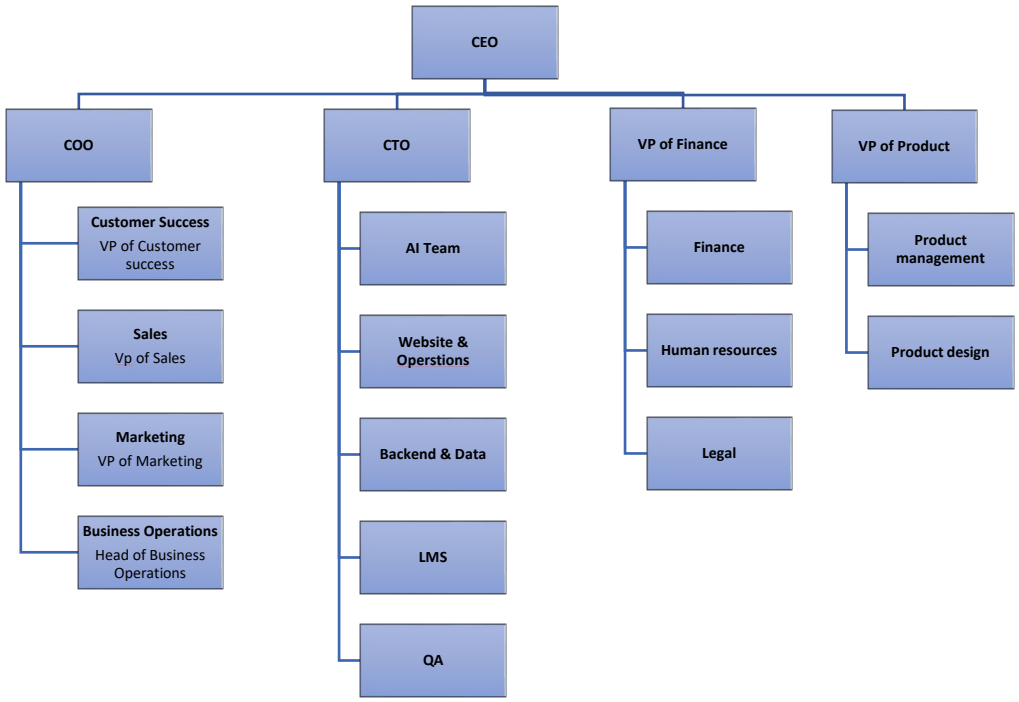
The Platform serves as an advanced text analysis platform with a diverse range of use cases. The Platform key features include:

- Plagiarism Detection- refers to the process of identifying and determining instances of plagiarism in written or creative works and source code.
- AI Content Detection - Detecting content that may be generated by tools such as ChatGPT.
- Writing Assistant-Information about grammatical mistakes, writing level, speaking time within a student assignment.
- LMS (Learning Management System) Integrations.
- API Integrations.
- Teams.
- Web-based platform which includes:
    - Organization options to view analytics on a department and user level.
    - Private repositories for organizations to store their own private documents that won't be compared against other Copyleaks Technologies LTD. users.

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting The Platform and does not extend to other products and services or the controls at third-party service providers.

Organizational Structure



The Company organizational structure provides the overall framework for planning, directing, and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. It represents the system through which employees, management, and operations interact to achieve business objectives. The structure clearly defines the lines of authority, responsibility, and communication, and provides the overall framework for planning, directing and controlling operations. Operating under this strategic design enables The Company to utilize its time and resources effectively to support its customers and progressively enhance the solutions offered to them. An organization chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.

Sales: The sales department is composed of specialized and experienced sales personnel. It is responsible for selling and optimizing sales to The Company's potential customers.

Marketing: The marketing department is responsible for building the company's brand, generating sales leads, and other marketing activities.

Customer Success/Support: The CS team is responsible for providing support to The Company customers. The support team is working closely with R&D and QA.

Business Operations: The Business Operations team improves data understanding and consistency across departments, streamline requests through single contact point, and consolidates intersecting projects to boost efficiency and alignment.

Product: The product team is responsible for defining the Copyleaks Technologies LTD. product lines and available services - requirements and priorities.

Research and Development (R&D): The R&D department is responsible for developing The Company products and the business services implemented within the production environment. This department includes three development teams as detailed below:

- Server side: This team is in charge of the development that concerns the server side, providing all the facilities and security features needed for the product delivery.
- Client side: This team is in charge of the web page and functions performed on the client's side as well on the desktop client application.
- Quality Assurance (QA): The QA department is responsible for testing and validating the R&D's deliverables according to predefined scenarios. The QA personnel are an integral part of R&D teams and are mentored by the CTO overseeing the entire QA activities at The Company.

Finance & Admin Team: The Finance and Admin department is responsible for the company's legal, compliance, HR, financial and control activities including financial planning and administrative tasks.

Description of the Control Environment, Information Communication, Monitoring and Risk Assessment Process

Copyleaks Technologies LTD. 's internal control is a process affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable Google Cloud Platform and regulations. The following section is a description of the five components of internal control for The Company.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods, and organizational structure. The Company executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Policies and procedures documents for significant processes that address system requirements and relevant updates are available on the internal intranet. Policies and procedures are documented, reviewed, approved on an annual basis by the management team, and available to The Company employees within its Google drive.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through Copyleaks Technologies LTD.:
(1) Management operating style.
(2) Organizational structure.
(3) Employee job descriptions and.
(4) Organizational policies and procedures.

Board of Directors: The Board of Directors (BOD) of Copyleaks Technologies LTD. is composed of both external directors and directors who are executive officers of the Company. The external directors are both: (1) Industry experts; (2) Investor representatives. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations. It has sufficient members who are independent from management and objective in evaluations and decision making. Members of the Board meet on at least a quarterly basis to discuss matters pertinent to the Company and to review financial information. Part of the Board's mission is to define, maintain and periodically evaluate the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of the Company through its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate. The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control. The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the standards of conduct. Company board of directors meets on a quarterly-basis. The board meeting has a fixed agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) the product discussion with new features (**1**).

Management Philosophy and Operating Style: The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage Copyleaks Technologies LTD. and its business on a daily basis. The Company is led by a team with proven ability in media and online customer solutions to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand The Company's objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. The Management Team convenes on a weekly basis or more frequently if necessary.

Integrity and Ethical values: Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Technologies LTD. ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. These include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the

communication of the organization's values and behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within Technologies LTD. to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Human Resources Policy and Practices: Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting, and compensating personnel. The competence and integrity of Technologies LTD. personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent, and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the Technologies LTD. policies that define how services should be delivered, and products need to be developed. These are located on The Platform and can be accessed by relevant Copyleaks Technologies LTD. team members while communicated by emails or other messaging applications, such as Slack, on an as-needed basis. Internal employees sign on an NDA as part of their employment contract with the Company while clients and 3rd parties sign on NDA within the business contract.

Commitment to Competence: Competence at Copyleaks Technologies LTD. is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. Job descriptions are documented and maintained. Candidates go through screening and appropriate background checks based on regulations in the Country the company hires personnel.

Risk Assessment

Risk assessment: The process of identifying, assessing, and managing risks is a critical component of Copyleaks Technologies LTD. internal control system. The purpose of the risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of The Company and include regular management and supervisory activities. Managers of each department are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. Minutes of risk assessment meetings and action items are documented into emails. On an annual basis risks are reviewed and updated in order to, among others, re-assess risks, review operational aspects of the control environment, and monitor the control environment.

Risk Mitigation

Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. Copyleaks Technologies LTD. selects and develops control activities that contribute to the mitigation of risks to the achievement of the company's objectives to acceptable levels. The risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet The Company's objectives during response, mitigation, and recovery efforts. Copyleaks Technologies LTD. requires Third party Vendors to have a valid SOC2 certification.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity's objectives.
Copyleaks Technologies LTD. operating and functional units are required to implement control activities that help achieve business objectives associated with:
(1) The reliability of financial reporting,

(2) The effectiveness and efficiency of operations and
(3) Compliance with applicable Google Cloud Platform and regulations.

The controls activities are designed to address specific risks associated with Copyleaks Technologies LTD. operations and are reviewed as part of the risk assessment process. The Company has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities. New employees go through a boarding process during which, among others, are communicated their responsibilities and the different Copyleaks Technologies LTD. policies.

Information and Communication

Information and communication are an integral component of Copyleaks Technologies LTD. internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At The Company information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors, regulators and employees. The management team meets on at least a monthly basis, in order to evaluate risks and threats and discuss security and non-compliance issues and address them. Minutes of the meeting are retained.
Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate The Company personnel via dedicated system.

Monitoring

Copyleaks Technologies LTD. uses a monitoring tool to monitor Copyleaks Platform. Alerts are sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. The notifications are reviewed and addressed according to their level of urgency. Metrics produced from these systems are used to identify the strengths and achievements as well as the weaknesses, inefficiencies, or potential performance issues with respect to a particular process. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time. The Company Management Team monitors the progress with respect to Copyleaks Service processes on a regular basis. Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through emails, meetings, and a project portal tool in order to prevent future occurrences. Changes impacting customers are communicated to clients through release notes within The Platform or by email. While internal employees receive notifications through a dedicated system.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Assets are assigned owners to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

Antivirus

EDR is implemented on employees' laptops to prevent or detect and act upon the introduction of unauthorized or malicious software.

Support

The Company customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. Client issues are documented within the CRM tool. Cases are prioritized and processed based on the internal support policy.

Ticketing and Management

Copyleaks Technologies LTD. opens a ticket when an issue is raised by a client or when an issue is proactively identified. The Company uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are

classified by the level of urgency and assigned to the appropriate support tier for resolution. In addition, client's issues are documented. Cases are prioritized and processed based on the internal support policy.

Database Backup and restoration

Meta data retained in the database is dumped daily and stored into a bucket enabling geo redundancy. The backup system automatically generates a backup log. In case of failure, a notification is sent to the R&D team. Restore tests are performed on an annual basis. The test includes a full restore to a separate database server and bringing up the database to verify data integrity and accessibility as well as backup restoration test. The Company perform backup in order to maintain full redundancy in different locations.

Data Protection Procedures

Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information. Transmission of data is a key aspect of Copyleaks' internal controls. Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points. The transmission of data can be performed through removable media as well as through mobile devices. Processes are in place to protect mobile devices (such as laptops, smartphones, and tablets) that serve as information assets. When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.

Disaster Recovery Plan (DRP)

Copyleaks Technologies LTD. has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis. The Company maintains a backup at a separated location within the Google Cloud Platform environments. The backup file has been designed to allow full functionality of the Copyleaks platform in case of a disaster in the main data center. The Company annually documents and approves a restoration document that outlines the necessary steps to perform a restore.

Privacy

Organization has appointed a Privacy Officer who is accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disclosure of personal information.

Copyleaks Technologies LTD. collects personal information in accordance with the organization's privacy commitments. Consents obtained from data subjects for collection, usage and disclosure of personal information are retained in accordance with privacy laws and regulations as well as objectives defined in the privacy policy.

The Company describes the purposes for which personal information is collected, used, maintained, and disclosed in its Privacy Policy.

The Company has documented and implemented a privacy risk assessment process to assess risks resulting from the collection, storage, transmission, use and disclosure of personal information. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.

Sub-service organizations carved-out control:

Google Cloud Platform

Copyleaks Technologies LTD. hosts the application data primarily in Google Cloud Platform data centers which are certified as ISO 27001, PCI DSS Service Provider Level 1, and is SOC 2 compliant.

Business continuity plan arrangements in Google Cloud Platform have been reviewed and approved by Copyleaks Technologies LTD. and Google Cloud Platform specialists and are implemented in all The System backups processes.

#	Control Activity Expected to be Implemented by Google Cloud Platform (Subservice organization)	Applicable Trust Service Criteria
1	Subservice organizations are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its infrastructure as a Service (IaaS) cloud hosting services where Information systems reside.	CC6.1 – CC6.4, CC6.6
2	Subservice organizations are responsible for implementing and maintaining environmental protection.	A1.3
3	Subservice organizations are responsible to revoke access to the scoped data centers in a timely manner of employee or vendor record being deactivated.	CC6.2
4	Subservice organizations are responsible to periodically review access to the scoped data center by appropriate personnel.	CC6.2
5	Subservice organizations are responsible for monitoring and maintaining processing capacity on an ongoing basis.	A1.1
6	Subservice organizations are responsible for notify of unauthorized use of any account or other breaches related to the security, availability, confidentiality, and Privacy in service usage.	CC7.1 - CC7.5
7	Subservice organizations are responsible for installing anti-malware solutions to detect or prevent unauthorized or malicious software on hosted systems	CC6.8
8	Subservice organizations are responsible for implementing strong authentication mechanisms.	CC6.1
9	Subservice organizations are responsible for monitoring backup operations and alerting of backup failures	A1.3

User Entity Responsibilities

#	User Entity Responsibilities	Related Complemented Criteria Ref. Number
1	Ensure strong password policy.	CC6.1
2	Ensure multi-factor Authentication.	CC6.1
3	Ensure timely removal of user accounts for employees when user access is no longer required.	CC6.2
4	Configure roles and authorization – configure access to be based on the individual's roles and responsibilities and be limited to the minimum access right necessary to perform an assigned job function.	CC6.3
5	Secure on-premises components.	CC6.1, CC6.8, CC7.1
6	Integrating with monitored The Platform /applications in a secure manner and according to necessary compliance requirements.	CC6.1, CC6.7
7	Notify The Company of unauthorized use of any account or other breaches related to the security, availability, and confidentiality in service usage.	CC4.2, CC7.2, CC7.4