System and Organization Controls Report Relevant to Security, Availability and Confidentiality (SOC 3)

June 1, 2023 – May 31, 2024

Deloitte.

Deloitte.

Independent Service Auditor's Report

To: Management of Elementor Ltd.

Scope

We have examined Elementor Ltd. ("Elementor") accompanying assertion titled "Assertion of Elementor's Management" (assertion) that the controls related to Elementor Ltd.'s Platform were effective throughout the period June 1, 2023 to May 31, 2024 (the "Description"), to provide reasonable assurance that Elementor's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality" set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria").

The description of the boundaries of the system indicates that certain applicable trust services criteria specified in the description of the boundaries of the system can be met only if complementary user-entity controls contemplated in the design of Elementor's controls are suitably designed and operating effectively, along with related controls at Elementor We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Elementor uses Google Cloud Platform, GCP ("subservice organization") for its Cloud computing services. The description of the boundaries of the system indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system presents the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period June 1, 2023 to May 31, 2024.

Service Organization's Responsibilities

Elementor Ltd. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Elementor Ltd.'s service commitments and system requirements were achieved. Elementor has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Elementor is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the

applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Elementor's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Elementor's service commitments and system requirements based the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion management's assertion that the controls over the information systems and technology supporting Elementor's Platform were effective throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Elementor Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Brightman Almagor Zohar & Co.
Certified accountants
A firm in the Deloitte Global Network
August 12, 2024

Assertion of Elementor Management

We are responsible for designing, implementing, operating and maintaining effective controls within Elementor Ltd.'s (the "Service Organization" or "Elementor") Platform throughout the period June 1, 2023 to May 31, 2024 to provide reasonable assurance that Elementor Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria or description of the boundaries of the system is presented in Attachment A below and identifies the aspects of the system covered by our assertion.

Elementor uses Google Cloud Platform to provide Cloud computing services. The description of the boundaries of the system includes only controls and applicable trust services criteria of Elementor and excludes controls and applicable trust services criteria of Elementor. The description of the boundaries of the system indicates that the applicable trust services criteria specified in the description can be achieved only if controls at the subservice organizations contemplated in the design of Elementor's controls are suitably designed and operating effectively, along with the related controls at Elementor We have not evaluated the suitability of the design or operating effectiveness of such subservice organization controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Elementor Ltd.'s service commitments and system requirements were achieved based on the trust services criteria. Elementor's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2023 to May 31, 2024 to provide reasonable assurance that Elementor Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Elementor Ltd.

August 1, 2024

Attachment A

Elementor Ltd.'s Description of the Boundaries of its Platform

Overview of Elementor's Service

Elementor is a website builder platform for professionals on WordPress. Elementor serves web professionals, including developers, designers, and marketers, Elementor is an open-source, GPLv3 licensed offering its platform both as free and premium.

Elementor Plugin

Elementor is a visual website building plugin for WordPress, powering over 10 million websites worldwide. With its instant, live-design, and inline editing drag-and-drop Editor, as well as dozens of out-of-the-box widgets and features, web creators can create professional, pixel-perfect websites for any type of industry. Additionally, as it is open-source, users can also integrate with other marketing services. It is among the top 5 most installed plugins in the WordPress repository and supports a wide and lively community of developers who expand it with add-ons and templates.

Elementor Cloud Website

An Elementor Cloud Website is design for web creators who want to focus on building their professional website hassle-free.

Elementor Cloud was created to resolve a pain point the users had with creating websites on WordPress (WP) - having to navigate the potentially complex relationship between hosting, domains, the platform and building the website. The Elementor Website provides users with an easy-to-understand package that makes building websites faster and more efficient.

Principle Service Commitments and System Requirements

The Service Organization's security commitments regarding the systems and operations are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided to user entities. Those objectives are based on the service commitments that Elementor makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Elementor has established for the services.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Elementor's systems that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit
- Combat cyber threats by proactively monitoring and protecting Elementor and our customer's data
- Use strong identity management processes to secure data and systems from intrusion.
- Manage infiltration, intrusions, insider threats and anomalies by understanding who is on our networks, why they are on our networks, and what data they have permission to access.

Elementor establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Elementor's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of relevant service provided to its customers.

Subservice Organization

Elementor's uses subservice organizations that provides services as follows:

- Google Cloud Platform (GCP) virtual infrastructure are used for managed hosting services (storage, processing, and database).

Sub-processors Organizations

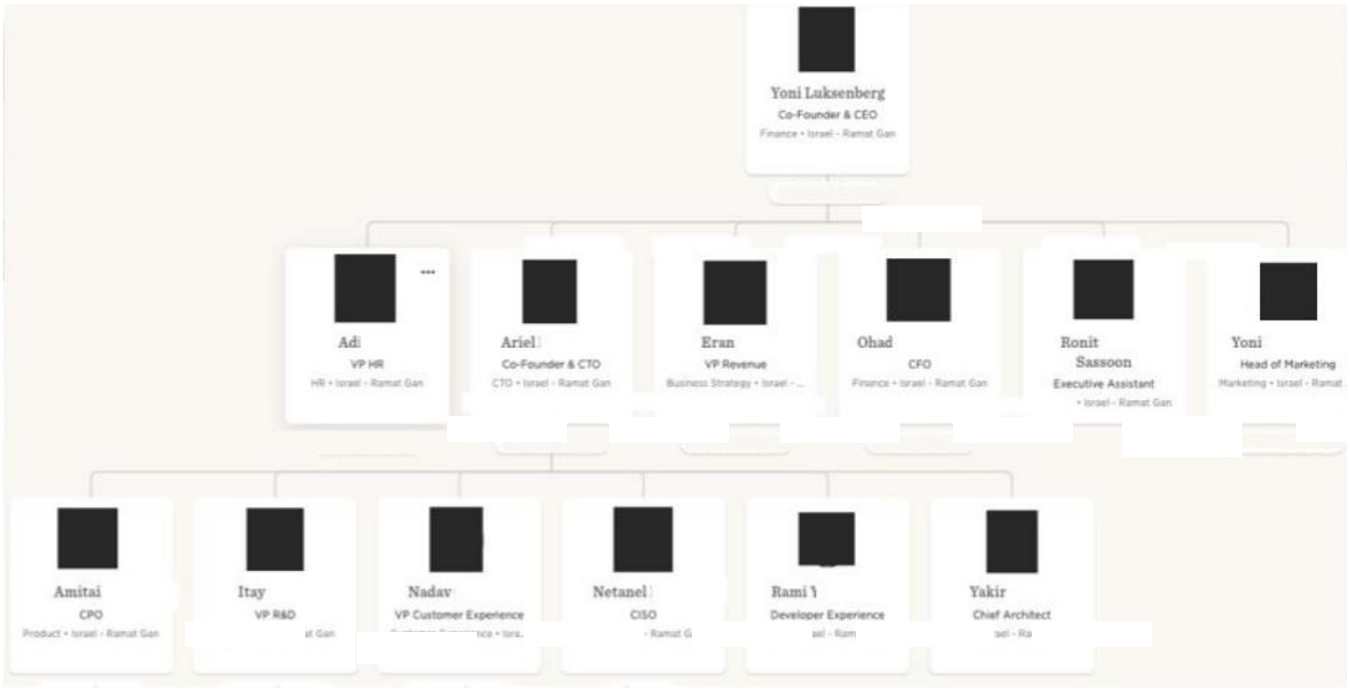
Elementor uses certain service-specific sub-processors to support the delivery of the Elementor services, provide specific functionality within the Elementor services or to provide professional services. The full sub-processors list could be found at - https://elementor.com/sub-processors-list/

Organizational Structure

Elementor's Organizational structure contains several teams and roles that impact the services provided as described above. Elementor's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and proper lines of reporting.

Below listed the main roles and responsibilities impact the services in the scope of this report.

See below Elementor's Organization Chart:



Roles and Responsibilities

The company has formally established requirements that describe the key roles including responsibilities and related job descriptions as required by Elementor management. With respect to relevant trust principal areas, there is assignment of responsibility and authority for decision-making in the company.

- Executive Management: responsible for overseeing and prioritizing strategic, company-wide goals and initiatives.
- Security & Privacy: responsible for driving the overall vision and direction of information security and Privacy at Elementor, whether for customer-facing products and systems, Elementor's internal systems and data, or data shared with third parties. Additionally, Security is also responsible for driving the overall vision and direction of Elementor's incident response, business continuity and disaster recovery programs.
- Law and Compliance: responsible for working with other departments to confirm technology environments, policies, and management processes align with relevant requirements, industry standards, and regulations.
- Human Resources (HR): responsible for maintaining HR-related policies and procedures for new and tenured employees. These areas of focus include recruiting/hiring, compensation, benefits, performance management, training, disputes, and employee development.
- Corporate Information Technology (IT): responsible for managing Elementor-issued employee devices and some aspects of user access management that relate to the Elementor production environment. Overall responsibility for provision and deprovision of access. The IT team manages all organizational assets according to best practices and regulatory requirements and oversees the introduction of new systems to the organization.
- DevOps: responsible for maintaining the various technology environments and the underlying systems and services (including operating systems, databases, and configuration management tools) that help configure, deploy, and monitor the operational health of those environments. This team is also responsible for maintaining the overall incident response framework and business continuity and disaster recovery programs for the Elementor platform. This team is also responsible for maintaining the configuration and security of network devices that support the Elementor platform, as well as real-time monitoring and preservation of the platform's health, performance, and planning for platform capacity needs.
- R&D: responsible for developing, integrating, and maintaining the core software and services that comprise Elementor's product functionality.
- Product: responsible for defining the product strategy, building the roadmap, and creating feature definition for Elementor platforms, including security and privacy aspects.
- Finance - Overall responsibility for verifying that security and privacy related efforts is being considered as part of the annual budgeting planning processes. Overall responsibility for reviewing and approving (financially) the annual security plan.
- Customer Experience: responsible for supporting customers in implementing and updating their service configurations, as well as triaging and resolving inbound customer-reported issues and questions. Client Services also assists in proactive communication to customers for widespread service-related issues.

Attachment B

Principal Service Commitments and System Requirements

CC1.0 Control Environment Area

The control environment at Elementor's is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. It reflects the overall attitude, actions of management and others concerning the importance of controls and the emphasis given to controls in Elementor's policies, procedures, methods, and organizational structure.
The Key elements of Elementor's control environment includes Oversight by Elementor's Board of Directors, HR Policies and practices and integrity and ethical values.

Board of Directors

Elementor's board of directors' responsibilities:

- The Board consists of key executives, subject matter experts and shareholders of the organization.
- The board of directors has been established and charged with governance in the organization and has the stature to challenge management's practices, decisions, and relevant trust principal breaches. Sufficient knowledge of the entity, its environment, its business risks, and relevant trust principal breaches are requirements for those charged with governance.
- Periodic meetings are held for those charged with governance to discharge their responsibilities.
- The board of directors are monitoring Elementor financial Resources

Organization and Management

Elementor's management team has been delegated by the Board the responsibility to manage Elementor and its business daily. The management team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. Elementor management team is committed to a high level of information security and privacy of its employees, clients, and partners.

The Information Security posture is an essential component of the company strategy to protect its reputation and corporate image.

Elementor Management team is committed to -

- Maintain data confidentiality, integrity, and availability
- Protect clients personally identifiable information
- Enable clients to meet legal and regulatory obligations
- Ongoing Information Security Management System (ISMS) and security posture improvement

Employee onboarding process

As part of Elementor HR onboarding processes, new employees will receive permissions to Elementor's information and system resources based on "least privileged" and "need-to-know" principles, in accordance with their specific role and responsibilities.

Access to Elementor systems and applications will be provided in accordance with Elementor's "Information Security Policy".

All Elementor employees sign a non-disclosure agreement (NDA) prior to being granted access to any system or cloud platform being used.

The contractual obligations reflect Elementor policies for information security in addition to clarifying and stating:

- That all Elementor staff who are given access to confidential information should sign a non-disclosure agreement (NDA)
- Elementor staff's legal responsibilities and rights (e.g., data protection legislation)
- Responsibilities for the classification of information
- Responsibilities of Elementor staff for the handling of information received from customers or other external parties
- Actions to be taken if the employee or contractor disregards Elementor's security and privacy requirements

Integrity and ethical values

Integrity and ethical values are essential elements of the control environment.

Specific control activities that Elementor has implemented in this area are described below.

- Verification processes are being conducted to verify our candidates' professional competence and provide a minimal assurance that they could be trusted to take on the role, especially as we consider every role to be critical for the organization. As part of Elementor policy requirements, employees must be screened prior to being offered employment and such verification must be performed under the strict guidance of HR and in accordance with local legislation.
- All the new employees are required to read and accept the code of conduct, which defines principles for proper ethical behavior, as part of Elementor's onboarding process.
- All new members, including temporary staff, are advised of their security responsibilities in Elementor within the first days of employment. Information on Elementor staff responsibilities in relation to security and acceptable use of resources is included within the HR policies as part of the onboarding process and signed by every new employee.
- Information security and privacy education and training takes place as part of the onboarding process and on a regular basis. Initial education and training apply to those who transfer to new positions or roles with substantially different information security and privacy requirements, not just new Elementor employees.
- Elementor's policies include probation, suspension, and termination as potential consequences of employee misconduct.

Elementor Code of conduct includes a section on Privacy and Data Protection and links to policies and procedures including the acceptable use policy and general information security policy to convey these controls and values to employees. The CoC contains sanctions for non-compliance with the policies and procedures.

CC2.0 Communication and Information

Information security policy and the company standards

The main objectives of Elementor Information Security Policy and Information Security Management System (ISMS) are to ensure the protection of information, creating controls, processes and procedures that focus on ensuring the confidentiality, integrity and availability of information resources as well as reducing the overall risk posture for the business.

The Information Security policy's objectives are designed to:

- Be consistent with the other organizational policies and global best practices
- Be measurable (where achievable)
- Consider requirements and results from risk assessment and treatments
- Be updated as needed, based on risk posture and business needs

These objectives are considered from initial software design and requirement phase to system implementation and have lay the foundation for the overall ISMS program. It is the policy of Elementor that the information assets will be protected from all types of threat, whether internal or external, deliberate, or accidental, such that:

- Confidentiality of information is maintained
- Integrity of information can be relied upon
- Information is available when the business needs it
- Relevant statutory, regulatory, and contractual obligations are met
- Elementor brand is protected

As part of the compliance processes, Elementor's policies and operational procedures are reviewed and updated annually by Elementor's Compliance Manager, Chief Information Security Officer (CISO), its management and by a non-dependent 3rd party.

All employees have access to Elementor's security and privacy policies and operational procedures.

CC3.0 Risk Assessment

Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of Elementor's internal control system. The purpose of Elementor's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives.

The Risk Management Program defines the process by which risk is evaluated and managed for reviewing,

maintaining, and continually improving the ISMS to effectively meet the information security objectives.

Control objectives and controls are selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection takes the criteria for accepting risks into account as well as legal, regulatory, and contractual requirements.

Elementor Management team defines how to measure the effectiveness of the selected controls or groups of controls and specifies how these measurements are to be used to assess control effectiveness to produce measurable and comparable results.

Results of a risk assessment become the primary content of risk reports. These reports are reviewed to provide Elementor's Management team with the data needed to make effective business decisions and to comply with internal policies as well as relevant industry regulations.

Updates to the risk assessment report occur annually or whenever there are significant changes in Elementor products, services, or the organizational environment.

CC4.0 Monitoring Activities

Monitoring

Elementor log and monitor activities and events on organizational systems and production environments.

Logging and monitoring processes include the log collection, event alerting, and protection of log information within Elementor users and production environments. Elementor logs and monitors multiple types of system and network events and activity to help detect and investigate potential security issues across production servers and network devices.
Monitored event types include the following:

- Invalid authentication attempts to production systems
- Anomalous network flow traffic
- The organization periodically assesses the sufficiency of its information systems to capture and report data that are timely, current, accurate, and accessible.
- For high severity incidents, Root Cause Analysis (RCA) is performed through various tools and meetings to improve the quality of the solution Elementor provides to customers.
- SLA with third parties exist and include monitoring the process and the access (as applicable).

Management assesses the risks associated with subservice organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner.

CC5.0 Control Activities

Internal Audit

Elementor has established internal audit procedures and techniques as part of its Risk-Management implementation.

Elementor's Compliance manager together with Elementor management team, hold an internal audit for the processes and procedures at least once a year.

Results are shared with management and relevant stakeholders, tracked, and remediated in accordance with the risk management standard.

To verify that all relevant processes, procedures, and controls are covered as part of the internal audit, Elementor initiated a non-dependent, 3rd party, internal audit assessment which is conducted at least once a year and is based on ISO 27001:2013 requirements.

Audit procedures steps are:

1. Assess current processes and procedures
2. Analyze and compare results against internal control objectives to determine whether audit results comply with internal policies and procedures as well as federal and state rules and regulations.
3. Compile an audit report to present to the business owner.
4. Track and remediate based on risk score

CC6.0 Logical and Physical Access Controls

Logical Access Management

Logical Security – Elementor Personnel Access:

Access is granted according to the principle of least privilege and is fully monitored, end-to-end. User access privileges are controlled by Elementor's IT team who manage users' privileges, access audits, and control. A limited number of operations engineers have access to production systems, and their access is fully monitored and audited (end-to-end) and protected by MFA. Operations are managed from a limited number of systems which centralized the administrative operations.
Also, as part of Elementor compliance processes annual user privileges review in all organizational systems is being conducted.
Access to Elementor's systems, tools, services, and endpoints is subject to strict password management standards in conjunction with multi factor authentication and integration with a central secure identity management provider.
Access to data is granted under the principle of least privileged and segregated based on duties.
Off-boarding of employees and removal of access associated with the terminated employee is automatically initiated following HR notice.

Logical Security – Customer Access:

Only customers have logical access to their accounts and data. Customers can restrict or expand access to data and actions within the service. This action is under the responsibility of the customers.
Elementor's customers acknowledge and agree to Elementor's Terms and Conditions of the subscription and Privacy Policy which include information related to system, operation, security, support, and responsibilities.

Physical and Environmental Security:

Elementor platform is hosted on AWS and GCP cloud infrastructure. All data will be stored online, as such, there should be no physical assets involved in the provision and maintenance of Elementor services.

Visitors to Elementor offices are required to sign-in at reception, and security cameras are located at entry points for Elementor offices.

Remote Access

Authentication to Production environments requires use of multi-factor authentication and password parameters consistent with the corporate password standard.

CC7.0 System Operations

Vulnerability Management and Secure System Development Life Cycle (SSDLC)

Elementor's infrastructure is being reviewed on an ongoing basis to identify any vulnerability or misconfiguration. Any identified issue from any source (including Bug Bounty Program, Penetration Tests, code reviews, etc.) are documented, prioritized, and tracked through resolution.

Changes are documented in an internal release notes document.

Every deployment is versioned and labeled. In addition to tests of specific changes, Elementor also conducts acceptance tests. Elementor emphasizes writing secure, clear, highly maintainable, and well-documented code.

All code is reviewed as part of the organizational SSDLC processes to identify possible security vulnerabilities. Elementor trains developers to follow OWASP principles and keep them in mind during code reviews and in general, development follows security best-practices.

Elementor conducts third-party Penetration Tests on Elementor's Production systems at least once a year and participates in a security Bug Bounty (Bug Crowd) program to improve the organizational security posture on an ongoing basis.

Incident Management

Elementor Incident Management procedure addresses the means necessary to ensure effective response to incident relevant to the system, identifying the lifecycle of the incident management, including the incident identification, investigation, prioritization, mitigation, and post-mortem processes.

Elementor follows a unified incident response framework to handle potential or actual incidents that affect the security or availability of the production network. Under this framework, Elementor maintains communication and escalation procedures to guide personnel in the reporting of security-related incidents and concerns.

The purpose of Elementor's incident and vulnerability management framework is to ensure the implementation of incident and vulnerability management processes and procedures that will help Elementor handle incidents using a structured and approved methodology and ensure that normal operations are restored as quickly as possible with the least impact to Elementor and its customers.

Elementor's incident and vulnerability management internal procedure is designed to handle security incidents and should be used as a baseline or reference document for dealing with information security threats.

Incident Management encompasses the people, processes, and technologies through the following process:

- Incidents & Vulnerabilities Identification
- Incidents & Vulnerabilities Reporting
- Exposure Assessment
- Response
- Post-mortem Processes

When a service issue is identified, Elementor updates the system status at https://status.elementor.com. Customers can also subscribe to receive status updates via multiple methods (email, RSS).
Technology changes following an incident review follow the standard change management process. Internally communicated incident reports are documented to record the description and timeline of the incident's discovery and resolution, as well as post-mortem review details.

Endpoint Protection

Elementor's endpoints run a best of breed endpoint protection software which is being updated daily. Endpoints are managed by an MDM solution which also mandates full disk encryption and secure configurations by policy.

Availability Procedures

Production Monitoring

Elementor's team monitors the service and environment for performance and data integrity, supports personal tracking the performance and availability of the service and cloud resources for application error, resource utilization and customer response time.

Alerts are sent to the On-Call group through an online massaging system (Slack). Alerts are investigated immediately and tracked to resolution.

Support

Elementor's customer support team responsible for managing client interaction, expectations including client onboarding support, account management and day-to-day customer reporting issues.
The team provides 24\7 support.

Backups, Recovery, Disaster Recovery and Business Continuity

Disaster Recovery Plan (DRP)

Elementor operates as a Software as a Service solution hosted in a public cloud. The infrastructure is hosted and managed by GCP and AWS and supports high availability and disaster recovery needs.

GCP and AWS operate under a shared responsibility model.

Elementor follows a unified Disaster Recovery and Business Continuity framework to handle potential or actual incidents that affect its production network.

Under this framework, Elementor maintains communication and escalation procedures to guide personnel in the reporting of potential and actual incidents.

The purpose of this framework is to provide guidance on how to plan and execute operations addressing potential business interruptions caused by emergency events in a manner minimizing any kind of loss.

The main goals of Elementor's Disaster Recovery and Business Continuity plans are to:

- Minimize interruptions to the normal operations.
- Limit the extent of disruption and damage.
- Minimize the economic impact of the interruption.
- Establish alternative means of operation in advance.
- Train personnel with emergency procedures.
- Provide for smooth and rapid restoration of service.

A business continuity management process is designed and implemented to reduce the disruption caused by disasters and security failures to an acceptable level.

As part of the organizational BCP and DR maintenance processes, the organizational procedures are being updated on an ongoing basis, including records of changes to configuration, applications, and backup schedules and procedures.

Backups are tested regularly, and at least annually, to verify Elementor ability to mitigate and recover from events that severely impact the availability of Elementor platform functionality.

All data is encrypted in transit, at rest, and when stored in backups.

CC8.0 Change Management

Elementor's Change Management policy describes the process for requesting, testing, and approving changes. All major systems or configuration changes follow a defined process of planning, evaluation, review, approval, and documentation.
Information Security risks related to all changes are being evaluated before performing the change and proper precautions are taken to reduce the probability of the related risks. As part of the risk evaluation process, planning critical changes include the ability to roll back the change in case of need.
Change requests are fully documented and tracked.

Elementor change management processes also include (when required) a formal notification to all customers upon the change which directly or indirectly affect the service.

CC9.0 Risk Mitigation

Vendor Risk Management

New 3rd party vendors go through an internal review process as part of their onboarding processes. As part of the onboarding processes, Elementor's team (Legal, Procurement, IT, Security) evaluates the 3rd party's overall security posture. The 3rd party's review process will be conducted at least annually to verify it still complies with Elementor's related security and privacy requirements. The annual assessment will include the collection of compliance certifications and attestation reports (e.g., SOC 2, ISO 27001) to determine if controls are sufficient to achieve Elementor's principal service commitments and system requirements.

Complementary Subservice Organization Controls ("CSOC")

Elementor's implementation of information technology and general IT controls is designed with the assumption that certain controls will be implemented by user entities. Such controls are called

complementary user entity controls. It is not feasible for all the control objectives related to Elementor general controls to be solely achieved by Elementor's control activities.

Accordingly, user entities, in conjunction with the information technology general controls system, should establish their own internal controls or procedures to complement those of Elementor.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

- Implement controls to enable security and monitoring tools within the production environment- CC1.5, CC5.2, CC7.1
- Implement logical access security measures to infrastructure component including native security or security software and appropriate configuration settings – CC6.1, CC6.2, CC6.3
- Restrict the access to the virtual and physical servers, software, firewalls, and physical storage to authorize individuals and to review the list of users and permissions on a regular basis- CC6.4, CC6.6, CC6.8
- Implement controls to: (CC6.1, CC6.2, CC6.3)
  - Provision access only to authorized persons.
  - Remove access when no longer appropriate.
  - Secure the facilities to permit access only to authorized persons

Complementary User-Entity Controls ("CUEC")

Elementor's system of general IT controls as it relates to applications, databases, and IT tools managed by Elementor were designed with the assumption that certain controls would be implemented from the above listed controls. These are required for proper processing under the assumption that the customer applies the following controls at their end of operations, where applicable, controls should be in place at the user entities to provide reasonable assurance that:

Logical Access (CC6.1, CC6.2, CC6.3)

- Customers are responsible for granting and revoking Elementor access to their users as appropriate, for periodically reviewing such access to ascertain access remains appropriate, and for monitoring access logs and addressing discrepancies.
- Customers are responsible for enforcing use of unique IDs and for configuring password parameters to Elementor, or their directory service where a directory service sync is utilized, which authenticates users to Elementor in accordance with their internal policies.
- Customers are responsible to notify in a timely manner of any updates regarding the list of authorized personnel that could impact services.

Network Services (CC7.1, CC7.2, CC7.3)

- Customers are responsible for monitoring log-in attempts and enforcing workstations to automatically lock after a predetermined period of inactivity.

Customers are responsible for the security of content once it is exported from Elementor.