REPORT ON

EnovaPoint’s

DESCRIPTION OF ITS JUNGLEMAIL NEWSLETTER AND JUNGLEDOCS DOCUMENT AUTOMATION PLATFORMS AND ON THE SUITABILITY OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD

JANUARY 7, 2022 TO DECEMBER 31, 2022

MARCUM
ACCOUNTANTS ▲ ADVISORS

Section 1: Assertion of the Management of EnovaPoint

Assertion of the Management of EnovaPoint

We are responsible for designing, implementing, operating, and maintaining effective controls within EnovaPoint's Newsletter (JungleMail) and Document Automation (JungleDocs) Platforms throughout the period January 7, 2022 to December 31, 2022, to provide reasonable assurance that EnovaPoint's service commitments and system requirements relevant were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the JungleMail Newsletter and JungleDocs Document Automation Platforms throughout the period January 7, 2022 to December 31, 2022, to provide reasonable assurance that EnovaPoint's service commitments and system requirements were achieved based on the trust services criteria. EnovaPoint's objectives for the Newsletter and Document Automation Platforms 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 those 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 JungleMail Newsletter and JungleDocs Document Automation Platforms were effective throughout the period January 7, 2022 to December 31, 2022, to provide reasonable assurance that EnovaPoint's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Andrejus Lizunovas

CEO

EnovaPoint

March 17, 2023

Section 2: Independent Service Auditors’ Report

MARCUM
ACCOUNTANTS ▲ ADVISORS

Independent Service Auditors' Report

To: EnovaPoint

Scope

We have examined EnovaPoint's accompanying assertion titled "Assertion of the Management of EnovaPoint" (assertion) that the controls within EnovaPoint's JungleMail Newsletter and JungleDocs Document Automation Platforms were effective throughout the period January 7, 2022 to December 31, 2022, to provide reasonable assurance that EnovaPoint'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022)* in AICPA, *Trust Services Criteria*.

EnovaPoint uses a subservice organization for IaaS. The description of the boundaries of the platforms indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EnovaPoint, to achieve EnovaPoint's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the JungleMail Newsletter and JungleDocs Document Automation Platforms were effective throughout the period to provide reasonable assurance that EnovaPoint'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 AICPA. Those standards require that we plan and perform our examination to obtain reasonable assertion 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 EnovaPoint'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 EnovaPoint's service commitments and system requirements based on 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 within EnovaPoint's JungleMail Newsletter and JungleDocs Document Automation Platforms were effective throughout the period January 7, 2022 to December 31, 2022, to provide reasonable assurance that EnovaPoint's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Marcum LLP

Marcum LLP

March 17, 2023
Tampa, FL

Attachment A: EnovaPoint’s Description of its JungleMail Newsletter and JungleDocs Document Automation Platforms

Purpose and Scope of Report

This report is intended to provide report users with information about the service organization's system relevant to security, availability, and confidentiality to enable such users to assess and address the risks that arise from their relationships with the service organization. This description is intended to focus on the internal control structure of EnovaPoint that is relevant to only users of its JungleMail Newsletter and JungleDocs Document Automation Platforms and does not encompass all aspects of the services provided or procedures followed by EnovaPoint.

System Description

Company Overview and Services Provided

Founded in 2007, Lithuania-based EnovaPoint makes it easy for Microsoft 365 and SharePoint users to communicate with employees, partners, or students as well as automate documents and reports based on SharePoint data. Instead of attempting to replicate or replace existing Office 365 functionality, EnovaPoint's products makes use of it, and utilizes real-time Office 365 data and content, without storing mailing lists or synchronizing content locally.

Newsletter and Document Automation Platforms

JungleMail is web-based email newsletter tool that is primarily designed to complement Microsoft 365 and SharePoint Intranets. The main purpose of JungleMail 365 is to improve employees' communication and engagement with an effective personalized internal newsletters and surveys.

With direct Azure AD communication, automatic newsletter content population from and to SharePoint Intranet, JungleMail sets new efficiency and best practices standards for company internal communication.

In addition, JungleMail offers a rich set of analytical data: Opens & clicks, Top links, Click Path, Surveys and polls results, Ideas & comments sharing, read time, reading devices, and segmented analytics by Job Title, Department, Office, Company, and Location.

JungleDocs is a document generation and automation tool that is specifically designed for SharePoint users. JungleDocs automates the document creation process by allowing users to prepare document templates, which can then be used to generate documents automatically from data stored in SharePoint lists or libraries.

One of the key features of JungleDocs is its ability to generate documents from smaller parts. Users can create reusable document parts, such as headers, footers, and sections, and then combine them to create complete documents. This can save significant time and effort, especially for complex or lengthy documents.

JungleDocs also includes smart metadata handling, which helps ensure that documents are properly tagged. Additionally, the tool can automate file naming, convert documents to PDF and

XPS, and generate documents automatically from Power Automate and API, further enhancing productivity for SharePoint users.

Infrastructure

The production environment that supports the operation of the JungleMail Newsletter and JungleDocs Document Automation Platforms is hosted in Azure data centers. EnovaPoint enforces MFA and secure passwords for access to production infrastructure within the Azure. Access to production environment is controlled via role-based permissions. Users assigned the appropriate role permission can authenticate to production infrastructure components through a VPN gateway to help ensure the security and confidentiality of the data passing over the public network. Encryption technologies are utilized for all communication between systems and the protection of data on employee workstations. The production environment is continuously monitored for suspicious activity. Backups are stored within Azure. Microsoft Azure is responsible for providing the physical safeguarding of the IT infrastructure to help ensure that unauthorized access does not occure, as well as providing environmental safeguards (power supply, fire suppression, etc.).

People

People involved in the operation of the system are:

- CEO – responsible for managing the company's overall operations
- COO – responsible for designing and implementing business operations, establishing policies that promote company culture and vision, and overseeing operations of the company and the work of executives
- CSO – responsible for developing future strategies and overseeing their implementation
- Lead Software Developer – responsible for leading software development team, engineering of the platforms
- Security Officer – responsible for providing secure workstations, corporate network access, and maintenance of appropriate security and availability of the systems.

Procedures

The key support policies and procedures provided by EnovaPoint include:

- Access Control Policy
- Application Development Policy
- Backup and Retention Policy
- Change Management Policy
- Data Protection Policy
- Disaster Recovery and Business Continuity Policy
- Disaster Recovery Plan
- Electronic Communication Policy
- Evaluation and Compliance Audit Policy
- Hardware and Software Maintenance Policy
- Incident Management Policy

- Internal Control Policy
- Inventory and Accountability Policy
- Laptop and Mobile Device Policy
- Network Protection Policy
- Password Management Policy
- Patch Management Policy
- Personnel Management
- Personnel Security Policy
- Protection from Malicious Software Policy
- Retention and Disposal Policy
- Risk Analysis Policy
- System and Services Acquisition Policy
- Systems Configuration Policy
- Teleworking Policy
- Vender Management Policy

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which EnovaPoint strives to achieve its business objectives. EnovaPoint has applied a risk management approach to the organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

Sensitive data is not stored or retained by EnovaPoint. Data that is retained is backed up on a daily basis within Azure and staff are notified of any failures in the backup process. There are no databases hosted within the EnovaPoint on-premises.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization, or personalization of data are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Significant Changes to the System Throughout the Period

There were no significant changes to the system throughout the period

Subservice Organization

Microsoft Azure

EnovaPoint uses Microsoft Azure for IaaS. Microsoft is responsible for the uptime, management, physical and logical security of the infrastructure that supports the delivery of internet, and environmental conditions that provide power and cooling to their devices. Microsoft is also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

EnovaPoint monitors the commitments of Microsoft and obtains attestation reports and/or supporting documentation, when applicable, on an annual basis to help ensure that security, availability, and confidentiality commitments are being met and reflect the current security control environment.

The applicable TSC that are intended to be met by controls at Microsoft, alone or in combination with controls at EnovaPoint, and the types of controls expected to be implemented at Microsoft to meet those criteria are described below:

Control Activities Expected to be Implemented by Microsoft	Applicable TSC
Microsoft is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2
Microsoft is responsible for restricting logical and physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers supporting the Azure managed cloud services.	CC6.1, CC6.2, CC6.4, CC6.6
Microsoft is responsible for securely disposing of physical assets once they have reached end-of-life.	CC6.5
Microsoft is responsible for the management, review, and validation of any third-party vendors with access to the Azure infrastructure and/or facilities.	CC9.2, C1.1, C1.2
Microsoft is responsible for ensuring the availability of hardware and software services.	A1.1, A1.2, A1.3
Microsoft is responsible for maintaining the confidentiality of information from other Microsoft clients.	C1.1, C1.2

Control Environment

Management at EnovaPoint has implemented management and organizational controls to address risk associated with the overall control environment. EnovaPoint management has documented an organizational chart to document and communicate the organizational structure and hierarchy within the organization.

Employees within the organization are responsible for assigned job responsibilities, which have been documented in written job descriptions that are made available for employee reference. Employees receive on the job training to assist in employee awareness and execution of assigned job responsibilities. In addition, new hire employees are evaluated during the on-boarding process through reference checks to assess qualifications of the position to be fulfilled by the new employee.

Management has established the Code of Conduct. Employees are required to acknowledge reading and understanding the documents upon hire as well as reaffirm and accept them on an annual basis.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how those standards are communicated, and how they are reinforced in practice. Behavioral standards could include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts and the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership's example.

EnovaPoint has implemented, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior. EnovaPoint's management conducts business dealings with employees, suppliers, customers, investors, creditors, competitors, agents, resellers, counsel, accountants, and auditors on a high ethical plane and insists others have similar business practices.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

EnovaPoint assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job. EnovaPoint reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions for the security of information. EnovaPoint's management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions, and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge, and experience required of key personnel and the appropriate number of people to carry out duties. In addition, management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

EnovaPoint has defined job responsibilities and clear communication channels to disseminate information within the organization; this enables EnovaPoint to react to market and regulation changes and to meet its goals and objectives. EnovaPoint is appropriately staffed to support its operations, particularly with respect to critical areas such as software development, implementation, customer support, and IT system support.

HR Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counseling, and remedial action. Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior demonstrate EnovaPoint is committed to hiring and retaining only highly competent and trustworthy people. Training policies were created by EnovaPoint to communicate personnel roles and responsibilities and include practices such as regular training programs to illustrate expected level of performance, IT practices, and employee behavior. Personnel who work for EnovaPoint are required to read and acknowledge the company's internal policies and requirements regarding confidentiality requirements as well as customer managed information.

Risk Assessment

EnovaPoint’s management performs periodic risk assessments, which require management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. EnovaPoint’s management reevaluates the risk assessment at least annually to both update the previous results and to identify any new potential areas of concern.

The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for the other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
- Monitoring – The monitoring phase includes the performance of monitoring activities by EnovaPoint’s management team to evaluate whether the processes, initiatives, functions and/or activities are mitigating the risk as designed.

Information and Communication

Information

Information is necessary for EnovaPoint to carry out internal control responsibilities to support the achievement of its objectives related to the JungleMail Newsletter and JungleDocs Document Automation Platforms. Management obtains or generates relevant and quality information from both internal and external sources to support the functioning of internal control.

Communication

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. EnovaPoint’s management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

Internal Communications

EnovaPoint has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees and ongoing training for employees.

If incidents are communicated, personnel follow documented escalation procedures. Incidents are documented in a central repository and tracked by management until resolved. Formal procedure changes are distributed to management before they are incorporated into the policy and distributed to relevant parties.

External Communications

EnovaPoint has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in communication of significant events. These methods include the EnovaPoint website, e-mail messages, in-app notifications, and customer contact information to communicate time-sensitive information.

Monitoring

Monitoring is generally performed through active, hands-on management, including regularly scheduled meetings to discuss operational issues. Management is involved and active in the business. EnovaPoint utilizes a risk-based approach to monitor business units and other entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance. Results from the risk evaluation are documented in formal communications to Executive management and other relevant parties.

Management strives to be proactive in responding to customer complaints and maintain a high level of inter-departmental communication about these events. Customer complaints and other issues are handled by EnovaPoint's Chief Operating Officer.

User Entity Controls

The control activities performed by EnovaPoint cover only a portion of the overall internal control structure of EnovaPoint's user entities. Therefore, each customer's internal control structure must be evaluated in conjunction with EnovaPoint's control policies and procedures described in this report. EnovaPoint's controls were designed with the understanding that certain user entity controls were in place and operating effectively.

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for notifying EnovaPoint of any approved contact modifications.	CC2.2
User entities are responsible for determining whether EnovaPoint's logical security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.	CC6.1
User entities are responsible for managing their own user access requests to EnovaPoint's systems.	CC6.1

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for ensuring that user IDs and passwords used for accessing the JungleMail Newsletter and JungleDocs Document Automation Platforms are assigned only to authorized individuals and that the roles assigned to the user accounts are appropriate.	CC6.1, CC6.2
User entities are responsible for immediately notifying EnovaPoint of any actual or suspected information security breaches, including compromised user accounts and confidential information.	CC7.3
User entities are responsible for maintaining their own system of record of data files provided to EnovaPoint.	A1.1, A1.2, A1.3
User entities are responsible for using secure methods provided by EnovaPoint to facilitate confidential data transfer.	C1.1
User entities are responsible for providing their data to EnovaPoint in accordance with their corporate confidentiality policies.	C1.1, C1.2

Attachment B - EnovaPoint's Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

EnovaPoint designs its processes and procedures related to its JungleMail Newsletter and JungleDocs Document Automation Platforms to meet its objectives. Those objectives are based on the service commitments that EnovaPoint makes to user entities and the financial, operational, and compliance requirements that EnovaPoint has established for the services provided.

Security commitments to user entities are documented in client agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the JungleMail Newsletter and JungleDocs Document Automation Platforms that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect client data at rest and in transit.

Availability commitments to user entities are documented in client agreements. Availability commitments are standardized and include, but are not limited to, the following:

- Managing software, servers (including storage), network, internet and infrastructure capacity as is necessary to provide a commercially reasonable level of performance of the JungleMail Newsletter and JungleDocs Document Automation Platforms
- Meeting company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.

Confidentiality commitments to user entities are documented in client agreements. Confidentiality commitments are standardized and include, but are not limited to, the following:

- Data retention and disposal policies and procedures are documented and in place.
- Data is stored and maintained in accordance with confidentiality agreements.

EnovaPoint establishes operational requirements that support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in EnovaPoint's system policies and procedures, system design documentation, and agreements 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 the system.

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

Marcum LLP
www.marcumllp.com

Marcum Bernstein & Pinchuk
www.marcumbp.com

Marcum Insurance Services
www.marcumis.com

Marcum RBK Ireland
www.marcumrbk.com

Marcum Search
www.marcumsearch.com

Marcum Strategic Marketing
marketing.marcumllp.com

Marcum Technology
www.marcumtechnology.com

Marcum Wealth
www.marcumwealth.com

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com

MARCUM
ACCOUNTANTS ▲ ADVISORS