BOARD MEETING DATE: April 16, 2024

ITEM: XIII - A

RECOMMEND that the District Board of Trustees for North Florida College approves the Master Subscription Agreement and Order Form from GoodKind Software Corporation.

ATTORNEY REVIEW STATUS: This item has been reviewed and approved by the Board Attorney.

THIS RECOMMENDATION: will allow multiple departments on campus solve the problem of meeting students where they are and effectively communicate throughout key moments in the student experience.

MASTER SUBSCRIPTION AGREEMENT

This Master Subscription and Services Agreement is made as of **March 15, 2024** (the “**Effective Date**”) between Goodkind Software Corporation, a Canadian corporation (“**Goodkind**”) and **North Florida College** (“**Customer**”).

A. Goodkind offers a SaaS platform that empowers organizations to connect and engage with their customers with asynchronous, video-based interactions.

B. Customer wishes to engage Goodkind to provide services to Customer, as described in order forms and statements of work entered into between Goodkind and Customer from time to time.

The parties agree as follows:

1. DEFINITIONS

“**Admin User**” means a natural person who is an employee, contractor or agent of Customer authorized by Customer to use the Services for administrative purposes, and to whom Customer or, when applicable, Goodkind, upon Customer’s written request, has supplied a user identification and password (for Services utilizing authentication). Admin Users may include, for example, employees of Customer or of third parties with which Customer transacts business.

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. For the purposes of this definition, control means direct or indirect ownership or control of more than 50% of the voting interests of the entity or subject entity.

“**Agreement**” means this Master Subscription Agreement and any schedules, exhibits, addenda and hyperlinked documents, and all Order Forms between Goodkind and Customer, as it or they may from time to time be amended or supplemented.

“**Applicable Laws**” means, in respect of any person, property, transaction or event, all applicable Canadian, U.S., or foreign federal, provincial, state, municipal or local government laws, statutes, rules, by-laws and regulations, and all applicable official rules, policies, notices, directives, orders, judgments and decrees of any Governmental Authority, all as amended from time to time.

“**Beta Services**” means Goodkind services or functionality that may be made available to Customer to try at its option and which are clearly designated as beta, pilot, limited release, developer preview, non-production, evaluation, trial, or by a similar description.

“**Content**” means any text, audio, video, images, and other content that is provided by Customer or by others on behalf of Customer, such as (without limitation) information about third party contractors, services, events, and policies. Content does not include Third Party Service Content or Customer Data.

"**Customer Data**" means data submitted by or for Customer to the Services or provided by Goodkind to Customer in output files generated by the Services, excluding Content and Third Party Service Content. The term Customer Data does not include Personal Data or Service Data.

“**Data Center Service Provider**” means any third party retained by Goodkind to provide all or part of the Services at one or more secure data centers at any time during this Agreement.

“**de-identified**” means, in relation to information and a natural person, information that has been processed such that natural persons can no longer be identified, in reasonably foreseeable circumstances, from such processed information either alone or in combination with other information.

“**Documentation**” means the Goodkind documentation and policies applicable to the Services, as amended by Goodkind from time to time, which are generally available to Admin Users through the Web Portal.

“**Force Majeure Event**” means any event or circumstances beyond the reasonable control of a party, including an act of God, act of government, flood, fire, pandemic, epidemic, disease, earthquake, civil unrest, act of terror, strike or other labour problem, Internet or telecommunications service failure or delay, Third Party Service Provider failure or delay, World Health Organization declared pandemic or epidemic (including, but not limited to, COVID-19), recognized health threats as determined by the World Health Organization, the Centers for Disease Control or the Public Health Agency of Canada (but only with respect to new restrictions in effect subsequent to the Effective Date), H1N1 or similar infectious diseases, or government action, decree or order affecting the jurisdiction where the Services are to be provided to Customer or a denial of service attack

“**Governmental Authority**” means any governmental or regulatory authority, agency, commission or board of any applicable Canadian, U.S., or foreign federal, provincial, state, municipal or local government, parliament or legislature, or any court or, without limitation, any other law, regulation or rule-making entity having jurisdiction in the relevant circumstances, and whether now or in the future constituted or existing, or any person acting or purporting to act under the authority of any of them.

“**identified or identifiable**” means, in relation to information and a natural person, that the natural person is specifically identified in the information or that there is a serious possibility that the natural person could be specifically identified through the use of that information, alone or in combination with other reasonably available information, and in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier, or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Malicious Code**” means code, files, scripts, agents or programs intended to do harm, including viruses, worms, time bombs and Trojan horses.

“**Mobile App**” means Goodkind’s mobile application enables Admin Users to record video messages using the platform.

“**Order Form**” means an ordering document describing the Services to be provided under this Agreement that is entered into between Customer and Goodkind, including any schedules, exhibits, addenda and hyperlinked documents, as it or they may from time to time be amended or supplemented. By entering into an Order Form that references this Agreement, an Affiliate agrees to be bound by the terms of this Agreement as if it were an original party to this Agreement.

“**Personal Data**” means any information relating to an identified or identifiable natural person.

“**Platform**” means Goodkind’s proprietary platform comprised of various components, which is made available by Goodkind as a SaaS service.

“**Services**” means the services that are ordered by Goodkind under an Order Form and made available by Goodkind to Customer as SaaS services. Services do not include Third Party Services.

“Storytellers” means a natural person who is an employee, contractor or agent of Customer authorized by Customer to use the Services to record video messages, and to whom Customer or, when applicable, Goodkind, upon Customer’s written request, has supplied a user identification and password (for Services utilizing authentication). Storytellers may include, for example, employees of Customer or of third parties with which Customer transacts business.

“**Third Party Service**” means a service that is provided by a third party through the Platform.

“**Third Party Service Content**” means any text, audio, video, images, and other content that is provided by a Third Party Service Provider (or by others on behalf of the Third Party Service Provider), such as (without limitation) information about the Third Party Services.

“**Third Party Service Provider**” means the provider of a Third Party Service.

“Usage Data” means information about Customer’s and Admin Users’ use or interaction with the Platform and Services.

“**Web Portal**” means Goodkind’s standard web portal that enables Admin Users to obtain access to the Platform for administrative purposes.

2. PROVISION OF SERVICES BY GOODKIND

2.1 Services. Goodkind will make the Services available to Customer pursuant to this Agreement and the applicable Order Forms.

2.2 Beta Services. From time to time, Goodkind may make Beta Services available to Customer. Customer may choose to try such Beta Services or not in its sole discretion. Beta Services are intended for evaluation purposes and not for production use, are not supported, and may be subject to additional terms. Beta Services are not considered “Services” under this Agreement. However, all restrictions, Goodkind reservations of rights, and Customer obligations concerning the Services, and use of any related Third Party Services, will apply equally to Customer’s use of Beta Services. Unless otherwise stated, any Beta Services trial period will expire on the earlier of one year from the trial start date or the date that a version of the Beta Services becomes generally available without the applicable Beta Services designation. Goodkind may discontinue Beta Services at any time in its sole discretion and may never make them generally available. Goodkind will have no liability for any harm or damage arising out of or in connection with a Beta Service.

3. USE OF SERVICES BY CUSTOMER

3.1 Subscriptions. Unless otherwise provided in the applicable Order Form, Services are purchased as subscriptions for the term stated in the applicable Order Form; and (b) any added subscriptions for Services will terminate on the same date as the initial subscription for Services.

3.2 Service Limits. Customer’s access to the Services may be subject to service limits specified in Order Forms, including with respect to the number of Admin Users. Customer will not exceed such service limits, without Goodkind’s prior written consent.

3.3 Customer Responsibilities. Customer shall (a) be responsible for its Affiliates and Admin Users’ compliance with this Agreement, the Documentation and the Order Forms, (b) subject to the service limits, invite and de-authorize any Admin Users using the Web Portal, (c) use commercially reasonable efforts to prevent unauthorized access to or use of the Services and Documentation, and notify Goodkind promptly of any such unauthorized access or use, (d) use Services and Documentation only in accordance with this Agreement, the Documentation, the Order Forms and Applicable Laws, and (e) comply with terms of service of any Third Party Services with which Customer uses the Services and be responsible for its Admin Users’ compliance with such terms of service.

3.4 Customer Restrictions. Customer shall not, or permit any third party to, directly or indirectly: (a) make any Services, Third Party Services or Documentation available to, or use any Services, Third Party Services or Documentation for the benefit of, anyone other than Customer, Affiliates or Admin Users, unless expressly stated otherwise in an Order Form or the Documentation; (b) sell, resell, license, sublicense, distribute, make available, rent or lease any Services, Third Party Services or Documentation, or include any Services, Third Party Services or Documentation in a service bureau or outsourcing offering; (c) use the Services or Third Party Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party rights, including intellectual property rights and privacy rights; (d) use the Services or Third Party Services to store or transmit Malicious Code, or to send spam; (e) interfere with or disrupt the integrity or performance of the Platform or any Services, Third Party Services, or third-party data; (f) attempt to gain unauthorized access to the Platform or any Services, Third Party Services or Documentation or their related systems or networks; (g) permit direct or indirect access to or use of any Services, Third Party Services or Documentation in a way that circumvents a contractual service limit, or use any Services or Third Party Services to access or use any Goodkind intellectual property except as permitted under this Agreement, an Order Form, or the Documentation; (h) copy the Services or the Third Party Services or any part, feature, function or user interface of the Services or the Third Party Services; (i) copy Documentation except for internal use by Customer; (j) frame or mirror any part of any Services, Third Party Services or Documentation, other than framing on Customer's own intranets or otherwise for its own internal business purposes or as permitted in the Documentation; (k) access or use any Services, Third Party Services, or Documentation in order to build a competitive product or service or to benchmark with a non-Goodkind product or service; (l) reverse engineer any Services or Third Party Services or any software used to provide them (to the extent such restriction is permitted by Applicable Laws); or (m) otherwise use the Services in contravention of this Agreement, an Order Form or Documentation. Unless otherwise specified in an Order Form, an Admin User's access credentials may not be shared with any other person and an Admin User's identification may only be reassigned to a new natural person replacing one who will no longer use the Services.

4. FEES AND PAYMENT

4.1 Fees. Customer will pay all fees and expenses specified in Order Forms and this Agreement. Except as otherwise specified in an Order Form, (a) payment obligations are non-cancellable and fees paid are non-refundable, and (b) quantities purchased cannot be decreased during the relevant subscription term. Except as otherwise specified in an Order Form, Customer will also pay reasonable travel, accommodation and meal expenses for pre-approved travel. Customer represents and warrants to Goodkind that all information provided by Customer to Goodkind that is used by Goodkind to calculate the fees is and shall be accurate, true and complete, in all material respects.

4.2 Invoicing and Payment. Unless otherwise stated in the Order Form, (a) fixed fees will be invoiced in advance and variable fees and expenses in arrears, (b) fees and expenses are due net 30 days from the invoice date, and (c) fees and expenses are payable by electronic funds transfer. Customer is responsible for providing complete and accurate billing and contact information to Goodkind and notifying Goodkind of any changes to such information. If Customer does not notify Goodkind in writing of any issue that Customer may have with an invoice within 30 days of the invoice date, then Customer is deemed to have accepted the invoice and Customer waives any right to dispute the amount of the invoice.

4.3 Overdue Charges. If any invoiced amount is not received by Goodkind by the due date, then, without limiting Goodkind's rights or remedies, the invoiced amounts will accrue late interest at the rate of 1.5% of the outstanding balance per month (equivalent to 19.56% per annum), or the maximum rate permitted by law, whichever is lower.

4.4 Taxes. Goodkind's fees and expenses do not include any taxes, levies, duties or similar governmental assessments of any nature, including value-added, HST, GST, sales, use or withholding taxes, assessable by any jurisdiction whatsoever (collectively, "**Taxes**"). Customer is responsible for paying all Taxes associated with its purchases under this Agreement. If Goodkind has the legal obligation to pay or collect Taxes for which Customer is responsible under this section, Goodkind will invoice Customer and Customer will pay that amount unless Customer provides Goodkind with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, Goodkind is solely responsible for taxes assessable against it based on its income, property and employees. All payments by Customer under this Agreement will be without deduction or withholding for Taxes unless Customer is compelled by Applicable Laws to deduct or withhold Taxes, in which event Customer will pay to Goodkind such additional amounts necessary to enable Goodkind to receive, after all deductions and withholdings for such Taxes, a net amount equal to the full amount which would otherwise have been payable under this Agreement if no such deduction or withholding was required.

5. ADDITIONAL TERMS

5.1 Mobile App. Admin Users and Storytellers are solely responsible any data charges and similar fees associated with their respective access and use of the Services through the Mobile App or otherwise through a mobile device.

5.2 Goodkind Security. Goodkind will implement and maintain appropriate technical and organizational measures, as determined by Goodkind, designed to protect the security of Personal Data and non-public Customer Data, including measures designed to protect such data from unauthorized access, use, modification, deletion, loss or disclosure.

5.3 Security Incidents.

(a) Goodkind will report to Customer any material security breach or other event where there is an actual material loss, theft, unauthorized access, acquisition, use, disclosure, alteration, or destruction of or to Personal Data or non-public Customer Data that is within the possession or control of Goodkind (a "**Security Incident**") promptly following determination by Goodkind that a Security Incident has occurred, and in any event within 24 hours following such determination. The initial report will be made to the security contacts designated by Customer from time to time. Customer acknowledges that the Services are provided from the data centers of the Data Center Service Provider, and that Goodkind relies and depends on the Data Centre Service Provider providing notice to Goodkind of Security Incidents relating to those data centers.

(b) Customer will report to Goodkind any Security Incident (not previously reported by Goodkind to Customer) promptly following determination by Customer that a Security Incident has occurred, and in any event within 24 hours following such determination. The initial report will be made to the Goodkind security contacts designated by Goodkind from time to time.

(c) Goodkind will investigate the Security Incident. Goodkind will provide Customer with detailed information about the Security Incident to the extent reasonably possible and to the extent known. Goodkind will take reasonable steps within its systems to mitigate the effects of the Security Incident. Goodkind will use commercially reasonable efforts to provide to Customer the information required by Customer to fulfil any obligations under Applicable Laws to notify Customer, regulators and data subjects of the Security Incident. Customer acknowledges that the Services are provided from a multi-tenant cloud environment used by many Goodkind customers, and that Goodkind may be obligated to provide notice of the Security Breach to other Goodkind customers, Admin Users, and other third parties.

5.4 Applicable Laws. Goodkind will comply with all Applicable Laws which are (a) generally applicable to Goodkind, and (b) generally applicable to Goodkind's provision of the Services to Customer. Customer will comply with all Applicable Laws which are (i) applicable to Customer, (ii) generally applicable to Customer's use of the Services, and (iii) applicable to Customer's collection, use or disclosure of Personal Data of Admin Users.

5.6 Changes to the Services. Subject to Goodkind's obligations under "Warranty for Services", Goodkind may make changes to the Services from time to time, in its discretion, including to add or modify features or functionality.

5.7 Goodkind Personnel, Subcontractors and Service Providers. Goodkind will be responsible for the performance of its personnel, subcontractors and service providers and for their compliance with Goodkind's obligations under this Agreement, except as otherwise specified in this Agreement. For greater certainty, Third Party Service Providers are not subcontractors or service providers of Goodkind.

5.8 Third Party Services. If Customer elects to use any Third Party Services with the Services, then Customer grants Goodkind permission to allow the Third Party Service Provider to access the Services as required for the interoperation of the Third Party Services with the Services. Goodkind is not responsible for any disclosure, modification or deletion of Content, Customer Data or Personal Data resulting from access by the Third Party Service Provider. Any use by Customer of a Third Party Service, and any exchange of data between Customer and the Third Party Service Provider, is solely between Customer and the Third Party Service Provider. Goodkind does not warrant or support Third Party Services or other non-Goodkind products or services, whether or not they are designated by Goodkind as “certified” or otherwise, unless expressly provided in an Order Form. Goodkind does not guarantee the continued availability of Third Party Services. If Goodkind reasonably forms the view that a Third Party Service used with the Services by Customer is causing or will cause Goodkind to violate Applicable Laws or third-party rights, then Goodkind may notify Customer. Promptly after receipt of such notice by Customer, the parties will meet and negotiate in good faith to resolve the issue. If within 10 days after receipt of such notice by Customer (or such longer period as may be agreed between the parties, each acting reasonably) the parties do not agree on a solution or Customer does not instruct Goodkind to disable the applicable Third Party Service, then Goodkind may disable the applicable Third Party Service until the potential violation is resolved.

5.9 Service Data. Goodkind uses Customer Data, Personal Data and Usage Data collected by the Platform and Services in a de-identified form (“**Service Data**”). Goodkind may combine the Service Data with that of other customers. Goodkind may use the Service Data to perform, deliver, support, test and improve the Services, to develop new products and services, to understand usage, and for any other Goodkind business purposes. No identifiable Customer Data or Personal Data is contained in the Service Data, nor any data that would identify any company or organization. Goodkind may combine the Service Data with that of other customers**.**

5.10 Overage fees. Goodkind shall adjust the provision of services to ensure that the Customer's messaging capabilities are restricted to the quantity commensurate with their pre-purchased credits, thereby precluding any excess messaging activity.

6. PROPRIETARY RIGHTS AND LICENSES

6.1 Reservation of Goodkind Rights. Notwithstanding anything to the contrary contained in this Agreement, Goodkind and its licensors have and will retain all right, title and interest in and to the Platform, the Services, the Documentation, and the software and systems used to provide the Platform and the Services (including all patent, copyright, trademark, trade secret and other intellectual property rights), and all copies, modifications, improvements, developments, enhancements and derivative works of any of them. Each Third Party Service Provider and its licensors have and will retain all right, title and interest in and to its Third Party Services, documentation, and the software and systems used to provide the Third Party Services (including all patent, copyright, trademark, trade secret and other intellectual property rights), and all copies, modifications and derivative works of any of them. Customer acknowledges that it is obtaining only a limited right to use the Services, Third Party Services and Documentation. No rights are granted to Customer under this Agreement other than as expressly set forth in this Agreement.

6.2 License by Goodkind for Documentation. Goodkind grants to Customer a worldwide, non-exclusive, non-transferable, royalty-free license to use the Documentation solely for Customer’s internal business purposes associated with its use of the Services, and solely for the applicable subscription term. Customer will reproduce Goodkind’s copyright notice on all copies of the Documentation. On the expiry of the applicable subscription term, Customer will destroy or delete all copies of the Documentation then in its possession or control.

6.3 License by Customer for Content and Customer Data. As between Customer and Goodkind, Customer and its licensors own all right, title and interest in and to all Content and Customer Data. Customer grants Goodkind, its Affiliates and applicable contractors a worldwide, limited-term license to host, copy, transmit and display Content and Customer Data as necessary for Goodkind to perform, deliver, support, test, and improve the Services, and to otherwise provide the Services in accordance with this Agreement and no other purpose.

6.4 License by Customer to use Feedback. Customer grants to Goodkind and its Affiliates a worldwide, perpetual, irrevocable, royalty-free, transferable, sublicensable (through multiple tiers) license to use and incorporate into its services any suggestion, enhancement request, recommendation, correction or other feedback provided by Customer or Admin Users.

7. CONFIDENTIALITY

7.1 Definition of Confidential Information. "**Confidential Information**" means all information disclosed by a party ("**Disclosing Party**") to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information of Customer includes non-public Customer Data. Confidential Information of Goodkind includes the Platform, the Services and the Documentation. Confidential Information of each party includes the terms of this Agreement and all Order Forms (including pricing), as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that (a) is or becomes generally known to the public without breach of any obligation owed by the Receiving Party to the Disclosing Party; (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (c) is received from a third party without breach of any obligation owed to the Disclosing Party; or (d) was independently developed by the Receiving Party without reference to or use of the Confidential Information of the Disclosing Party.

7.2 Protection of Confidential Information. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care) to (a) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (b) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those in this Agreement. Customer shall not disclose Goodkind's Confidential Information to any person who would reasonably be understood to be a competitor of Goodkind or the personnel of any such person without the prior written consent of Goodkind (which consent may be conditioned on such party entering into a non-disclosure agreement directly with Goodkind). Goodkind may disclose relevant aspects of Customer's Confidential Information to Third Party Service Providers, to the extent that such disclosure is reasonably necessary for the provision of Third Party Services. Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel and accountants without the other party's prior written consent, provided that a party that makes any such disclosure to its Affiliates, legal counsel or accountants will remain responsible for such Affiliates', legal counsel's or accountant's compliance with this "Confidentiality" section.

7.3 Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, then the Disclosing Party will reimburse the Receiving Party for its reasonable costs of compiling and providing secure access to that Confidential Information.

7.4 Return of Confidential Information. Except as otherwise expressly provided below, on the request of the Disclosing Party, the Receiving Party will (a) return or destroy all tangible forms of Confidential Information of the Disclosing Party in its possession or control, (b) use all commercially reasonable efforts to erase or destroy all electronic copies of such Confidential Information, and (c) certify to the Disclosing Party that such materials have been either returned, erased or destroyed, in each case except as to signed original copies of any contractual documents or other materials customarily held by the Receiving Party as legal archival material. Notwithstanding the above, the Receiving Party may retain copies of the Confidential Information of the Disclosing Party for archival, audit, legal and/or regulatory purposes.

8. WARRANTIES AND DISCLAIMERS

8.1 Warranties for Services. Goodkind warrants that during an applicable subscription term (a) the Services will perform materially in accordance with the applicable Documentation, and (b) Goodkind will not materially decrease the overall functionality of the Services. For any breach of this warranty, Customer's exclusive remedy and Goodkind's entire liability will be for Goodkind to use commercially reasonable efforts to cause the Services to comply with the warranty within a reasonable period of time after receipt of notice in writing from Customer.

8.2 Disclaimers. EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTY OR CONDITION OR OTHER TERM OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES OR CONDITIONS OR OTHER TERMS, INCLUDING ANY STATUTORY OR IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. THIRD PARTY SERVICES AND BETA SERVICES ARE PROVIDED "AS IS," AND AS AVAILABLE, EXCLUSIVE OF ANY WARRANTY WHATSOEVER. GOODKIND DOES NOT WARRANT THAT THE SERVICES WILL OPERATE ERROR FREE OR WITHOUT INTERRUPTION OR DELAY, THAT THE SERVICES WILL MEET ALL OF CUSTOMER'S REQUIREMENTS, OR THAT THE SERVICES SATISFY ALL APPLICABLE LAWS OR REGULATORY REQUIREMENTS THAT ARE APPLICABLE TO CUSTOMER. GOODKIND DISCLAIMS ALL LIABILITY AND INDEMNIFICATION OBLIGATIONS FOR ANY HARM OR DAMAGES CAUSED BY ANY DATA CENTER SERVICE PROVIDER.

8.3 Future Functionality. Customer agrees that, unless otherwise expressly provided in an Order Form, Customer's purchases of the Services are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Goodkind regarding future functionality or features.

9. MUTUAL INDEMNIFICATION

9.1 Indemnification by Goodkind. Goodkind will defend Customer against any claim, demand, suit or proceeding made or brought against Customer by a third party alleging that any Service infringes or misappropriates such third party's intellectual property rights (a "**Claim Against Customer**"), and will indemnify Customer from any damages, legal fees and costs finally awarded against Customer as a result of, or for amounts paid by Customer under a settlement approved by Goodkind in writing of, a Claim Against Customer, provided Customer (a) promptly gives Goodkind written notice of the Claim Against Customer, (b) gives Goodkind sole control of the defense and settlement of the Claim Against Customer (except that Goodkind may not settle any Claim Against Customer unless the settlement unconditionally releases Customer of all liability), and (c) gives Goodkind all reasonable assistance, at Goodkind's expense. If Goodkind receives information about an infringement or misappropriation claim related to the Services, Goodkind may in its discretion and at no cost to Customer (i) modify the Services so that they are no longer claimed to infringe or misappropriate, subject to Goodkind's warranties under "Warranties for Services", (ii) obtain a license for Customer's continued use of the Services in accordance with this Agreement, or (iii) if the options under clauses (i) or (ii) are not possible on terms that Goodkind considers to be commercially reasonable, terminate Customer's subscriptions for the Services on 30 days' written notice and refund Customer any prepaid fees covering the remainder of the subscription terms of the terminated subscriptions. The above defence and indemnification obligations do not apply to the extent a Claim Against Customer arises from (A) a Third Party Service or Customer's use of a Third Party Service, (B) Customer's breach of this Agreement, the Documentation, applicable Order Forms or the service terms applicable to Third Party Services, (C) use or combination of the Services with any other product or service, (D) modification of the Services or any component without Goodkind's express written approval, or (E) use of the Services for any purpose or in any manner other than as specifically contemplated by this Agreement without Goodkind's express written approval. Nothing contained in this Agreement shall constitute a waiver of sovereign immunity or the limitations on liability contained in Chapter 768, Florida Statutes.

9.2 Indemnification by Customer. Customer will defend Goodkind against any claim, demand, suit or proceeding made or brought against Goodkind by a third party alleging that any Customer Data or Content, or any Customer communication that infringes or misappropriates such third party's intellectual property rights or other rights, or arising from Customer's use of the Services, Third Party Services or Documentation in breach of this Agreement, the Documentation, any Order Form or Applicable Laws (each a "**Claim Against Goodkind**"), and will indemnify Goodkind from any damages, legal fees and costs finally awarded against Goodkind as a result of, or for any amounts paid by Goodkind under a settlement approved by Customer in writing of, a Claim Against Goodkind, provided Goodkind (a) promptly gives Customer written notice of the Claim Against Goodkind, (b) gives Customer sole control of the defence and settlement of the Claim Against Goodkind (except that Customer may not settle any

Claim Against Goodkind unless the settlement unconditionally releases Goodkind of all liability), and (c) gives Customer all reasonable assistance, at Customer's expense.

9.3 Exclusive Remedy. This "Mutual Indemnification" section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this section.

10. LIMITATION OF LIABILITY

10.1 Limitation of Liability. IN NO EVENT SHALL THE MAXIMUM AGGREGATE LIABILITY OF GOODKIND AND ITS AFFILIATES, SUBCONTRACTORS, SERVICE PROVIDERS, LICENSORS, AND THIRD PARTY SERVICE PROVIDERS, AND ITS AND THEIR DIRECTORS, OFFICERS, EMPLOYEES AND AGENTS (COLLECTIVELY, THE "**GOODKIND TEAM**"), FOR ALL CLAIMS, ACTIONS, DAMAGES, LIABILITIES, COSTS AND EXPENSES OF EVERY KIND AND NATURE, INCLUDING LEGAL FEES AND EXPENSES (COLLECTIVELY, "**LOSSES**") ARISING OUT OF OR RELATED TO THE SERVICES OR UNDER OR IN CONNECTION WITH THIS AGREEMENT, EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER FOR THE SERVICES DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THESE LIMITATIONS WILL APPLY WHETHER AN ACTION IS IN CONTRACT (INCLUDING AN INDEMNITY) OR TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY.

10.2 Exclusion of Consequential and Related Damages. IN NO EVENT WILL CUSTOMER OR ANY MEMBER OF THE GOODKIND TEAM HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THE SERVICES OR UNDER OR IN CONNECTION WITH THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES OR GOODWILL, FAILURE TO REALIZE EXPECTED SAVINGS, OR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, COVER, BUSINESS INTERRUPTION OR DOWNTIME COSTS, THIRD-PARTY DAMAGES (INCLUDING ANY SERVICE LEVEL CREDITS PAYABLE BY CUSTOMER OR ANY OTHER PERSON), LOSS OF DATA, OR PUNITIVE, EXEMPLARY OR AGGRAVATED DAMAGES, WHETHER AN ACTION IS IN CONTRACT (INCLUDING UNDER AN INDEMNITY) OR TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THIS DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW AND WILL NOT LIMIT CUSTOMER'S PAYMENT OBLIGATIONS UNDER "FEES AND PAYMENT".

10.3 Proportional Liability. Any liability of a party for Losses, however caused (including by negligence), in connection with the Services or this Agreement is reduced to the extent that the other party or its Affiliates, or its or their employees, contractors or agents, contribute to the Losses.

10.4 No double claiming. Neither party will be able to recover the same Loss more than once by bringing separate claims under or in connection with this Agreement.

11. TERM AND TERMINATION

11.1 Term of Agreement. This Agreement commences on the Effective Date and continues until all subscriptions under this Agreement have expired or have been terminated.

11.2 Term of Subscriptions. The term of each subscription will be as specified in the applicable Order Form. Except as otherwise specified in an Order Form, subscriptions will automatically renew for additional periods equal to the expiring subscription term or one year (whichever is shorter), unless either party gives the other notice of non-renewal at least 30 days before the end of the relevant subscription term. The pricing during any renewal term will increase by 10% or more against the applicable pricing in the prior term, unless Goodkind provides Customer notice of different pricing at least 30 days prior to the applicable renewal term. The parties will sign a new Order Form for each renewal.

11.3 Termination for Breach. Either party may terminate this Agreement and/or any Order Form, immediately upon written notice to the other party if the other party (a) materially breaches this Agreement and, where curable, failures to cure such breach within 30 days after its receipt of written notice of such breach, or (b) becomes the subject of a petition in bankruptcy, insolvency proceeding, receivership, liquidation or composition for the benefit of creditors. If any Order Forms are terminated by Customer in accordance with this Section 11.3, then Goodkind will refund Customer any prepaid fees covering the remainder of the subscription terms of the terminated subscriptions. In no event will termination relieve Customer of its obligation to pay any fees for the period prior to the effective date of termination. If this Agreement is so terminated by Goodkind, then Customer will pay to Goodkind an amount equal to the aggregate of all fees payable for the Services for the remainder of the subscription terms applicable to the Services.

11.4 Surviving Provisions. Any sections that by their nature are intended to survive the termination or expiry of this Agreement will survive any termination or expiration of this Agreement.

11.5 Suspension. Goodkind may suspend use of some or all of the Services if Goodkind believes the suspension is reasonably needed to prevent unauthorized access to the Platform, or for other security reasons, or to otherwise protect Goodkind's systems or other customers. In such circumstances, Goodkind will give as much notice as reasonably possible before Goodkind suspends, except where Goodkind reasonably believes that Goodkind needs to suspend immediately. Goodkind may also suspend use of some or all of the Services on 30 days written notice to Customer if (a) Customer does not pay any undisputed amounts that are due under this Agreement within 30 days of their due date, or (b) Customer or an Admin User is in material breach of this Agreement, and if either such breach remains uncured at the expiration of such 30 day notice period. A suspension will remain in effect only for so long as the condition or need exists.

12. GENERAL PROVISIONS

12.1 Export Compliance. The Platform, the Services, other Goodkind technology, and derivatives of them may be subject to export laws and regulations of Canada, the United States, and other jurisdictions. Goodkind and Customer each represents that it is not named on any Canadian or U.S. government denied-party list. Customer will not permit any Affiliate or Admin User to access or use any Service in a country named on Canada's Area Control List under Canada's Export and Import Permits Act, in a U.S.-embargoed country or region (currently Cuba, Iran, North Korea, Sudan, Syria or Crimea), or provide the Services to an Affiliate that is, or appoint as an Admin User any person or entity that is, prohibited from receiving U.S. exports, or otherwise use the Services in violation of any Canadian or U.S. export law or regulation.

12.2 Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate this restriction.

12.3 Employee Non-Solicitation. During the term of this Agreement and for one year after the expiry of the term, Customer will not, either on its own account or for any other person, endeavour to employ or contract with any employee of Goodkind, its Affiliates, or its or their contractors, with whom Customer has dealt in relation to this Agreement. This restriction will not prevent Customer from making general advertisements or other solicitations to the public or from hiring any employee of Goodkind, its Affiliates, or its or their contractors who responds to such an advertisement or who otherwise initiates discussions with Customer. In the event of a breach of this provision, Customer will pay to Goodkind an amount equal to 6 months' salary of the applicable employee, as liquidated damages and not as a penalty.

12.4 Entire Agreement and Order of Precedence. This Agreement is the entire agreement between Goodkind and Customer regarding the Services, and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. The parties agree that any term or condition stated in a Customer purchase order or in any other Customer order documentation (excluding Order Forms) is void. This Agreement may not be amended except by a written amending agreement signed by duly authorized officers of both parties. In the event of any conflict or inconsistency among the following documents, the order of precedence will be (a) the applicable Order Form; (b) any schedule, exhibit, addendum or hyperlinked document to this Agreement; (c) the body of this Agreement; and (d) the Documentation.

12.5 Force Majeure Events. Neither party will be liable for damages caused by delay or failure to perform its obligations under this Agreement to the extent such delay or failure is caused by a Force Majeure Event; provided that the affected party: (a) provides the other party with prompt notice of the nature and expected duration of the

Force Majeure Event; (b) uses commercially reasonable efforts to address and mitigate the cause and effect of such Force Majeure Event; (c) provides periodic notice of relevant developments; and (d) provides prompt notice of the end of such Force Majeure Event. This provision will not excuse a failure to make a payment when due.

12.6 Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

12.7 Third-Party Beneficiaries. The Goodkind Team are third party beneficiaries of Section 10. There are no other third-party beneficiaries under this Agreement.

12.8 Publicity. Goodkind may issue a press release announcing the relationship between Customer and Goodkind and Customer will have the right to review and approve the press release prior to distribution; (b) Goodkind may publicize the launch of the Services (in coordination with Customer); (c) Goodkind may list Customer as a customer of Goodkind on the Goodkind website and on other Goodkind sales and promotional materials; and (d) for each of these purposes, Goodkind may make reasonable use of Customer's video messages, logos and trademarks in marketing and sales material. Any Goodkind use of Customer's logos and trademarks will be subject to any applicable trademark use guidelines provided by Customer to Goodkind from time to time.

12.9 Notices. All notices, requests, demands, claims, and other material communications under this Agreement must be in writing, and will be deemed duly given when delivered personally or by courier, or when delivered by email if receipt of the email is acknowledged by the intended recipient, in each case addressed to the intended recipient as follows:

If to Customer:

325 Turner Davis Dr
Madison, FL United States
32340

Attention: Allison Finley
Email: finleya@nfc.edu

If to Goodkind:

Goodkind Software Corporation
201-670 Bloor Street West
Toronto, ON Canada
M6G 1L2

Attention: Justin Rotman, Co-founder & CEO
Email: justin@goodkind.com

Either party may change its address for notice from time to time by notice given in accordance with this section.

12.10 Waivers. A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by or on behalf of the waiving party. No omission, delay or failure to exercise any right or power, or any waiver by either party of any breach or default, whether express or implied, or any failure to insist on strict compliance with any provision of this Agreement, will constitute a waiver of any other provision. Any waiver of any provision of this Agreement will not constitute a continuing waiver unless otherwise expressly provided.

12.11 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to Applicable Laws, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

12.12 Assignment. Neither party may assign any of its rights or obligations under this Agreement, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld). Notwithstanding this restriction, either party may assign this Agreement in its entirety (including all Order Forms) without the consent of the other party to any Affiliate or to a purchaser of all or substantially all of the assets of such party. The assigning party will obtain from the permitted assignee and deliver to the other party an undertaking in writing in favour of the other party (in form and content acceptable to the other party, acting reasonably) to be bound by and to perform all of the obligations of the assigning party under this Agreement. The assigning party and the permitted assignee will be jointly and severally liable to the other party for all of the assigning party's obligations under this Agreement. Any assignment in contravention of the above will not be effective against the non-assigning party.

12.13 Interpretation. The parties agree that this Agreement was drafted with the participation of both parties and will not be construed either against or in favour of either party. All amounts specified in this Agreement or an Order Form are in American dollars, unless otherwise specified. The term "including" and similar terms will mean "including without limitation". Except where otherwise expressly provided in this Agreement, remedies provided for in this Agreement shall be cumulative and in addition to and not in lieu of any other remedies available to either party at law, in equity or otherwise. The parties agree that this Agreement and all dealings in connection with this Agreement will be in English, and all Services will be provided in English, unless otherwise agreed by the parties.

12.14 Dispute Resolution.

(a) If any dispute or disagreement of any kind arises at any time with respect to this Agreement, its interpretation or application, its performance by the parties, or in respect of any defined legal relationship associated with or derived from this Agreement or its performance (a "**Dispute**"), the parties agree that good faith negotiations shall take place between the parties with the objective of resolving the Dispute. If such good faith negotiations have not resolved the Dispute within a period of 14 days, the dispute or disagreement shall be referred to the Chief Executive Officers of the parties or their designates who will attempt in good faith to resolve such dispute or disagreement.

(b) If within the next following period of 14 days, the Dispute has not been resolved to the satisfaction of the parties, the Dispute shall be referred to binding arbitration pursuant to the Arbitration Act (Ontario) or the International Commercial Arbitration Act (Ontario), as applicable. Within 10 days of the giving of such notice of arbitration, the parties will jointly select a single arbitrator who will be independent of the parties and acceptable to the parties. If a single arbitrator has not been selected during such 10 day period, then, unless the parties agree otherwise, the Dispute will be resolved by a single arbitrator appointed pursuant to the Arbitration Act (Ontario) or the International Commercial Arbitration Act (Ontario), as applicable, on application by either party. The fees and expenses of the arbitrator will be borne equally between the parties. The arbitrator may order interest on any award and the arbitrator may award costs to either party. In the absence of any such award of costs, each of the parties will bear its own costs of the arbitration. The arbitration will take place in Toronto, Ontario, unless the parties agree otherwise.

(c) The parties agree that negotiations and arbitration will all be without recourse to the courts and that the award of the arbitrator will be final and binding, except that (i) either party may appeal an arbitration award to the courts of Ontario on a question of law, and (ii) either party may apply to the courts of Ontario for an interim measure of protection or for any order for equitable relief which the arbitrator does not have the jurisdiction to provide.

(d) Subject to any express rights of suspension provided in this Agreement, the parties will continue to perform their obligations under this Agreement pending resolution of any Dispute.

12.15 Governing Law. This Agreement, and any disputes arising out of or related to this Agreement, will be governed exclusively by the laws of the state of Florida and the federal laws of the United States of America applicable in the state of Florida, without regard to its conflicts of laws rules or the United Nations Convention on the International Sale of Goods. Subject to "Dispute Resolution", the provincial and federal courts located in Madison, Florida will have exclusive jurisdiction over any disputes arising out of or related to this Agreement, and each party consents to the exclusive jurisdiction of those courts.

12.16 Counterparts. The parties agree that this Agreement may be executed by electronic means, and in counterparts.

12.17 Public Records Access. Goodkind must keep and maintain public records as defined in Chapter 119, Florida Statutes. Upon request from the Customer's custodian of public records, Goodkind must provide the Customer with a copy of the requested public records or allow the records to be inspected or copied within a reasonable time at a cost not to exceed that permissible under Chapter 119, Florida Statutes, or as otherwise provided by Florida Law. Goodkind may not disclose those records which are exempt or confidential pursuant to Florida Law. Upon completion of this Agreement, Goodkind shall transfer to the Customer all public records in its possession or shall keep and maintain such records for those periods required by Florida Law. If Goodkind transfers such records, it shall destroy any duplicate records which are confidential or exempt from disclosure. The Customer may unilaterally terminate this contract if Goodkind refuses to allow access to public records made or maintained by Goodkind in conjunction with this Agreement unless such records are exempt from Article 1 section 24 of the Florida Constitution and Chapter 119, Florida Statutes.

[*signature page follows*]

To confirm their agreement, the parties have signed this Agreement as of the Effective Date.

North Florida College

Per: ____
Name: ____
Title: ____
Date:

Goodkind Software Corporation

Per: ____
Name: ____
Title: ____
Date:

-

goodkind

Goodkind Software Corporation

SOC 2 REPORT

FOR THE

Goodkind Cloud-Hosted Software Application

TYPE 1 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY & AVAILABILITY

15th November 2023

Attestation and Compliance Services

CertPro

Effective. Efficient. Economical.

This report is intended solely for use by the management of Goodkind Software Corporation, user entities of Goodkind Software Corporation’s services, and other parties who have sufficient knowledge and understanding of Goodkind Software Corporation’s services covered by this report (each referred to herein as a “specified user”).

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against CertPro and the service auditor as a result of such access. Further, CertPro and the service auditor do not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Board of Directors
Goodkind Software Corporation

Scope

We have examined the accompanying "Description of Goodkind, a Cloud-Hosted Software Application" provided by Goodkind Software Corporation as on 15th November 2023 (the Description) and the suitability of the design and operating effectiveness of controls to meet Goodkind Software Corporation's service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity & Privacy principles set forth in TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Confidentiality and Availability (applicable trust services criteria) as on 15 November 2023.

Goodkind Software Corporation uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-As-A-Service (SaaS), Microsoft Azure, a cloud computing service operated by Microsoft for application management, GitHub, a cloud computing service operated by GitHub Inc. (GitHub), a subservice organization, to provide and host the GitHub application, and Google Workspace, a collection of cloud computing, productivity and collaboration tools, software, and products such as Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more. The description presents Goodkind Software Corporation's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Goodkind Software Corporation's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description presents Goodkind Software Corporation's controls, the applicable trust services criteria and the types of complementary user entity controls assumed in the design of Goodkind Software Corporation's controls. The description does not disclose the actual controls at the user entity organizations. Our examination did not include the services provided by the user entity organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service organization's responsibilities

Goodkind Software Corporation has provided the accompanying assertion titled "Goodkind Software Corporation's Management Assertion as on 15th November 2023" about the fairness of the presentation of the Description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet Goodkind Software Corporation's service commitments and system requirements based on the applicable trust services criteria. Goodkind Software Corporation is responsible for: (1) preparing the description and assertion; (2) the completeness, accuracy and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) specifying the controls that meet Goodkind Software Corporation's service commitments and system requirements based on the applicable trust services criteria and stating them in the description; (6) designing, implementing, maintaining and documenting controls to meet Goodkind Software Corporation's service commitments and system requirements based on the applicable trust services criteria stated in the description.

Service Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Goodkind Software Corporation's assertion and on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that the service organizations commitments and system requirements were met based on applicable trust services criteria.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria and (2) the controls were suitably designed to provide reasonable assurance that the service organization's commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria (3) the controls operated effectively to provide reasonable assurance that the service organization's commitments and system requirements were achieved based on the applicable trust services criteria as on 15 November 2023.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's commitments and system requirements meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the service organization's commitments and system requirements based on the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

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 it's own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria.

Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Description of tests of controls

In Section III, the specific controls tested and the nature and timing, and results of those tests are listed in the accompanying description of Criteria, Controls, Tests and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the description criteria described in Goodkind Software Corporation's assertion and the applicable trust services criteria:

a. The description fairly presents Goodkind, a cloud-hosted software application, provided by Goodkind Software Corporation that were designed and implemented as on 15 November 2023.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the service organizations commitments and system requirements would be achieved if the controls operated effectively based on the applicable trust services criteria and if sub-service organizations and user entities applied the controls contemplated in the design of Goodkind Software Corporation’s controls as on 15 November 2023

c. The controls tested, which were those necessary to provide reasonable assurance that the service organizations commitments and system requirements based on the applicable trust services principles criteria were met, operated effectively as on 15 November 2023

Restricted Use

This report, including the description of tests of controls and results thereof in the description of tests and results is intended solely for the information and use of user entities of Goodkind Software Corporation’s Goodkind, a cloud-hosted software application as on 15 November 2023, and prospective user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of service provided by the service organization.
- How the service organizations’ system interacts with the user entities, subservice organizations, or other parties
- Internal controls and its limitations
- Complementary subservice organizations and complementary user entity controls and how those controls interact with the controls at the service organizations to achieve the service organization’s service commitments and system requirements.
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

JAY MARU CPA
License no.
41401
Washington State

JAY MARU
Certified Public Accountant
License Number: 41401
08th December 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

Goodkind Software Corporation's Management Assertion as on 15 November 2023

We have prepared the attached description titled "Description of Goodkind Software Corporation's cloud-hosted software application, Goodkind" as on 15 November 2023 (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 given in DC Section 200 prepared by AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2® Guide Working Group to be used in conjunction with the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Goodkind provided by Goodkind Software Corporation, that may be useful when assessing the risks from interactions with the system as on 15 November 2023 particularly information about the suitability of the design and operating effectiveness of controls to meet Goodkind Software Corporation service commitments and system requirements based on the criteria related to Security, Confidentiality & Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy, (AICPA, Trust Services Criteria).*

Goodkind Software Corporation uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-As-A-Service (SaaS), Microsoft Azure, a cloud computing service operated by Microsoft for application management, GitHub, a cloud computing service operated by GitHub Inc, (GitHub), a subservice organization, to provide and host the GitHub application, Google Workspace, a collection of cloud computing, productivity and collaboration tools, software, and products such as Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Goodkind Software Corporation, to achieve Goodkind Software Corporation's service commitments and system requirements based on the applicable trust services criteria. The description presents Goodkind Software Corporation's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Goodkind Software Corporation' s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity organization controls that are suitably designed and operating effectively are necessary, along with controls at Goodkind Software Corporation, to achieve Goodkind Software Corporation's service commitments and system requirements based on the applicable trust services criteria. The description presents Goodkind Software Corporation's controls, the applicable trust services criteria and the types of complementary user entity organization controls assumed in the design of Goodkind Software Corporation's controls. The description does not disclose the actual controls at the user entity organizations.

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

a) The "description of Goodkind, a cloud-hosted software application" provided by Goodkind Software Corporation as on 15 November 2023 the criteria for description are identified below under the heading "Description Criteria".

b) The controls stated in the description were suitably designed and operated effectively to meet Goodkind Software Corporation's service commitments and system requirements based on the applicable trust services criteria as on 15 November 2023, to meet the applicable trust services criteria.

Description Criteria:

i. The description contains the following information:

1. The types of services provided.
2. The principal service commitments and system requirements.
3. The components of the system used to provide the services, which are the following:
    - Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).
    - Software. The programs and operating software of a system (systems, applications, and utilities).
    - People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
    - Procedures. The automated and manual procedures involved in the operation of a system.
    - Data. The information used and supported by a system (transaction streams, files, databases, and tables).
4. The boundaries or aspects of the system covered by the description.
5. The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved.
6. Other aspects of the service organization’s control environment, risk assessment process, communication and information 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 organizations’ 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 needs.

For Goodkind Software Corporation

Authorized Signatory

Michael Warshafsky

Founder & Chief Operating Officer

Section 3

Description of the System

Overview of Operations

Types of Services Provided

Goodkind is a cloud-hosted software application built by Goodkind Software Corporation (hereby referred to as Goodkind).

Goodkind is a video-first engagement platform made for higher education institutions. Founded during the pandemic and during falling new student enrollment trends, Goodkind helps customers admit more students and retain them. The Goodkind platform has 4 products: video messaging, video reels, SMS, and chatbot. The Goodkind platform's products all work with each other and bolt onto a customer's CRM and student information system. In an age of declining attention,

Goodkind's goal is to build a modern toolbox to help universities and colleges not only survive but thrive.

Any other services provided by Goodkind are not in the scope of this report.

Principal Service Commitments and System Requirements

Goodkind designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Goodkind makes to customers and the compliance requirements that Goodkind has established for their services.

Security commitments to user entities are documented and communicated in Goodkind’s customer agreements, as well as in the description of the service offering provided online. Goodkind’s security commitments are standardized and based on some common principles.

These principles include but are not limited to, the following:

1. The fundamental design of Goodkind’s software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
2. Goodkind implements various procedures and processes to control access to the production environment and the supporting infrastructure.
3. Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Goodkind and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Goodkind establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Goodkind’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 networks are managed, and how staff is hired.

Components of the System used to provide services

Infrastructure & Network Architecture

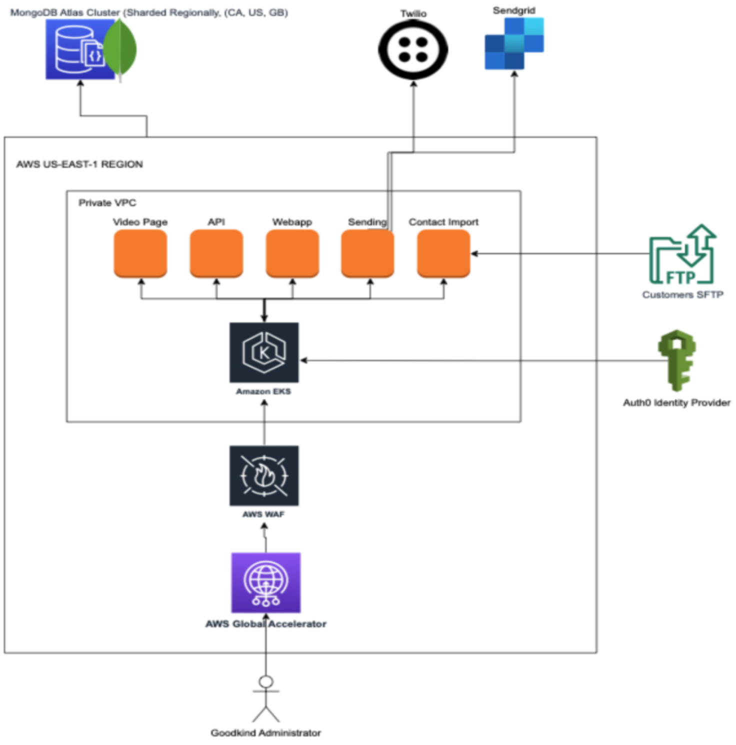
The production infrastructure for the Goodkind software application is hosted on Amazon Web Services and Microsoft Azure in their various regions across Us-east-1.

Goodkind software application uses a virtual and secure network environment on top of Amazon Web Services and Microsoft Azure infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. Goodkind software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer’s client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the Amazon Web Services and Microsoft Azure Internet Gateway, over to a Virtual Private Cloud that:

1. Houses the entire application runtime.
2. Protects the application runtime from any external networks.

The internal networks of Amazon Web Services and Microsoft Azure are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through. Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS Guard duty to spot malicious activity and unauthorized behavior. Specifically, AWS Guard Duty uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats.



Software

Goodkind Software Corporation is responsible for managing the development and operation of the Goodkind platform including infrastructure components such as servers, databases, and storage systems. The in-scope Goodkind infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**Underlying Operating System & Storage**	**Physical Location**
Goodkind Application	Access to the Goodkind SaaS application is through a web/mobile interface and user authentication.	MongoDB Atlas, Linux	Amazon Web Services and Microsoft Azure Us-east-1
Amazon Web Services and Microsoft Azure IAM	Identity and access management console for AWS resources.	Amazon Web Services and Microsoft Azure Proprietary	Amazon Web Services and Microsoft Azure
Amazon Web Services and Microsoft Azure Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	Amazon Web Services and Microsoft Azure Proprietary	Amazon Web Services and Microsoft Azure
GitHub App	Source code repository, version control system, and build software.	GitHub App	GitHub App Cloud

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**Underlying Operating System & Storage**	**Physical Location**
Google Workspace	Identity/Email provider for all Goodkind employees	Google Workspace Proprietary	Google Workspace

Supporting Tools	
System / Application	**Business Function / Description**
Javascript	Programming Language used for Goodkind application
Sprinto	Provide continuous compliance monitoring of the company's system.
Google Workspace	Office communication services

People

Goodkind's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel has also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support the Goodkind software application. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter). Goodkind also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Goodkind software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Data

Data, as defined by Goodkind, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

All data that is managed, processed, and stored as a part of the Goodkind software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally or was entrusted to Goodkind Software Corporation by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Goodkind Software Corporation's PII • Unpublished financial information • Documents and processes explicitly marked as confidential. • Unpublished goals, forecasts, and initiatives marked as confidential. • Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases • Public website

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data backup policy.

Physical Security

The in-scope system and supporting infrastructure are hosted by Amazon Web Services and Microsoft Azure. As such, Amazon Web Services and Microsoft Azure is responsible for the physical security controls of the in-scope system. Goodkind reviews the SOC 2 report provided by Amazon Web Services and Microsoft Azure on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Goodkind software application.

Logical Access

The Goodkind software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates the database.

Goodkind has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires multi-factor authentication (MFA) wherever possible. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Goodkind customer data. Staff is encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special character based. Password configuration settings are configured on each critical system. Additionally, company-owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Change Management

A documented Change Management policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Goodkind system are reviewed, deployed, and managed. The policy covers all changes made to the Goodkind software application, regardless of their size, scope, or potential impact.

The change management policy is designed to mitigate the risks of

- Corrupted or destroyed information.
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc

A change to the Goodkind software application can be initiated by a staff member with an appropriate role. Goodkind uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities. Further AWS CloudTrail is configured to track all changes to the production infrastructure.

Incident Management

Goodkind has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Goodkind via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of Goodkind being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.

- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.

- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.

- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Cryptography

User requests to Goodkind's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to Goodkind web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Goodkind uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that includes policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

Availability

Goodkind has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Boundaries of the System

The scope of this report includes the Goodkind software application. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

Goodkind depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

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

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Goodkind's description of the system. This section provides information about the five interrelated components of internal control at Goodkind, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

Control Environment

Integrity & 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 Goodkind’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Goodkind’s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Goodkind and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members.
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Goodkind’s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees’ roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data..
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

Goodkind’s management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management’s approach to monitoring business risks, and management’s attitudes toward personnel and the processing of information.

Goodkind's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities that the Goodkind has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.

Organizational Structure and Assignment of Authority and Responsibility

Goodkind’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring 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. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources Policies and Practices

Goodkind's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

Specific control activities that the Goodkind has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

Goodkind's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Goodkind identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Goodkind software application, and the management has implemented various measures designed to manage these risks.

Goodkind believes that effective risk management is based on the following principles:

1. Senior management's commitment to the security of Goodkind software application
2. The involvement, cooperation, and insight of all Goodkind staff
3. Initiating risk assessments with discovery and identification of risks

4. A thorough analysis of identified risks
5. Commitment to the strategy and treatment of identified risks
6. Communicating all identified risks to the senior management
7. Encouraging all Goodkind staff to report risks and threat vectors

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Goodkind software application. The Goodkind risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Goodkind's Information Security Officer and the department or individuals responsible for the area being assessed. All Goodkind staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

Goodkind uses a number of vendors to meet its business objectives. Goodkind understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Goodkind employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Goodkind assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Goodkind's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Goodkind management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Goodkind Software Corporation identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Goodkind Software Corporation's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Control Activities

Goodkind's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Monitoring

Goodkind management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Information and Communication Systems

Goodkind maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, Goodkind also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Significant Events and Conditions

Goodkind has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the software application.

Trust Services Categories

The following Trust Service Categories are in scope: **Common Criteria (to the Security, Confidentiality, and Availability Categories).**

1. **Security** refers to the protection of:
    a. information during its collection or creation, use, processing, transmission, and storage, and
    b. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or another unauthorized removal of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

2. **Confidentiality** addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the

collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

3. **Availability** refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Any applicable trust services criteria that are not addressed by control activities at Goodkind Software Corporation are described within the sections titled **"Complementary Customer controls"** and "**Complementary Subservice Organization Controls**".

Complementary Customer Controls

Goodkind's controls related to Goodkind cover a subset of overall internal control for each user of the software application. The control objectives related to Goodkind cannot be achieved solely by the controls put in place by Goodkind; each customer's internal controls need to be considered along with Goodkind's controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Complementary Customer Control List	Related Criteria
Customers are responsible for managing their organization's Goodkind software application account as well as establishing any customized security solutions or automated processes through the use of setup features	CC5.1, CC5.2, CC5.3, CC6.1
Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Goodkind software application account	CC5.2, CC6.3
Customers are responsible for notifying Goodkind of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Goodkind software application.	CC7.2, CC7.3, CC7.4
Customers are responsible for any changes made to user and organization data stored within the Goodkind software application.	CC8.1
Customers are responsible for communicating relevant security and availability issues and incidents to Goodkind through identified channels.	CC7.2, CC7.3, CC7.4

Complementary Subservice Organization Controls

Goodkind uses subservice organizations in support of its system. Goodkind's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Goodkind to be achieved solely by Goodkind. Therefore, user entity controls must be evaluated in conjunction with Goodkind's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Goodkind periodically reviews the quality of the outsourced operations by various methods including

- Review of subservice organizations' SOC reports.
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Amazon Web Services and Microsoft Azure	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	Amazon Web Services and Microsoft Azure	CC6.4, CC6.5
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	Amazon Web Services and Microsoft Azure	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	Amazon Web Services and Microsoft Azure	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	Amazon Web Services and Microsoft Azure	A1.2
A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	Amazon Web Services and Microsoft Azure	C1.1
A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	Amazon Web Services and Microsoft Azure	C1.2
Encryption methods are used to protect data in transit and at rest.	Amazon Web Services and Microsoft Azure	CC6.1

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Goodkind provided by Goodkind Software Corporation The scope of the testing was restricted to Goodkind, and its boundaries as defined in Section 3. Goodkind Software Corporation conducted the examination testing on 15 November 2023.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Goodkind Software Corporation considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, CertPro utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. CertPro, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selectingsamples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: CONTROL ENVIRONMENT			
CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Entity has established a policy to define behavioral standards and acceptable business conduct and makes it available to all staff members on the company employee portal.	Inspected the behavioral standards which are defined in the Code of Business Conduct Policy. Has been made available to all staff members on the company employee portal.	No exceptions noted.
CC1.1.2	Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	Inspected the company policies & Code of Business Conduct Policy. Has been reviewed and acknowledged by new staff members.	No exceptions noted.
CC1.1.3	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Has been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC1.2.2	Entity's Senior Management reviews and approves the state of the Information Security program annually.	Inspected the internal audit assessment report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC1.2.3	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the Organizational Chart for all employees. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC1.2.4	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC1.2.5	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Vendor Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Entity appoints an owner of Infrastructure operations, who is responsible for all assets in the inventory.	Inspected Infrastructure Operations Person assigned.	No exceptions noted.
CC1.3.2	Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.	Inspected the planning, assessing, implementing and internal control environment.	No exceptions noted.
CC1.3.3	Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	Inspected the Organizational Structure. They maintain authorities, facilitate information flow and establish responsibilities.	No exceptions noted.
CC1.3.4	Entity ensures clarity in job responsibilities for client serving, IT and engineering positions (via OKRs, Job Descriptions etc.) to increase the operational effectiveness of the organization.	Inspected the job descriptions.	No exceptions noted.
CC1.3.5	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	Inspected Compliance Program Manager assigned.	No exceptions noted.
CC1.3.6	Entity appoints a People Operations Officer to develop and drive forward all HR security-related strategies across the company.	Inspected People Operations Officer assigned.	No exceptions noted.
CC1.3.7	Entity's Senior Management reviews and approves the state of the Information Security program annually.	Inspected the Internal Audit Assessment report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Entity ensures that new hires have been duly evaluated for competence in their expected job responsibilities.	Observed the competence evaluation for new hires.	No exceptions noted.
CC1.4.2	Entity ensures that new hires go through a background check as part of their onboarding process.	Observed the onboarding background check for new hires.	No exceptions noted.
CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Entity has established an Information Security Awareness training, and its contents are available for all staff on the company employee portal.	Inspected the Information Security Awareness Information. Contents are available for all staff on the company employee portal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.2	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Has been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.5.3	Entity requires that all staff members complete Information Security Awareness training annually.	Observed the Information Security Awareness Training logs.	No exceptions noted.
CC1.5.4	Entity requires that new staff members complete Information Security Awareness training upon hire.	Observed the Information Security Awareness training records.	No exceptions noted.
CC1.5.5	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their Job responsibilities.	Observed the periodical evaluation of job responsibilities.	No exceptions noted.
CC2.0: COMMUNICATION AND INFORMATION			
CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Inspected the functioning of internal controls. Has been reviewed and evaluated in the system.	No exceptions noted.
CC2.1.2	Entity makes all policies and procedures available to all staff members via the company employee portal.	Inspected the policies and procedures. Has been made available to all staff members via the company employee portal.	No exceptions noted.
CC2.1.3	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the current information about its services on their website.	No exceptions noted.
CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Entity has established a policy to define behavioral standards and acceptable business conduct and makes it available to all staff members on the company employee portal.	Inspected the behavioral standards which are defined in the Code of Business Conduct Policy. Has been made available to all staff members on the company employee portal.	No exceptions noted.
CC2.2.2	Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	Inspected the company policies & Code of Business Conduct Policy. Has been reviewed and acknowledged by new staff members.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.3	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the Information Security Policy.	No exceptions noted.
CC2.2.4	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Has been reviewed and acknowledged by staff members.	No exceptions noted.
CC2.2.5	Entity requires that all staff members complete Information Security Awareness training annually.	Inspected the Information Security Awareness Training logs.	No exceptions noted.
CC2.2.6	Entity requires that new staff members complete Information Security Awareness training upon hire.	Observed the Information Security Awareness training records.	No exceptions noted.
CC2.2.7	Entity makes all policies and procedures available to all staff members via the company employee portal.	Inspected the company policies and procedures. Has been made available to all staff members via the company employee portal.	No exceptions noted.
CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the current information about its services on its website.	No exceptions noted.
CC2.3.2	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the Information Security Policy.	No exceptions noted.
CC3.0: RISK ASSESSMENT			
CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	No exceptions noted.
CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Observed the risk mitigating factors.	No exceptions noted.
CC3.2.3	Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	Inspected the company policies & Code of Business Conduct Policy. Has been reviewed and acknowledged by new staff members.	No exceptions noted.
CC3.2.4	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the Vendor Management Policy. Observed the annual vendor risk assessment exercise.	No exceptions noted.
CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Observed the risk matrix records.	No exceptions noted.
CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	No exceptions noted.
CC3.4.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Observed the risk mitigating factors.	No exceptions noted.
CC3.4.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the Vendor Management Policy. Observed the annual vendor risk assessment exercise.	No exceptions noted.
CC4.0: MONITORING ACTIVITIES			
CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Entity appoints an owner of Infrastructure, who is responsible for all assets in the inventory.	Inspected Infra Operations Person document. Said person is responsible for all assets in the inventory.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.2	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Observed subservice organizations defined in the system. Has been reviewed and evaluated by the entity.	No exceptions noted.
CC4.1.3	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Vendor Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.1.4	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.1.5	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the Organizational Chart for all employees. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.1.6	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.1.7	Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing, and reviewing the internal control environment.	Inspected the planning, assessing, implementing and internal control environment.	No exceptions noted.
CC4.1.8	Entity maintains and periodically reviews the inventory of systems which are critical to security commitments and requirements.	Observed the review and monitoring of the inventory of systems.	No exceptions noted.
CC4.1.9	Entity's Senior Management reviews and approves the state of the Information Security program annually.	Inspected the Internal Audit Assessment report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.1.10	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Sprinto tool that continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the Information Security Policies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Sprinto tool that continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC4.2.3	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.2.4	Entity's Senior Management reviews and approves the state of the Information Security program annually.	Inspected the Internal Audit Assessment report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.0: CONTROL ACTIVITIES			
CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the control environment policies.	No exceptions noted.
CC5.1.2	Entity has documented guidelines on Acceptable Usage of Entity's assets and makes it available for all staff on the company employee portal.	Inspected the Acceptable Usage Policy. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC5.1.3	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Observed the responsibilities and duties across the organization.	No exceptions noted.
CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Sprinto tool that continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC5.2.2	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.3	Entity's Senior Management reviews and approves the state of the Information Security program annually.	Inspected the Internal Audit Assessment report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.4	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the employees Organizational Chart. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.5	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.6	Entity's Infosec officer reviews and approves the list of people with access to production console annually.	Inspected the production console list in the system. Has been reviewed and approved by Information Security officer.	No exceptions noted.
CC5.2.7	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Vendor Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.8	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Observed the periodic reviews and evaluations of subservice organizations in the system.	No exceptions noted.
CC5.2.9	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the control environment policies.	No exceptions noted.
CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Entity makes all policies and procedures available to all staff members via the company employee portal.	Inspected the company policies and procedures. Has been made available to all staff members via the company employee portal.	No exceptions noted.
CC5.3.2	Entity requires that all staff members review and acknowledge company policies annually.	Inspected company policies. Has been reviewed and acknowledged by all staff members.	No exceptions noted.
CC5.3.3	Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	Inspected the company policies & Code of Business Conduct Policy. Has been reviewed and acknowledged by new staff members.	No exceptions noted.
CC5.3.4	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Observed policies in the system relating to the control environment.	No exceptions noted.
CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inspected Password Policy. Has been made available to all staff members via the company employee portal.	No exceptions noted.
CC6.1.2	Entity has developed a policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.3	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.	Inspected the Sprinto tool that continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC6.1.4	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Observed entity's system access. Has been reviewed and approved by Senior Management or Information Security Officer.	No exceptions noted.
CC6.1.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Observed entity's administrative system access. Has been reviewed and approved by Senior Management or Information Security Officer.	No exceptions noted.
CC6.1.6	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Observed entity's access to critical systems.	No exceptions noted.
CC6.1.7	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected entity's access provisioning logs. Has been reviewed protected from public internet access.	No exceptions noted.
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Entity has developed a policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy.	No exceptions noted.
CC6.2.2	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Observed entity's access to critical systems.	No exceptions noted.
CC6.2.3	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	Observed the offboarding process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Observed entity's administrative system access. Has been reviewed and approved by Senior Management or Information Security Officer.	No exceptions noted.
CC6.3.2	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Observed entity's system access. Has been reviewed and approved by Senior Management or Information Security Officer.	No exceptions noted.
CC6.3.3	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	Observed the offboarding process.	No exceptions noted.
CC6.3.4	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Observed entity's access to critical systems.	No exceptions noted.
CC6.3.5	Entity has developed a policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy.	No exceptions noted.
CC6.3.6	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Observed the production databases access.	No exceptions noted.
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the Media Disposal Policy.	No exceptions noted.
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor authentication.	Observed the Multifactor authentication for all critical system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.2	Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	Observed the malware-protection software.	No exceptions noted.
CC6.6.3	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Observed the encryption process for unauthorized access.	No exceptions noted.
CC6.6.4	Entity maintains the inventory of endpoint assets and segregates assets with access to critical data from the others.	Observed the production infrastructure assets records. Has been segregated from staging/development assets.	No exceptions noted.
CC6.6.5	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	Observed the auto-screen-lock process.	No exceptions noted.
CC6.6.6	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Observed the Entity's firewall in the system.	No exceptions noted.
CC6.6.7	Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal.	Inspected the Endpoint Security Policy. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC6.6.8	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected entity's access provisioning logs. Has been reviewed and protected from public internet access.	No exceptions noted.
CC6.6.9	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Observed the encryption process for unauthorized access.	No exceptions noted.
CC6.6.10	Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner.	Observed the version on Operating System. Has been found to be up to date.	No exceptions noted.
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Observed the encryption process.	No exceptions noted.
CC6.7.2	All production database[s] that store customer data are encrypted at rest.	Observed the encryption process.	No exceptions noted.
CC6.7.3	User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.	Observed the https (TLS algorithm) and industry standard encryption.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.4	Entity maintains an inventory of infrastructure assets and segregates production assets from its staging/development assets.	Observed the production infrastructure assets records. Has been segregated from staging/development assets.	No exceptions noted.
CC6.7.5	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Observed production and non-production environments maintain the same level of protection for customer data.	No exceptions noted.
CC6.7.6	Entity has a documented policy to manage encryption and makes it available for all staff on the company employee portal.	Inspected the Encryption Policy. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC6.7.7	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Observed the encryption process for unauthorized access.	No exceptions noted.
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner.	Observed the version on Operating System. Has been found to be up to date.	No exceptions noted.
CC6.8.2	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Observed the Entity's cloud provider's firewall.	No exceptions noted.
CC7.0: SYSTEM OPERATIONS			
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed the vulnerability scans records.	No exceptions noted.
CC7.1.2	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected the Operations Security Policy and Procedure.	No exceptions noted.
CC7.1.3	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inspected the internal audit logs. Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program.	No exceptions noted.
CC7.1.4	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed the Production assets and their alerting system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.5	Entity has a documented policy to establish guidelines on managing technical vulnerabilities and makes it available for all staff on the company employee portal.	Inspected Operations Security Procedure and Policy. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC7.1.6	Entity's infrastructure is configured to review and analyse audit events for anomalous or suspicious activity and threats.	Inspected the internal audit logs.	No exceptions noted.
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed the vulnerability scans records.	No exceptions noted.
CC7.2.2	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected Operations Security Policy and Procedure.	No exceptions noted.
CC7.2.3	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inspected the internal audit logs. Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program.	No exceptions noted.
CC7.2.4	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed the Production assets and their alerting system.	No exceptions noted.
CC7.2.5	Entity has a documented policy to establish guidelines on managing technical vulnerabilities and makes it available for all staff on the company employee portal.	Inspected Operations Security Policy and Procedure. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC7.2.6	Entity's infrastructure is configured to review and analyze audit events for anomalous or suspicious activity and threats.	Inspected the internal audit logs.	No exceptions noted.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Sprinto tool that continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.3.2	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the record of information security incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.3	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed the vulnerability scans records.	No exceptions noted.
CC7.3.4	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected Operations Security Policy and Procedure.	No exceptions noted.
CC7.3.5	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inspected the internal audit logs. Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program.	No exceptions noted.
CC7.3.6	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed the Production assets and their alerting system.	No exceptions noted.
CC7.3.7	Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner.	Observed the version on Operating System. Has been found to be up to date.	No exceptions noted.
CC7.3.8	Entity has a documented policy to establish guidelines on managing technical vulnerabilities and makes it available for all staff on the company employee portal.	Inspected Operations Security Policy and Procedure. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC7.3.9	Entity's infrastructure is configured to review and analyze audit events for anomalous or suspicious activity and threats.	Inspected the internal audit logs.	No exceptions noted.
CC7.3.10	Entity identifies vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third-party service provider.	Observed the VAPT Report.	No exceptions noted.
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the Information Security program to the Information Security Officer and other stakeholders.	Inspected the Sprinto tool that continuously monitors, tracks, and reports the health of the Information Security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.4.2	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.	Inspected the Incident Management Policy. Has been made available to all staff members via the company employee portal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the record of information security incidents.	No exceptions noted.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Entity has documented guidelines to manage Business Continuity that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan.	No exceptions noted.
CC7.5.2	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Disaster Recovery Policy.	No exceptions noted.
CC7.5.3	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Observed the Data Backup Policy. Has been made available for all staff on the company employee portal.	No exceptions noted.
CC8.0: CHANGE MANAGEMENT			
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Entity has a documented policy and procedure to manage changes to its operating environment that includes critical information. Such documentation is available to all relevant Staff Members via the company employee portal.	Observed the Change Management Policy. Has been made available to all Staff Members via the company employee portal.	No exceptions noted.
CC8.1.2	Entity uses a change management system to track, review and log all changes to the application code.	Observed the change management system.	No exceptions noted.
CC8.1.3	Entity maintains an inventory of infrastructure assets and segregates production assets from its staging/development assets.	Observed the production infrastructure assets records. Has been segregated from staging/development assets.	No exceptions noted.
CC8.1.4	Entity ensures that all planned changes undergo a review and approval process as per the guidelines documented in the policy and procedure defined to manage changes.	Observed the change management system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.0: RISK MITIGATION			
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Assessment and Management Policy.	No exceptions noted.
CC9.1.2	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the Risk Assessment and Management Policy. Observed the annual risk assessment exercise.	No exceptions noted.
CC9.1.3	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Observed the risk score and mitigating factors.	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Assessment and Management Policy.	No exceptions noted.
CC9.2.2	Entity has a documented policy to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inspected the Vendor Management Policy.	No exceptions noted.
CC9.2.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the Vendor Management Policy. Observed the annual vendor risk assessment exercise.	No exceptions noted.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY			
A.1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed the entity's production assets and their alerting system.	No exceptions noted.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Observed the Data Backup Policy. Has been made available for all staff on the company employee portal.	No exceptions noted.
A1.2.2	Entity backs-up their production databases periodically.	Observed the periodical production databases backs-up.	No exceptions noted.
A1.2.3	Entity's data backups are restored and tested annually.	Observed the annual restoration and testing of data backups.	No exceptions noted.
A1.2.4	Entity has documented guidelines to manage Business Continuity that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan.	No exceptions noted.
A1.2.5	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Disaster Recovery Policy.	No exceptions noted.
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Entity has documented guidelines to manage Business Continuity that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan.	No exceptions noted.
A1.3.2	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Disaster Recovery Policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.3	Entity ensures that the Disaster Recovery Plan is tested periodically, and learnings documented.	Observed test of the Disaster Recovery Plan.	No exceptions noted.
A1.3.4	Entity's data backups are restored and tested annually.	Observed the annual restoration and testing of data backups.	No exceptions noted.

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Entity has an Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inspected Information Security Policy.	No exceptions noted.
C1.1.2	Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	Inspected the company policies & Code of Business Conduct Policy. Has been reviewed and acknowledged by new staff members.	No exceptions noted.
C1.1.3	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Has been acknowledged by all staff members annually.	No exceptions noted.
C1.1.4	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	Inspected the Data Classification Policy. Has been made available for all staff on the company intranet.	No exceptions noted.
C1.1.5	All production database[s] that store customer data are encrypted at rest.	Observed the encryption process in the system.	No exceptions noted.
C1.1.6	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Observed the encryption process in the system.	No exceptions noted.
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the Media disposal Policy.	No exceptions noted.
C1.2.2	Entity has a documented policy that establishes guidelines for Data Retention and makes it available for all staff on the company employee portal.	Inspected the Data Retention Policy. Has been acknowledged by all new staff members.	No exceptions noted.

goodkind

Goodkind Software Corporation
670 Bloor Street West, Unit 201, M6G1L2
Toronto, Ontario, Canada
goodkind.com

ORDER FORM

Valid through March 31, 2024

Customer Information:

Customer Name:	North Florida College
Customer Address:	325 Turner Davis Dr, Madison, FL 32340, United States
Primary Contact Name:	Allison Finley
Primary Contact Email:	finleya@nfc.edu
Primary Contact Phone:	
Invoicing Email Address:	
EIN Number:	

Order Details:

Subscription Term	Billing Term	Currency	Subscription Service Start Date
36 months	Net 30 days	USD	March 15, 2024

Section 1: Subscription Service

Item	Description	Unit Price	Quantity	Discount	Annual Fee
Video messaging module	Unlimited access, support, onboarding training for 4 teams (under 500 FTE total)	$10,000	4	$10,000	$30,000
SMS module	Access, support, training, 5 free phone numbers, 25,000 free SMS credits	NA	NA	$1,000	See 1.2
CRM Integration	FTP based Banner Integration	$3,500	1	-	$3,500
Special conditions 1. 25% discount on base video messaging fees (one team free) 2. 5 free phone numbers and 25,000 free SMS credits ($1,000 value) 3. 5% increase year over year				Subtotal	$33,500
				Year 1 total	**$33,500**
				Year 2 total	**$35,675**
				Year 3 total	**$37,958**

Section 1.2: Goodkind Conversations, SMS Credits

Item	Price
25,000 SMS credits (message sent or received)	$500
Phone number	$100 per number

Conditions: Applies to sms or MMS sending within the US or Canada. A credit is a message sent or received. An MMS takes two credits, an SMS one credit. Credits roll over month to month. Credits can be purchased in batches of $500 at any time.

Section 2: Additional Services

Item	Description	Unit Price	Quantity	Discount	Fee
Send via custom domain	Send video messages via branded NFC website	$1,800	1	$1,800	Free
Phone numbers	14 unique phone numbers	$100	14	$500	$900
Single-Sign On Support	Support for NFC Microsoft based Single-Sign On	$3,500	1	-	$3,500
Special conditions: 1. Send via custom domain discounted at 100% 2. 5 free phone numbers included in package				Subtotal	$4,400
				Total One Time Fees	**$4,400**

Section 3: Billing

Year	Service Type	Term Start	Term End	Fees	Billing Cycle	Payment Terms
1	Subscription	March 15, 2024	March 14, 2025	$33,500	Annual	Net 30
All	Additional Services	March 15, 2024	March 14, 2027	$4,400	One-time	Net 30
2	Subscription	March 15, 2025	March 14, 2026	$35,675	Annual	Net 30
3	Subscription	March 15, 2026	March 14, 2027	$37,958	Annual	Net 30

Section 4: Terms & Conditions

The Subscription Term Commences on the Subscription Service Start Date and incorporates by reference the Company's Master Subscription Agreement found at https://www.goodkind.com/terms (the "**Agreement**"), and supersedes and replaces all previous agreements, memoranda, or correspondence, whether written or oral among the parties with respect to the subject matter of this Agreement. Prices shown do not include taxes.

North Florida College

Signature: ______________________
Name: ______________________
Title: ______________________

Goodkind

Signature: ______________________
Name: Justin Rotman
Title: Co-founder, CEO