HIDALGO COUNTY HEAD START PROGRAM
P.O. BOX 0117
EDINBURG, TEXAS 78540
956-383-0706

DATE: March 13, 2025

TO: Hidalgo County Head Start Program Policy Council

FROM: Elma P. Carrera, Assistant Program Director for Fiscal Operations EPCarrera

Thru: Irma Peña, Executive Director

RE: MIP Cloud and Microix Migration

==========

Administration is requesting approval to integrate and migrate to the MIP Cloud, a secure and reliable online hosted services support operation. What does this mean and what are the advantages of migrating our Program data to the Cloud?

Listed below are some of the benefits and safeguards our Program would secure:

- MIP products hosted in the Cloud guarantee secure system availability 24/7 from anywhere with an internet connection
- Features a data center with industry standard security which will reduce risk of fraud or loss of data
- Uses software encryption technology to protect and authenticate data transactions
- All users will be required to have Multi-Factor Authentication (MFA) for added security measures
- Collects and registers user login information for audit purposes
- Features data center Uninterruptible Power Supply (UPS) backup power to ensure no data is lost
- Automatic backups are performed which will allow users to restore data to a specific time frame
- All updates are applied as soon as notification is received

There will be a one-time cost of approximately $54,378 which also includes the addition of an electronic purchase order module, a supplies inventory software module to include scanning devices, and onsite training sessions for all users.

If this meets your approval, migration to the Cloud will take approximately 4 hours down time and will be performed on a non-payroll week to ensure all data is successfully migrated to the Cloud.

As always, we thank you for your guidance and support for our Head Start Program.

MIP Cloud: Fixed Assets - Subscription - 1	$1,428.00
MIP Cloud: GASB Reporting - Subscription - 1	$588.00
MIP Cloud: Additional Hosting Storage - Subscription - 1	$240.00
Microix Cloud: Hosting - Subscription - 1	$300.00
MIP Cloud: Encumbrances - Subscription - 1	$468.00
MIP Cloud: Human Resource Management Additional User(s) - Subscription - 10	$1,800.00
MIP Cloud Fundamentals: Human Resource Management - Subscription - Active Employees: 1,000	$6,335.00
MIP Cloud Fundamentals: Payroll - Subscription - 1	$1,790.00
MIP Cloud Fundamentals: Direct Deposit - Subscription - 1	$0.00
Microix On-Premise: Requisitions - License - 1	$2,695.00
Microix On-Premise: Inventory - License - 1	$3,500.00
Microix On-Premise: Vendor Punchout - License - 1	$1,000.00
Software Subtotal	**$34,234.00**
Discount	**$2,649.90**
Software Total	**$31,584.10**
Annual M&S Total (Microix only)	**$1,798.75**

ADDITIONAL PRODUCTS

The following table provides a description of the hardware, shipping/handling and corresponding fees.

Product Name	Qty	One-time Fee
Microix: Inventory Barcode Scanner - Hardware	2	$1,798.00
Microix: Shipping and Handling Fee	3	$75.00
Microix: DT50Q Barcode Scanner Backup Battery - Hardware	1	$60.00
Additional Products Total		**$1,933.00**

PROFESSIONAL SERVICES

During the Term, Provider may perform certain implementation, consulting and or training services (the "Professional Services") as specified in a written statement of work ("SOW") which shall be mutually executed between the parties subject to the terms of this Agreement. Any Customer request for changes to the Professional Services ordered in a previously-executed SOW may result in additional fees to be billed to Customer, and will require a written change order agreed to and signed by both parties.

This Order Form includes the following Services and the price to be charged for each during the Term.

Services	Qty	Charge Type	(Estimated) One-time Fees
MIP Cloud User Setup	1.00	T&M	$62.50
MIP Cloud HR/EWS Provisioning	1.00	T&M	$250.00
MIP Cloud Microix Provisioning - Existing with DB attachments	2.00	T&M	$500.00
MIP Cloud Microix User Setup	8.00	T&M	$500.00

MIP Cloud Organization Setup	1.00	T&M	$250.00
MIP Cloud Level V Database Setup	8.00	T&M	$2,000.00
MIP Cloud Project Management	6.00	T&M	$1,500.00
MIP Cloud Modern Overview	2.00	T&M	$500.00
Microix Training	50.00	Fixed Price	$12,500.00
MIP Cloud Linked Attachments	4.00	T&M	$1,000.00
Professional Services Total			**$19,062.50**

TOTAL
$54,378.35

ESTIMATED TAX

TOTAL WITH ESTIMATED TAX
$54,378.35

Customer Notes:
The training hours were reduced to 50hrs and include:
- Up to 18hrs Requisition module implementation and training.
- Up to 3hrs Credit Card Statement setup training.
- Up to 4hrs Vendor Punchout setup training.
- Up to 3hrs Shopping Cart setup training.
- Up to 18hrs Microix Inventory module implementation and training.
- Up to 4hrs Barcode Scanner setup and training setup training.

Note: Customer will need to purchase additional hours if needed.

Please confirm your tax-exempt status by checking one of the following boxes:

We are tax-exempt: We are not tax-exempt:

The total contract value includes an estimated tax value. If you have not already submitted your business's tax exempt certificate, please email it to salestax@momentivesoftware.com. You will be invoiced and responsible for tax payments until your certificate is received and approved by our tax department.

Term

The Term of this Order Form shall continue for 12 months and automatically renew for a twelve (12) month term (each a "Renewal Term") unless either party provides the other party with written notice of intent not to renew no later than one hundred twenty (120) days prior to the expiration of the current Term.

[Remainder of this page intentionally left blank; signature pages follow next page]

IN WITNESS WHEREOF, the parties hereto, each by a duly authorized officer, have entered into this Agreement as of the Effective Date.

CUSTOMER: Hidalgo County Headstart	**PROVIDER: Momentive Software, Inc.**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Momentive SOFTWARE

MOMENTIVE SOFTWARE, INC.
NEW ORDER FORM

This order form cover sheet and any product addenda, schedules, or attachments hereto (collectively, the "Order Form") is entered into on the date of last signature below ("Effective Date") by and between Hidalgo County Headstart with offices located at PO Box 117, Edinburg, Texas, 78540-0117, United States (the "Customer") and Momentive Software, Inc. and its brand affiliates ("Provider") for the provision of the Products and Services listed below. Customer and Provider agree to be bound by Provider's terms and conditions (the "Terms and Conditions"), a copy of which is available on Provider's website at Terms and Conditions and incorporated herein by reference, and supersedes all prior, conflicting agreements or representations, written or oral between the parties for the Products and Services listed below. Capitalized terms in this Order Form will have the meanings given in the Terms and Conditions. The Order Form and the Terms and Conditions shall be known, collectively, as the "Agreement." In the event of conflict between the Order Form and the Terms and Conditions, the Order Form shall control.

QUOTE DETAILS	PREPARED BY
Quote Number: Q-70675 Quote Date: 03/12/2025 Quote Expires on: 04/11/2025	MOMENTIVE SOFTWARE, INC. 9620 Executive Center Drive N. #200 St. Petersburg, Florida 33702
Term Commencement Date: 03/31/2025 Term Completion Date: 03/30/2026 Term Duration: 12 Months Payment Terms: Net 30	Representative: Bianca Dubay

BILLING INFORMATION	PRIMARY CONTACT
Hidalgo County Headstart PO Box 117 Edinburg,Texas 78540-0117 United States	Elma Carrera 1 (956) 383-0706 elma.carrera@hchsp.org

ORDER SUMMARY:

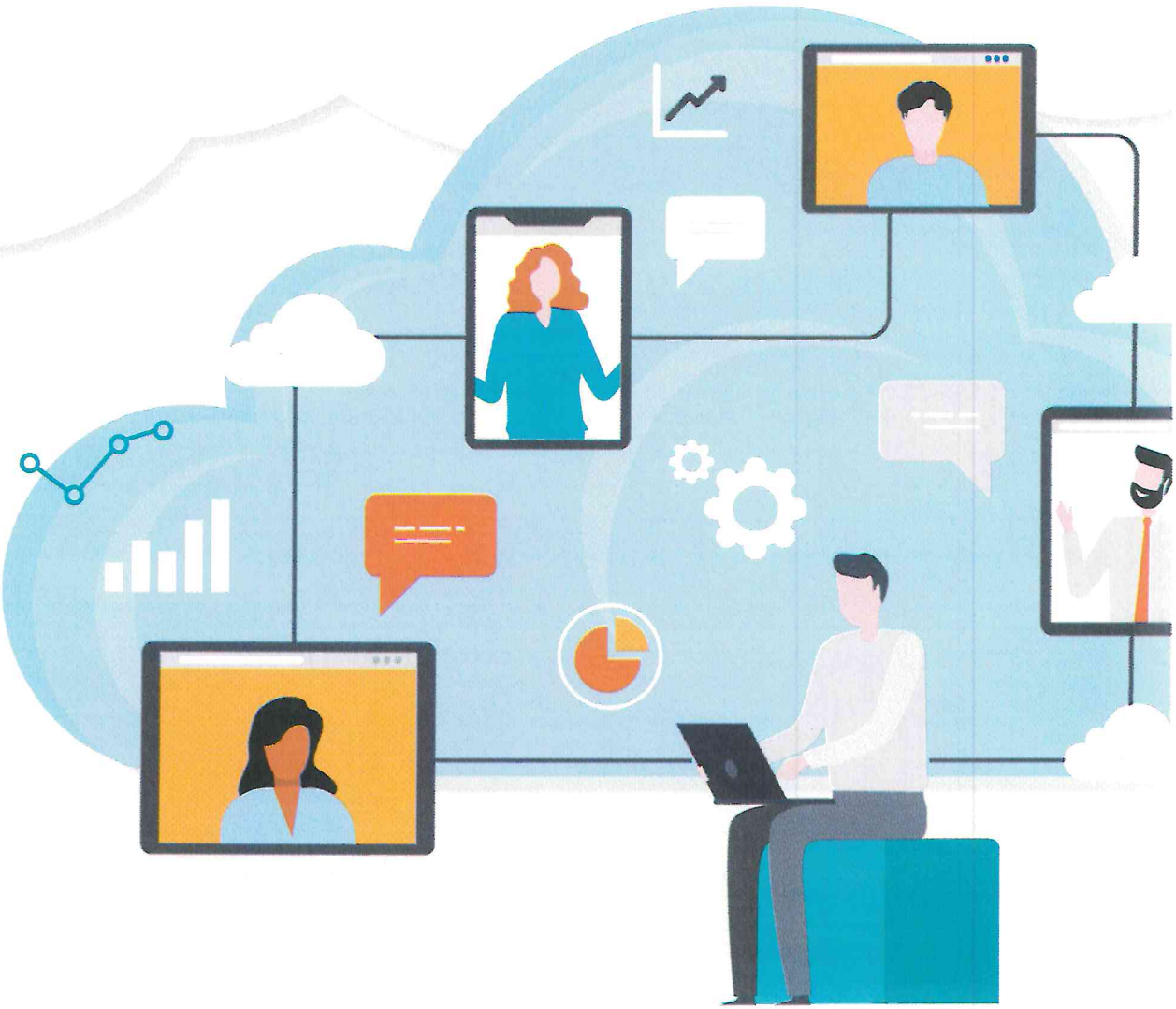
LICENSED SOFTWARE and SAAS	
This Order Form includes the following Products and the annual price to be charged for each during the Term.	
Product Name	**Annual Price**
Nonprofit Suite - Fundamentals Bundle - 4	$7,490.00
MIP Cloud: Additional User(s) - Subscription - 11	$6,600.00

mip FUND ACCOUNTING by communitybrands

Everything you need to know about MIP Cloud.

We know growth, scalability, and availability are important to you. With MIP Cloud, you have dependable, 24/7 access through secure and reliable online hosted services.

Access your data online anytime, from any location, without the cost and burden of managing hardware, software, and on-site support operations. On the following pages is all the information you need in detail to help you understand and integrate the power of MIP Cloud!



Top Rated 2021

System availability—24/7, any location access

- MIP guarantees system availability equal or exceeding 99.9% during each month
- MIP products hosted in the Cloud are available 24/7, provided there is an internet connection
- It is important that users stay up to date on MIP system requirements and to ensure a stable internet connection for all users. This will provide users with a quality experience

Data center security—reduce risk of fraud or loss of data

- MIP's data center locations are not publicly disclosed to maintain the highest physical security
- Access to any of our data centers is tightly controlled, monitored in person and by closed-circuit video surveillance inside and outside of the facility, 24x7x365
- Access to various areas of the Data Center is strictly controlled on a role-specific basis
- Within each data center's security perimeter, sensitive server equipment is housed in a secure zone which is subject to further and additional security controls
- MIP software uses 2048-bit RSA, the standard on SSL encryption technology to protect and authenticate data transactions; program administrators can set user credentials with specific access to data, along with recording login information for audit purposes

Data center backup power supplies—to ensure no data loss

- To ensure a 99.9% availability each month, MIP's data centers are equipped with the latest technology
- Power delivery capability:
  - 135 Watts per square foot
  - UPS – 9x2000 KVA systems, 328 panels for 30 min battery life
- Backup power system:
  - 2 sets of 4x1500 KW Generators
  - 2 sets of 4x2000 KW Generators for 48-hour capacity
  - Generators auto start in the event of power failure
- HVAC system:
  - 1,504,250 CFM for 7500 tons of cooling capacity
- Networking partners:
  - Multiple Tier-1 providers
  - 10-Gigabit Ethernet per carrier

communitybrands mip FUND ACCOUNTING

Data infrastructure

Our hardware partner guarantees one-hour replacement for any piece of hardware that fails. Service redundancy means there is always a backup available on-site. Geographic redundancy is not offered as part of our solution. If our data center is destroyed the data is secure, however it will take a reasonable amount of time to bring it back online.

- Data center hardware configuration:
  - » Clustered Windows-based SQL servers in Active/Active mode
  - » Hypervisor servers running VMWare in High Availability (HA) mode
  - » Cisco firewalls operating in HA mode
  - » F5 BigIP load balancers operating in HA mode
- Software configuration:
  - » Windows Active Directory
  - » Windows Remote Desktop Servers
  - » Windows Web/API Servers
- Onsite infrastructure:
  - » 24/7 monitoring with regularly scheduled maintenance performed by onsite engineers
  - » Hardware spare parts maintained onsite

Access to backup and backup planning

- Full backups weekly
- Daily differential backups
- Backups are logged hourly
- 28 days of backups maintained online, with additional backup information maintained offsite
- Full backups of the operating systems are done on a weekly basis and maintained by onsite engineers
- MIP customers may request one free back up of their databases once a month through the MIP Support team

Requesting SSAE18 audit information

A Statement on Standards for Attestation Engagements – Number 18 (SSAE18) Report is a Generally Accepted Auditing Standard (GAAS) produced and published by the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board. Its focus is reporting on the quality (accuracy, completeness, fairness) of financial reporting with particular attention on internal controls. This report is obtained via a request to MIP Support. A Non-Disclosure Agreement must first be signed by the requesting party prior to obtaining the report.

communitybrands

mip FUND ACCOUNTING

MIP platform system requirements

- Supported Operating Systems:
  - » Windows 10 (32-bit, 64-bit) Standard edition or greater
  - » Windows 8.1 (32-bit, 64-bit) Standard edition or greater
  - » Apple macOS systems are not supported by MIP Cloud but can be accessed through a Microsoft Remote Desktop application, which is available as a free download from Microsoft. MIP does not currently offer any customer support for macOS systems.
- Connectivity:
  - » Internet accessible with the latest browser service pack
- Supported Browsers:
  - » Google Chrome (recommended)
  - » Microsoft Edge
- For the latest specifications, visit www.mip.com/system-requirements/

Additional Supported Workstation Operating Systems:

MIP is optimized to run on the recommended systems specified above. For customers with legacy equipment and software, our MIP Support team will troubleshoot and generally try to help to the best of our ability. Should an MIP software defect be discovered on these systems, Community Brands will attempt to resolve the problem in a future release or will suggest a viable workaround. Community Brands will give prior notice before ending support of these systems.

Accessing your product and updates in MIP Cloud

The services supplied by MIP Cloud are updated as the product teams release new or revised products and features.

- Normal product updates are usually deployed on a Friday night and generally completed by Saturday
- Resources during the update are managed expertly to ensure the customer always has access to their application
- Any critical updates are applied as soon as possible, reducing downtime
- Notification for any update activity is issued by MIP Support via the Customer Community as well as via email (at a minimum) 48 hours before the deployment date and time

communitybrands

mip FUND ACCOUNTING

Security Statement

Introduction

This security statement provides details of Community Brands information security practices. In the event that any regulatory, state or Federal laws, now or hereafter in effect, impose a higher standard of confidentiality or security with respect to Data or systems, such standard shall prevail over the provisions of this document. Community Brands has a dedicated Risk & Compliance team, which focuses on application, network, system security, compliance, education, and incident response.

This security page applies to Community Brands and was created to provide Community Brands customers with the confidence needed to trust our company as the leading provider of cloud-based software.

Community Brands is not responsible for the security practices of non-Community Brands entities. If you are a customer of one of our customers, please refer to the security practices specific to that organization.

1. **How Does Community Brands Protect its Customer Data?** Community Brands regards security as a broad, critical, and multi-faceted requirement, achieving full platform security through a combination of securing physical access to servers, network perimeter defenses, security-conscious operational procedures and policies within the corporate facilities, and component redundancy with backup process and procedures. To learn more, please review Community Brands' Privacy Policy found here: https://www.communitybrands.com/privacy-policy/.

2. **Use of Confidential Information and Personal Information.** Community Brands will only access, use, maintain, collect, modify, merge, share or disclose customer data as is necessary for Community Brands to perform its obligations of services agreed and for no other purpose. As between Community Brands and customer, all customer data is, will be deemed to be, and will

remain the exclusive property of customer. Except as set forth under contract agreement or as customer otherwise directs in writing, Community Brands may not modify customer data provided by customer or allow such customer data to be modified without authorization. Community Brands' subcontractors or subprocessors have agreed in writing to maintain terms that are not less protective than the provisions of this Security Statement.

3. **Security.** Consistent with applicable data privacy and security laws, Community Brands uses practices and safeguards designed to reasonably protect customer data, including from any unauthorized collection, access, use, storage, disposal, disclosure, or unavailability of customer data by its employees, agents or subcontractors. To fulfill obligations under this section, Community Brands maintains, at a minimum, physical, technical, administrative, and organizational safeguards that provide for and reasonably ensure: (a) protection of business facilities, paper files, servers, computing equipment, including without limitation mobile devices and other equipment with information storage capability, and backup systems containing customer data; (b) network, application (including databases) and platform security; (c) secure transmission and storage of customer data, including encryption of sensitive data; (d) authentication and access control mechanisms over customer data, media, applications, operating systems and equipment; (e) storage limitations such that customer data resides only on servers in data centers that comply with industry standard data center security controls; and (f) restrictions to ensure that customer data files are not placed on any notebook hard drive or removable media, such as compact disc or flash drives, unless encrypted. Community Brands' may at any time apply methods and safeguards that are more secure.

4. **Information Security Policy.** Community Brands incorporates a risk assessment-based approach to managing the Information Security Policy which considers Community Brands' unique mission, customer needs, business requirements, and corporate culture. The Information Security Policy is reviewed at a minimum annually to stay current with industry standards and reflect any changes in Community Brands business environments or objectives. The Information Security Policy is considered internal confidential.

5. **Risk Assessments.** Community Brands maintains a cross functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect the Community Brands' ability to meet its contractual obligations. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through policies.

6. **Incident Response.** Documented incident response and support procedures are in place to guide operations personnel in the monitoring, documenting, escalating, and resolving of problems

affecting managed hosting and network services. These procedures include procedures regarding severity level definitions, escalation procedures, and ticket handling procedures.

7. **Physical and Environmental Security.**

   Community Brands primary office locations physical security: facilities are secured using restricted access policies and surveillance technologies.

   Cloud, Colocation, and Data Center Environmental Security: physical and environmental security is managed with restrictive access controls and surveillance technologies.

8. **Data Storage.** To provide optimal hosting options to customers, Community Brands utilizes world class Data Centers, Colocation Services, and Cloud hosting environments.

9. **Access Limitations.** Community Brands will restrict access to customer data only to those Community Brands employees who have a need to know or otherwise access the customer data to enable Community Brands to perform its obligations, provided those employees are bound in writing by obligations of confidentiality sufficient to protect the customer data.

10. **Cyber Security Insurance.** Community Brands carries cyber liability insurance. To request a copy of the policy, please contact your Account Manager.

11. **Third Party Management.** Community Brands utilizes third-party services to support our products and services. We evaluate each third party for inherent information security risk. Third party relationships concerning industry and/or regulatory requirements are reviewed no less than annually. Each third party must enter into agreements with Community Brands that include a non-disclosure agreement and data processing terms and conditions.

12. **Security Awareness Training.** Community Brands provides annual security awareness training to all its employees. Every Community Brands employee is required to participate in and stay up to date with this training.

13. **Secure Software Development Training.** Community Brands' Developers establish web applications based on industry best practices for security, complete annual secure development training, and are required to be familiar with the Open Web Application Security Project (OWASP) guidelines.

14. **Change Management.** Documented maintenance and change management policies and procedures are in place to guide personnel in change management activities affecting existing customer infrastructure. The policies apply to the deployment, modification, and removal of configuration items in the delivery of the Community Brands services.

15. **Audit Compliance**. Community Brands completes various internal and external security audits that review Community Brands' adherence to regulatory guidelines. Depending upon the Community Brands product in question, external audits are specific to the environment or application. For products that process merchant transactions, Community Brands performs PCI-related audits (PCI- DSS and/or PA-DSS/SSF-SSA, etc.). Community Brands also conducts multi-level vulnerability testing using industry standard tools. Ad-hoc vulnerability scanning of environments and individual deployments are performed by the Risk and Compliance team as necessary. Any threats are prioritized and remediated in a timely manner. Annual penetration testing of network environments and products are completed as an aspect of compliance operations. To request applicable audit report(s), please contact your Account Manager. A Non-disclosure Agreement (NDA) may be required.

16. **Security Breach.** In the event that Community Brands becomes aware of a confirmed "Security Breach" (as defined below) of customer data or receives a complaint from a third party alleging that a Security Breach has occurred, Community Brands will notify affected customer of the actual breach via email as soon as practical, no later than 72 hours after Community Brands identifies, is notified of, or otherwise becomes aware of an actual breach. "Security Breach" means unauthorized access, acquisition, use or release of customer data where maintained by Community Brands.

    In the event of a security breach, Community Brands shall take prompt steps to remedy the Security Breach and shall notify affected customer without undue delay by email to customer. Such notice shall include a full description of the Security Breach, to the extent available, as well as the name and contact information for a primary security contact within Community Brands. Community Brands agrees to cooperate with customer in customer's handling of the matter, including without limitation any investigation, reporting or other obligations required by applicable law or regulation, or as otherwise required by customer, and will work with customer to otherwise respond to and mitigate any damages caused by the Security Breach. Community Brands shall not notify any third party, other than Community Brands' agents who are subject to the obligations of confidentiality to Community Brands, of the breach without customer's prior written authorization. Both parties shall work in good faith at all times to respond to any occurrence of

unauthorized access and to share information within their control that is needed in relation to the remediation or correction of any unauthorized access.

17. **Global Data Protection Regulations.** In relation to the processing of personal data, Community Brands will comply with Global Data Protection Laws. Community Brands is dedicated to working closely with partners and customers to ensure Community Brands meets the obligations of a data processor. To learn more about Cross Boarder Transfers of Data, Community Brands Data Processing Agreement (DPA), or view the full list of Community Brands subprocessors, please visit the Community Brands Privacy Policy found here: https://www.communitybrands.com/privacy-policy/.

18. **Return of Confidential Information.** Unless otherwise agreed to in writing between the parties, Community Brands will return or at customer's election in a secure manner, destroy (or anonymize) and certify in writing, all customer data within a reasonable timeframe, but no later than ninety (90) days upon the termination or expiration of the agreement for any reason.

19. **Data Subject Request.** If Community Brands receives a data subject request in the capacity as the data controller, Community Brands will respond to it. If Community Brands receives a data subject request from a customer's customer (i.e. a user of the services, to whom a customer has provided a user login), Community Brands is the data processor, and Community Brands will, to the extent that applicable legislation does not prohibit Community Brands from doing so, promptly inform the customer's customer to contact the customer (i.e. the data controller) directly about any request relating to his/her personal data. Community Brands will not further respond to a data subject request without the customer's prior consent.

20. **Anti-Corruption.** Community Brands follows industry standards to achieve zero-tolerance against bribery and corruption and in doing so ensures that appropriate anti-corruption and bribery procedures are in place in accordance with relevant laws and regulations. To learn more, please visit the Community Brands Code of Ethics and Business Conduct found here: https://secure.ethicspoint.com/domain/media/en/gui/80438/code.pdf

21. **Contact Us.** For more information regarding this Security Statement, please contact your Account Manager.