ORDINANCE C-09-26

AN ORDINANCE TO AUTHORIZE THE CITY ADMINISTRATOR TO ENTER INTO AN AGREEMENT WITH GOVWELL TECHNOLOGIES INC.

WHEREAS, GovWell provides software building permits, inspections, contractor registration, and code enforcement; and

WHEREAS, the City desires to contract with GovWell for this software; and

WHEREAS, because this agreement exceeds twelve months, it must be approved by Ordinance.

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF GROVE CITY, STATE OF OHIO, THAT:

SECTION 1. The City Administrator is hereby authorized to enter into an agreement with GovWell Technologies Inc. as attached hereto as Exhibit A.

SECTION 2. This Ordinance shall take effect at the earliest opportunity allowed by law.

Ted A. Berry, President of Council

Passed: 03-02-2026
Effective: 04-02-2026

Richard L. Stage, Mayor

Attest:

Tami K. Kelly, MMC, Clerk of Council

I Certify that this ordinance is correct as to form.

Stephen J. Smith, Director of Law

C-09-26
Exhibit "A"

GovWell Order Form

This Order Form, dated as of the Effective Date, is entered into by and between GovWell Technologies Inc. ("**GovWell**") and the customer identified below ("**Customer**"), and is subject to the Terms of Service (as defined below), which are incorporated by reference herein.

Customer: Grove City, OH	**Effective Date:**
Customer Contact: Todd Hurley	**Contact Email:** thurley@grovecityohio.gov
Contact Phone: 614-277-1725	**Billing Contact:**
Billing Email:	**Billing Phone:**

1. SOFTWARE MODULES AND SERVICES.

The table below outlines the GovWell software modules and services included in Customer's purchase:

Software Module	Description	Annual Subscription Fee	Deployment Services Fees	Data Migration Services	Data Migration Fees
Building Permits & Inspections	Manage building permits, inspections, and plan review. Includes online portal for improving access and transparency to the public.	$30,000	$15,000	Data + Files	$5,000
Contractor Registration	Manage contractor registration and recurring annual renewals.	INCLUDED	-	Data + Files	-
Planning & Zoning	Online planning & zoning applications, workflow management, meetings management, and plan review.	$15,000	$6,000	Data + Files	$2,500
Code Enforcement	Online citizen complaints + code enforcement case management.	$15,000	$6,000	Data + Files	$3,000
TOTALS		**$60,000**	**$27,000**		**$10,500**

2. SCOPE OF WORK.

By signing this Order Form, the Customer agrees to the Scope of Work ("SOW") attached as Exhibit A. The SOW outlines the specific services GovWell will provide, as well as the responsibilities of the Customer with respect to Deployment Services, Data Migration Services, Continuous Deployment Services, and Product Support. The Customer acknowledges that GovWell's obligations are limited to the hours and scope defined in the table below. Any services requested beyond these limits may incur additional fees, as described in the SOW.

Item	Quantity / Scope
Deployment Services	60 hours
Data Migration Services	64 hours
Staff Training	Nine (9) 60-minute sessions conducted via Zoom
Continuous Deployment Services	20 hours / year
Product Support	Included for free.

3. INITIAL TERM

Three (3) years, beginning on the Effective Date.

4. SUMMARY OF FEES AND TERMS

Item	Description
Deployment & Data Migration Services Fees (one-time)	$37,500
Annual Subscription Fees	$60,000
Total Year 1 Cost	$97,500
Annual Uplift	5% (not applicable during initial term)
Initial Term Invoice Schedule	Annual, invoiced on signing. Invoice schedule: • $97,500, invoiced on Effective Date • $60,000, invoiced on anniversary of Effective Date 2027 • $60,000, invoiced on anniversary of Effective Date 2028
Renewal Procedure	Automatic 1 year renewal term, unless 30 days notice provided prior to renewal date

5. TERMS OF SERVICE.

The parties expressly acknowledge and agree that this Order Form, any appendices attached, and any amendments hereto signed by the parties, is subject to and conditioned upon Customer's agreement to the Terms of Service located at http://www.govwell.com/terms (as amended from time to time, the "**Terms of Service**"). By signing below, Customer expressly acknowledges and agrees that it has reviewed the Terms of Service and agrees to be bound thereby. In the event of any inconsistency or conflict between the terms of this Order Form and the Terms of Service, the terms of this Order Form shall take precedence and govern solely with respect to the specific services, fees, and terms outlined herein, unless otherwise stated in the Terms of Service. All other provisions of the Terms of Service shall remain in full force and effect. Customer further acknowledges and agrees that by signing below, the person signing this Order Form has the authority to execute this Order Form on behalf of Customer. This Order Form may not be amended or modified, except in a writing signed by both Customer and GovWell.

AGREED AND ACCEPTED on behalf of the parties by their duly authorized representatives as of the Order Form Effective Date.

CUSTOMER:	**GOVWELL TECHNOLOGIES INC.:**
By (Signature):	**By (Signature):**
Name (Printed):	**Name (Printed):**
Title:	**Title:**
Date signed:	**Date signed:**

Exhibit A: Scope of Work
Deployment Services, Data Migration Services, & Ongoing Support

This Scope of Work ("SOW") outlines the services to be provided by GovWell in connection with the implementation of its software platform for the Customer, as well as the ongoing support and maintenance services that follow. It also defines the responsibilities of both the Customer and GovWell to ensure a smooth and effective onboarding experience and continued successful use of the platform. This SOW is incorporated into and governed by the terms of the applicable Order Form.

1. Deployment Services

GovWell and the Customer will collaborate to deploy the GovWell software platform for the Customer's use. A dedicated GovWell Deployment Strategist will be assigned to the Customer to coordinate the deployment process and manage the activities necessary to ensure successful go-live of the platform (the "Deployment Services").

1.1 Scope

The following outlines the services and responsibilities included within the scope of this engagement. These items define the core activities that GovWell and the Customer will undertake to successfully deploy the GovWell platform.

- **Regular meetings with GovWell Deployment Strategist.** Mutual consultations between Customer and the GovWell Deployment Strategist will be conducted via Zoom to define and document Customer's goals, timelines, and workflows; demonstrate deployment progress; and gather and incorporate Customer feedback throughout the deployment process.

- **System configuration.** GovWell will configure the software to reasonably align with the Customer's expressed needs, including setup of the online portal, relevant modules, workflows, forms, document templates, fee structures, inspection settings, user roles and permissions, and other applicable system components. While every effort will be made to reflect the Customer's requirements, configurations will be based on a commercially reasonable interpretation of those needs within the capabilities of the platform.

- **Staff training.** GovWell to conduct virtual training sessions for Customer staff via Zoom. Training sessions are limited to the quantity and duration specified in the Order Form. GovWell will also provide a library of digital training materials and guides, including video demonstrations of key functionality.

- **Integration with Geographic Information System (GIS).** GovWell will reach out to the Customer's designated GIS contact to initiate integration efforts. The Customer is responsible for providing accurate contact information, facilitating introductions, and ensuring their GIS team provides all necessary data in a timely manner. GovWell's ability to integrate is directly dependent on the completeness and responsiveness of the information shared by the Customer's GIS team. Timely access and communication are essential to ensure a smooth integration.

- **Configuration of online payment processing through GovWell.** The Customer is responsible for completing all onboarding forms required by GovWell's integrated payment processor, Finix. GovWell does not support the use of alternative payment processors.

1.2 Timeline

GovWell is committed to bringing the Customer live as quickly as possible and will make commercially reasonable efforts to do so. While the deployment timeline will be discussed and generally targeted during the deployment kickoff meeting, the inherently variable nature of deployment processes means that no specific timeline is guaranteed. GovWell is not responsible for delays resulting from incomplete or inaccurate inputs, delayed responses, or changes in the availability of key Customer personnel, including due to vacations, leave, or other time off.

1.3 Customer Responsibilities

Customer acknowledges that active, timely participation from Customer is necessary to achieve a smooth and effective deployment. Customer responsibilities include, but are not limited to:

- Assign a primary point of contact for each software module to coordinate deployment activities.
- Participate in scheduled virtual meetings with the GovWell Deployment Strategist.
- Submit all requested information and materials in the required formats and within specified timeframes.
- Review and test configurations, provide feedback and approvals to GovWell promptly.
- Complete all onboarding forms required by GovWell's integrated payment processor, Finix (GovWell does not support alternative payment processors).
- Facilitate an introduction to a point of contact responsible for GIS.

1.4 Exclusions & Terms

- Deployment Services do not include custom application development or third-party integrations (other than the ones specified in Section 1.1 (Scope).
- Additional Deployment Services beyond the initial scope may be subject to additional fees specified in section 4 of this SOW.

2. Data Migration Services

GovWell and the Customer will collaborate to migrate the Customer's data into the GovWell software platform for the modules specified in the Order Form. A dedicated GovWell Data Expert will be assigned to coordinate the data migration process and manage the activities necessary to prepare the Customer's data for use within the platform (the "Data Migration Services").

2.1 Scope

The following outlines the services and responsibilities included within the scope of this engagement. These items define the core activities that GovWell and the Customer will undertake to successfully migrate data into GovWell.

- Review and consultation with a GovWell Data Expert to determine project goals, which legacy data is relevant for migration, and appropriate mappings from into GovWell database model.
- Preparation of a written data migration plan for Customer approval.
- One-time import of structured tabular data into GovWell.

2.2 Customer Responsibilities

Customer acknowledges that active, timely participation from Customer is required to achieve a smooth and effective data migration. Customer responsibilities include, but are not limited to:

- **Primary point of contact.** Assign a primary point of contact to coordinate data migration activities in collaboration with GovWell representatives.
- **Data extraction and transfer.** Customer will extract or export source data from legacy systems and transfer to GovWell in structured file formats (e.g., CSV, Excel). GovWell requires two main exports: one export for analysis and planning, and a final export immediately prior to migration. If files are included in the Order Form, Customer will extract and transfer files and attachments to GovWell via SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP). If Customer cannot export source data independently, Customer will be solely responsible for coordinating with their current software vendor to obtain the necessary data.
- **Meeting participation**. Participate in scheduled virtual meetings with a GovWell Data Expert to consult on project goals, answer questions, and facilitate the mapping of source data to the GovWell data model.
- **Migration Plan Approval.** The Customer is responsible for carefully reviewing the written data migration plan and must digitally approve it prior to execution. By approving the plan, the Customer acknowledges that the accuracy, completeness, and alignment of the migration with their expectations are their sole responsibility. GovWell is not liable for any errors, omissions, or outcomes resulting from decisions made or information provided by the Customer. In the event of adverse consequences arising from the approved plan, GovWell will make commercially reasonable efforts to remediate the issue; however, additional costs may apply.
- **Complete migration tasks.** GovWell will make reasonable efforts to place migrated records in the appropriate steps within workflows and minimize the work required by Customer. However, limitations in the source data—such as missing or incompatible information—may prevent certain records from being automatically mapped into the current workflows. In these cases, Customers may be responsible for manually moving records to the correct workflow steps, validating data accuracy, and relocating attachments as needed.

2.3 Exclusions & Terms

In connection with GovWell's standard data migration services, the following are not in scope:

- Verification of source data accuracy, completeness, or quality.
- Data cleaning or validation of source data (e.g., spelling corrections, field splitting, schema mismatch resolution).

- Digitization of physical documents.
- Transforming scanned or handwritten documents into structured data.
- Imports of data that lack sufficient detail to generate a complete and usable entity in GovWell, such as a permit without a permit number or an inspection without a date of completion.
- Training sessions for Customer residents or the public.
- Additional Deployment Services beyond the scope may be subject to additional fees specified in section 4 of this SOW.

2.4 Timelines

GovWell is committed to making the data migration process as smooth and efficient as possible and will make commercially reasonable efforts to support Customer throughout. While timelines will be established and generally targeted during the deployment kickoff meeting, the complexity and variability of data migration means that no specific timeline or outcome can be guaranteed. GovWell is not responsible for delays or limitations resulting from incomplete, inconsistent, or improperly formatted source data, lack of access to required systems, or delays in Customer responses or availability—including due to vacations, leave, or other time off taken by key Customer personnel. This also includes situations where third-party vendors fail to provide data in a timely manner or where the Customer provides critical data, such as large files or datasets, at the last minute (e.g., under 5 days before the scheduled migration). Such circumstances can impact the migration timeline and overall project success, and any resulting delays or additional costs will not be the responsibility of GovWell.

To maintain the integrity and accuracy of the data migration, all configuration changes must be completed prior to the migration process. Because many configuration changes commonly occur after go-live as the platform is fine-tuned to meet the Customer's needs (e.g. modifying the process for a Solar Panel permit or adding required inspections for an Electrical permit), GovWell schedules data migration to take place only after the platform has gone live with the finalized configuration. Performing data migration before finalizing these changes risks data inconsistencies and errors, which can lead to significant additional work and may result in additional fees. This approach helps ensure a clean, reliable migration and a stable platform for ongoing use.

There will be a minimum of five (5) business days between GovWell's receipt of final data and the point at which that data will be accessible and usable within the GovWell system.

Longer timeframes may result from:

- Incomplete or incorrect file formatting.
- Customer-requested changes to migration plan or platform configuration.
- Transfer issues or SFTP protocol delays.

2.5 Limitations

Customer acknowledges that GovWell is not responsible for the quality, completeness, or accuracy of the source data provided for migration. The quality of the source data can directly impact the quality of the data as it appears and functions within the GovWell platform. Data migrations are inherently imperfect, and not all data or structures from legacy systems can be mapped precisely to the new environment. While GovWell will make commercially reasonable efforts to ensure a successful and functional migration, some migrated records may not process as

expected. This may include data appearing differently than in the original system, missing or partially mapped fields, or workflows and automations not functioning as intended.

2.6 Post-Migration Support and Customer Responsibilities

Customer is responsible for carefully reviewing the migration plan to ensure it aligns with their expectations and digitally signing prior to execution. Any data not listed in the migration plan will not be migrated by GovWell. Following the completion of the data migration, GovWell is committed to supporting Customer in addressing issues that may arise, including assisting with reasonable data adjustments if certain records did not migrate as intended. GovWell will make good faith efforts to resolve issues resulting from errors or discrepancies within the scope of the approved plan. Any post-migration adjustments must be scheduled in advance and are subject to GovWell's availability. Significant or time-intensive requests may incur additional charges, as outlined in section 4 of the SOW.

2.7 Service Hours

Data migration service hours are limited to the number of hours specified in the applicable Order Form. These hours cover all activities related to the data migration process, including planning, execution, validation, issue resolution, and consultations. Any services requested beyond the allotted hours may be subject to additional fees, as outlined in section 4 of this SOW.

2.8 Data Security

- If data that Customer intends to migrate contains Sensitive Personally Identifiable Information (SPII), Customer must notify GovWell in advance of sharing the data. SPII includes, but is not limited to, Social Security Numbers, Federal Tax Identification Numbers, Employer Identification Numbers, and other sensitive personal or organizational identifiers,
- All SPII must be transferred via GovWell's secure SFTP channel.
- GovWell is not responsible for data exposure resulting from insecure transmission methods (e.g., email).

3. Continuous Deployment & Product Support Services

GovWell will collaborate with the Customer to provide ongoing support and ensure the GovWell software platform continues to meet Customer's needs following deployment. A new GovWell Deployment Strategist will be assigned after go-live to coordinate support activities and manage the services necessary to ensure the continued successful use and optimization of the platform. In addition to this service, GovWell also offers regular product support channels to address general inquiries, technical issues, and troubleshooting needs.

3.1 Overview

Following the initial deployment, GovWell will provide ongoing support to help the Customer maintain effective use of the platform. This includes two types of services: (1) Continuous Deployment Services: for configuration changes, training, and strategic guidance, and (2) Product Support: for general inquiries, technical support and issue resolution. GovWell may adjust the nature and frequency of these support activities over time based on the Customer's usage of the platform and evolving needs.

3.2 Scope

Requests involving configuration changes, consultations, or training sessions may count against the Customer's allotted Continuous Deployment Services hours as outlined in the Order Form. Technical support inquiries—such as those related to login issues, bug reports, or basic troubleshooting—are not counted against service hours and are addressed through GovWell's regular support channels.

All major service requests submitted through any channel—regardless of whether routed through Deployment Strategists or general support—will be assessed for inclusion in Deployment Services hours. Any services requested beyond the allotted hours may be subject to additional fees, as outlined in Section 4 of this SOW. GovWell will notify Customer in advance of reaching their service hour limit.

The following activities are included in Continuous Deployment Services:

- Configuration changes: Any updates to settings, record types, workflows, fields, templates, etc.
- Consultations: Strategic guidance, best practices, and process mapping.
- Training sessions: Live or recorded training for new staff, refresher sessions, or training on specific modules or features.
- Other service-related tasks: Any request that requires a GovWell team member to perform work beyond a basic fix or answer—for example, correcting misentered data, adjusting a process flow, or preparing a custom report.

The following are not included in Continuous Deployment Services, and are covered by Product Support:

- Bug reports and resolution.
- Login/access issues.
- Basic troubleshooting and how-to questions (e.g., "How do I export a report?").

4. Out-of-Scope Services & Hourly Rates

GovWell is committed to delivering successful Deployment, Data Migration, Continuous Deployment, and Product Support services within the scope and hours outlined in the Order Form. GovWell understands that needs may evolve and additional work may sometimes be necessary to ensure a smooth experience. If the required effort exceeds the included hours or scope, GovWell will communicate with the Customer before proceeding. Any work beyond the agreed scope will only move forward with mutual consent and may be billed at GovWell's standard rates as a last resort.

- Deployment Services: $150 per hour
- Data Migration Services: $200 per hour
- Continuous Deployment Services: $150 per hour

CYBER SECURITY NON-DISCLOSURE ADDENDUM

1. THE PARTIES. This Cyber Security Non-Disclosure Addendum, hereinafter known as the "Addendum," created this [MM/DD/YYYY], is by and between GovWell Technologies Inc., and the City of Grove City, Ohioand collectively known as the "Parties." Each Party may be a disclosing (the "Disclosing Party") or receiving ("Receiving Party") the Confidential Information of the other during the term of this Addendum.

WHEREAS, the Disclosing Party possesses and may disclose certain confidential and proprietary information (the "Confidential Information") to the Receiving Party for the purposes outlined in the Master Agreement;

WHEREAS, the Disclosing Party desires to maintain its internal security processes and procedures as confidential to protect the general public from malicious actors;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

2. DEFINITION OF CONFIDENTIAL INFORMATION. The term "Confidential Information" shall mean any non-public information, including but not limited to technical, financial, business, and any other proprietary information, disclosed by the Disclosing Party to the Receiving Party during the course of diagnostic discussions and consultations, whether explicitly identified as confidential or not.

3. OBLIGATIONS. The Receiving Party agrees to hold the Confidential Information in strict confidence and to take all reasonable precautions to prevent unauthorized disclosure or use of the Confidential Information. The Receiving Party shall not disclose, reproduce, or use the Confidential Information for any purpose other than the purposes explicitly stated in this Agreement.

4. EXCEPTIONS TO CONFIDENTIAL INFORMATION. The obligations of confidentiality shall not apply to information that: (a) was already known to the Receiving Party at the time of disclosure; (b) becomes publicly available or known other than through a breach of this Agreement by the Receiving Party; (c) is independently developed by the Receiving Party without reference to the Confidential Information; or (d) is rightfully received by the Receiving Party from a third party without any confidentiality obligations.

5. RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION. Upon the Disclosing Party's request or termination of discussions, the Receiving Party shall promptly return all copies of the Confidential Information or, at the Disclosing Party's option, certify the destruction of such information in writing.

6. (Reserved)

7. SEVERABILITY. If a court finds that any provision of this Agreement is invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the Parties.

8. ENFORCEMENT. The Parties acknowledge and agree that due to the unique and sensitive nature of the Confidential Information, any breach of this Agreement would cause irreparable harm for which damages and/or *equitable* relief may be sought. The harmed Party in this Agreement shall be entitled to all remedies available at law.

9. GOVERNING LAW. This Agreement shall be governed under the laws of the State of Ohio, and any legal action necessitated by a breach of this Agreement shall be brought in a court of competent jurisdiction in Franklin County, Ohio.

WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date written below.

Receiving Party Signature	Printed Name	Date
GovWell Technologies Inc.		

Disclosing Party Signature	Printed Name	Date

0127090.0607160 4927-7901-2739v2

Vendor Data Protection Addendum

During the course of providing Services, Vendor may obtain, access, or otherwise process Grove City Information, including Personal Information and Sensitive Personal Information from, or on behalf of, Grove City and any affiliated entity identified in the signature pages (collectively, "Grove City"). Vendor agrees to protect all Grove City Information as detailed in this Data Protection Addendum ("DPA").

1. DEFINITIONS. Capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement.

1.1. "Grove City Information" means any Personal Information as defined herein owned or controlled by Grove City, in any form, format, or media (including paper, electronic, and other records), that is provided to Vendor or that Vendor has access to, obtains, uses, maintains, or otherwise handles in connection with the performance of Services.

1.2. "Data Protection Law" means any applicable transnational, foreign, or domestic federal, state, or local law, statute, code, ordinance, regulation, rule, consent agreement, order, injunction, judgment, decree, ruling, constitution, treaty, or other similar requirement of any governmental authority relating to the Processing of Grove City Information.

1.3. "Personal Information" means any information that identifies an individual or relates to an identifiable individual, as defined by Data Protection Law.

1.4. "Process" or "Processing" means the collection, recording, organization, structuring, alteration, access, Disclosure, copying, transfer, storage, deletion, retention, combination, restriction, adaptation, retrieval, consultation, destruction, disposal, sale, sharing, or other use of Grove City Information.

1.5. "Sensitive Personal Information" means any of the following types of Personal Information: (i) Social Security or identity card number, taxpayer identification number, passport number, driver's license number, or other government-issued identification number; (ii) credit or debit card details or financial account number, with or without any code or password that would permit access to the account including Cardholder Information or credit history; (iii) username and password; (iv) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical information, health information, genetic or biometric information, biometric templates, political, religious or philosophical beliefs, political party or trade union membership, background check information, or judicial data such as criminal records or information on other judicial or administrative proceedings; (v) geolocation information accurate within a radius of 1,850 feet or less; (vi) citizenship or immigration status; (vii) information from a known child under the age of 13; or (vii) the contents of an individual's mail, email, or text messages unless Grove City or Vendor is the intended recipient of the communication.

1.6. "Vendor Personnel" means any Vendor's employee, contractor, subcontractor, or agent to whom Vendor authorizes to access or Process Grove City Information.

2. DATA PROCESSING AND PROTECTION

2.1. Compliance with Law. Vendor will comply with all Data Protection Laws applicable to Vendor's Processing of Grove City Information.

2.2. Limitations on Use. Vendor will Process Personal Information only (i) on Grove City's behalf; (ii) to perform the Services; and (iii) in accordance with Grove City's instructions as documented, specified, and limited in the Agreement and as described in Annex I (Description of Transfer). Vendor

will inform Grove City if Vendor believes that any instructions of Grove City regarding the Processing of Grove City Information would violate Data Protection Law. For clarity, and without limiting the generality of the foregoing, in no event may Vendor: (A) sell or share Personal Information (as such term is defined under Data Protection Law); (B) retain, use, or disclose Grove City Information to any third party for the commercial benefit of Vendor or any third party; (C) retain, use, disclose, or otherwise Process Grove City Information outside of its direct business relationship with Grove City or for a commercial purpose other than the business purposes specified in the Agreement and this DPA; or (D) combine Personal Information with other information that identifies, directly or indirectly, an individual or relates to an identifiable individual that Vendor receives from, or on behalf of, other persons, or collects from its own interaction with the individual separate from the Services, except to the extent expressly permitted under the Data Protection Laws. Vendor certifies that it understands and will comply with the foregoing restrictions.

2.3. Confidentiality. Vendor will hold Grove City Information in strict confidence and impose confidentiality obligations on Vendor Personnel who will be provided access to, or will otherwise Process, Grove City Information, including to protect all Grove City Information in accordance with the requirements of this DPA (including during the term of their employment or engagement and thereafter).

2.4. De-identification and Aggregation. If Grove City permits or instructs Vendor to Process Grove City Information in de-identified, anonymized, and/or aggregated form as part of the Services, Vendor will ensure that any such Grove City Information qualifies and remains qualified as de-identified information, anonymized data, de-identified data, and/or aggregate information as defined by Data Protection Laws. Vendor will not attempt to re-identify any individual to whom such Grove City Information relates, will publicly commit to maintaining and using such Grove City Information without attempting to re-identify it, and will take reasonable measures to prevent such re-identification.

2.5. Information Security Program. Vendor will implement, maintain, monitor, and, where necessary, update a comprehensive written information security program that contains appropriate administrative, technical, and physical safeguards appropriate to the nature of the Grove City Information, that are designed protect Vendor's information systems and all Grove City Information against anticipated threats or hazards to its security, confidentiality, or integrity (such as unauthorized access, collection, use, copying, modification, disposal, or Disclosure; unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage; or any other unauthorized form of Processing) ("Information Security Program"). Vendor will assist Grove City in meeting Grove City's obligations under the Data Protection Laws in relation to the security of Processing Grove City Information. The safeguards will meet or exceed prevailing industry standards or an applicable third-party security assurance standard such as ISO 27001/2, SSAE 18 SOC 2, or ISAE 3402 SOC 2. The Information Security Program will include the measures listed in the attached Annex II (Security Measures).

2.6. Data Integrity. Vendor will ensure that all Grove City Information created by Vendor on Grove City's behalf is accurate and, where appropriate, kept up to date, and ensure that any Grove City Information that is inaccurate or incomplete is erased or rectified in accordance with Grove City' instructions.

2.7. Sub-processing. Vendor will not disclose or transfer Grove City Information to, or allow access to Grove City Information by (each, a "Disclosure"), any third party without Grove City' express prior written consent; provided, however, that Vendor may Disclose Grove City Information to its affiliates and subcontractors for purposes of providing the Services to Grove City, subject to the following conditions: (a) Vendor will maintain a list of the affiliates and subcontractors (with contact information and location) and the processing activities to be performed in connection with such Disclosures and will provide this list to Grove City upon Grove City' request; (b) Vendor will provide Grove City with at least 30 days' prior notice of the addition of any affiliate or subcontractor to this list and the opportunity to

object to such addition(s); and (c) if Grove City makes such an objection on reasonable grounds and Vendor is unable to modify the Services to prevent Disclosure of Grove City Information to the additional affiliate or subcontractor, Grove City will have the right to terminate the relevant Processing. If Grove City does not object to the addition of a third party, the new third party will be considered an "Authorized Subprocessor." Vendor will, before any Disclosure, enter into an agreement with such third party that is at least as restrictive as this DPA. \.

2.8. Requests or Complaints. Vendor will promptly notify Grove City in writing, and in any case within five (5) business days of receipt, unless specifically prohibited by applicable law, if Vendor or any Authorized Sub-processor receives: (i) any requests from an individual with respect to Personal Information Processed, including, but not limited to, opt-out requests; requests for access and/or rectification, erasure, or restriction; requests for data portability and all similar requests; or (ii) any complaint relating to the Processing of Grove City Information, including allegations that the Processing infringes on an individual's rights. Vendor will not respond to any such request or complaint except to redirect the individual to Grove City and/or inform the individual that their request was redirected to Grove City unless expressly authorized to do so by Grove City, or unless otherwise required by applicable laws and regulations, including Data Protection Laws. Vendor will cooperate with Grove City with respect to any action taken relating to an individual's request or complaint and will seek to implement appropriate processes (including technical and organizational measures) to assist

Grove City responds to such requests or complaints. Vendor will promptly and securely delete or destroy any Personal Information pertaining to an individual identified by Grove City where such information is within Vendor's possession or control. If applicable, Vendor will direct any Authorized Subprocessor that Processes Personal Information related to the identified individual to promptly and securely delete or destroy such Personal Information. Vendor will confirm to Grove City in writing that it has complied with its obligations under this section.

2.9. Production Requests. If Vendor receives any order, demand, warrant, or any other document requesting or purporting to compel the production of Grove City Information (including, for example, by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil or criminal investigative demands, or other similar processes) by any competent authority ("Production Request"), Vendor will immediately notify Grove City (except to the extent prohibited by applicable law). Vendor will provide Grove City with at least forty-eight (48) hours' notice before the required Disclosure, so that Grove City may, at its own expense, exercise such rights as it may have under law to prevent or limit such Disclosure. Notwithstanding the foregoing, Vendor will exercise commercially reasonable efforts to prevent and limit any such disclosure and to preserve the confidentiality of Grove City Information otherwise and will cooperate with Grove City with respect to any action taken relating to such request, complaint, order, or other document, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Grove City Information.

2.10. Audit. Upon Grove City' written request, to confirm Vendor's compliance with this DPA, as well as Data Protection Laws and any other applicable laws, regulations, and industry standards, Vendor grants Grove City or, upon Grove City' election, a third party on Grove City' behalf, permission to perform a written assessment, audit, examination, or review of all controls in Vendor's physical and/or technical environment in relation to all Grove City Information being handled and/or the Services being provided to Grove City pursuant to the Agreement at most once annually, and at Grove City's sole cost. Vendor shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that process, store, or transport Grove

City Information for Grove City pursuant to the Agreement. Vendor agrees to accurately and promptly complete, a written data privacy and information security questionnaire regarding Vendor's business practices and information technology environment in relation to all Grove City Information being handled and/or the Services being provided by Vendor to Grove City pursuant to the Agreement. Vendor shall fully cooperate with such inquiries. In addition, upon Grove City' request, Vendor shall provide Grove City with the results of any audit by or on behalf of Vendor performed that assesses the effectiveness of Vendor's information security program as relevant to the security and confidentiality of Grove City Information shared during the course of the Agreement, which may include, without limitation, all of the following, as applicable: Vendor's latest Payment Card Industry (PCI) Compliance Report (if applicable), Statement on Standards for Attestation Engagements (SSAE) No. 18 audit reports for Reporting on Controls at a Service Organization, Service Organization Controls (SOC) Type 1, 2, or 3 audit reports.. Vendor will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by Vendor's management.

2.11. Regulatory Investigations. Upon notice to Vendor, Vendor will assist and support Grove City in connection with requests from Grove City customers and law enforcement bodies, regulators, or data protection authorities, including in the event of an investigation, if and to the extent such request relates to Grove City Information handled by Vendor on behalf of Grove City in accordance with this DPA. Such assistance will be at Grove City' sole expense, except where investigation was required due to Vendor's acts or omissions, in which case, such assistance will be at Vendor's sole expense.

2.12. Security Incident.

a) Vendor will notify Grove City in writing by emailing _____ and by telephone at _____ promptly (and in any event within seventy-two (72) hours) whenever Vendor reasonably believes that there has been any accidental or unauthorized access, acquisition, use, modification, Disclosure, loss, destruction of, or damage to Grove City Information or any other unauthorized Processing of Grove City Information (each, a "Security Incident"). Vendor will provide Grove City with information regarding (i) the nature of the Security Incident; (ii) the number of individuals affected, the number of records affected, and the types of records affected; (iii) the likely consequences of the Security Incident;

and (iv) the measures taken or proposed to be taken to address the Security Incident, including measures to terminate unauthorized access or mitigate possible adverse effects of the Security Incident.

b) After providing notice, Vendor will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of the Grove City Information, and keep Grove City informed of the status, cause, and all related matters. Vendor further agrees to provide reasonable assistance and cooperation requested by Grove City and/or Grove City' designated representatives in the furtherance of any correction, remediation, investigation, or recording of any Security Incident and/or the mitigation of any potential damage, including any notification that Grove City may determine appropriate to send to affected individuals, regulators, or third parties, and/or the provision of any credit reporting service that Grove City deems appropriate to provide to affected individuals.

c) Unless required by law applicable to Vendor, Vendor will not notify any individual or third party, other than law enforcement, of any potential Security Incident involving Grove City Information without first obtaining written permission from Grove City.

d) In addition, within thirty (30) days of identifying or being informed of any Security Incident arising from any act or omission by Vendor, Vendor will develop and execute a plan that reduces the likelihood of a recurrence of a Security Incident.

e) To the extent that Grove City is subject to or involved in an investigation by a governmental authority or litigation arising out of or related to a Security Incident, Vendor will provide full cooperation to Grove City in responding to such event.

f) To the extent the Security Incident resulted from a violation of Vendor's duties under this DPA or the Agreement, Vendor will (i) assist with curing any alleged violation and ensure that no further violations shall occur; and (ii) provide Grove City with a written statement confirming such cure and no further violations..

2.13. Cardholder Information. For purposes of this DPA, "Cardholder Information" means any Grove City Information that includes: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates, and magnetic stripe data; and (ii) information relating to a payment card transaction that is identifiable with a specific account. If Vendor has access to Cardholder Information, Vendor must at all times comply with the security standards for the protection of Cardholder Information with which payment card companies require merchants to comply, including, but not limited to, the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time ("PCI Standards"). Vendor will promptly provide, at Grove City's request, current certification of compliance with the PCI Standards by an authority recognized by the payment card industry for that purpose. If, during the term of any relevant agreement (including, for the avoidance of doubt, this DPA), Vendor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI Standards, Vendor will promptly notify Grove City of such circumstances. Vendor will not take any actions that will compromise Grove City's ability to comply with the PCI Standards.

2.14. Return or Disposal. Vendor will, as appropriate and as directed by Grove City, regularly dispose of Grove City Information maintained by Vendor that is no longer necessary to provide the Services. Upon termination or expiration of this DPA for any reason or at any time, upon Grove City' request, Vendor will immediately cease handling Grove City Information and will return such Grove City Information in a manner and format reasonably requested by Grove City or, if specifically directed by Grove City, will destroy any or all Grove City Information in Vendor's possession, power, or control. If Vendor disposes of any paper, electronic, or other record containing Grove City Information, Vendor will do so by taking all reasonable steps (based on the sensitivity of Grove City Information) to destroy Grove City Information by: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying Grove City Information in such records to make it unreadable, unreconstructable, and indecipherable. Upon request, Vendor will provide a written certification that Grove City Information has been returned or securely destroyed in accordance with this DPA if Vendor is required to retain any Grove City Information to comply with a legal requirement. Vendor is permitted to retain one copy of the foregoing materials, as needed, provided that any such copy is encrypted, is not used or accessed for any other purpose, is protected in accordance with the requirements of this DPA, and is promptly destroyed in accordance with this section if no longer required to be retained by law.

2.15. Cooperation. Upon Grove City' request, Vendor will provide assistance and all information in its possession necessary to demonstrate Vendor's compliance with its obligations under this DPA and the Data Protection Laws and assist Grove City in meeting its obligations under Data Protection Laws, including: (i) registration and notification obligations; (ii) accountability; (iii) ensuring the security of Grove City Information; (iv) establishment and maintenance of a record of Grove City Information processing; and (v) conducting and documenting privacy and data protection impact assessments and related consultations of data protection authorities.

2.16. Adverse Changes. Vendor will notify Grove City in writing promptly if Vendor: (i) has reason to believe it is not or will not be able to comply with any of its obligations under the Data Protection Laws or this DPA; or (ii) becomes aware of any circumstances or change in law that is likely to prevent it from fulfilling its obligations under this DPA. Grove City has the right, upon providing notice to Vendor, to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Grove City Information, including where Vendor has notified Grove City that it can no longer meet its obligations under the Data Protection Laws. In the event that this DPA, or any actions to be taken or contemplated to be taken in performance of this DPA, do not or would not satisfy either party's obligations under the law applicable to each party, the parties will negotiate in good faith upon an appropriate amendment to this DPA.

3. PROCESSING LOCATIONS

3.1. Vendor Locations. Personal information will be transferred to and/or accessed from the jurisdiction(s) specified in Annex I ("Vendor Locations"). Vendor will not transfer, or participate in any transfer of, Personal Information to any other jurisdictions without the prior written consent of Grove City. To the extent that Grove City consents to such transfer, Vendor represents and warrants that any transfer of Personal Information will comply with applicable Data Protection Law.

4. MISCELLANEOUS

4.1. Indemnification. (Reserved)

4.2. Survival. The obligations of Vendor under this DPA will continue for as long as Vendor continues to have access to, is in possession of, or control of, or acquires Grove City Information..

4.3. Conflicts. To the extent the terms of the DPA conflict with any Agreement between the parties with regard to the Processing of Grove City Information, the terms of the DPA will prevail.

INFORMATION SECURITY ADDENDUM

This Information Security Addendum ("**Addendum**") is hereby incorporated by reference into the Master Service Provider Contract dated _____ (the "**Agreement**") by and between GovWell Technologies Inc. ("**Vendor**") and the City of Grove City, Ohio, and shall be considered a part of the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. In the event of any dispute or inconsistency between the terms of this Addendum and the terms of the Agreement, the terms of this Addendum shall control. Capitalized terms not defined in this Addendum shall have the meaning given to them in the Agreement. In addition to the mutual promises and obligations set forth in the Agreement, Supplier agrees to certain supplemental security provisions, as further described below and as applicable.

1. Information Security Program. This Addendum describes the minimum information security controls and standards that shall be maintained by Vendor to protect the confidentiality, integrity, and availability of data and information of Grove City (all such data and information "System Information", as such term is further defined below), whether in physical or electronic format.

Vendor shall maintain a comprehensive, written information security program in compliance with all applicable laws and regulations that includes appropriate administrative, technical, physical, organizational, and operational safeguards, designed to (a) insure the security, privacy, and confidentiality of System Information, (b) protect against any reasonably anticipated threats or hazards to the security or integrity of System Information, and (c) protect against unauthorized access to, use, deletion, or modification of System Information (hereinafter "**Information Security Incident**").

Vendor shall maintain a commercially reasonable process for identifying, assessing, and mitigating risks to System Information in Vendor's operations, and for evaluating the effectiveness of safeguards to control these risks.

In addition, Vendor shall monitor, test, and update its Information Security Program in alignment with ISO 27001 Information Security Standard Certification or NIST Cybersecurity Framework, and/or obtain ISO 27001, SSAE 16 SOC 2 TYPE II, or SOC 3 audit report.

Where applicable, Vendor shall comply with the PCI Data Security Standard (Payment Card Industry Data Security Standard of the PCI Security Standards Council) by obtaining a PCI Attestation of Compliance (AoC).

2. Data Security. Vendor shall safeguard information or items provided by Grove City to Vendor to allow Vendor to access System Information, their respective computer networks, or their respective premises or those of other service providers or their respective clients, including keycards, codes, usernames, passwords, keys, badges, as well as information that, if disclosed, would compromise the security of System Information, such as the designs of Grove City's networks, information controls, or design of their respective computer systems.

At Grove City's request, and in a timely manner, Vendor shall securely destroy or return all System Information in its possession and certify to Grove City in writing that it has done so. If Vendor destroys

System Information rather than return it, Vendor shall use destruction methods in compliance with all applicable state and federal laws and regulations.

3. Access Control. Vendor shall restrict access to System Information only to those employees, agents, or subcontractors who need to know the information to perform their job functions, including privileged access, based on need-to-know and Principle of Least Privilege.

Vendor shall deploy secure authentication and authorization security mechanisms, including password management, use of multifactor authentication ("**MFA**") for external Internet-Facing systems, remote access, and privileged access, and use of secure proxy or jump box server to further secure privileged access.

4. Cryptographic Controls. Vendor shall use commercially reasonable cryptographic controls using AES 256-bit or stronger and TLSv1.2 and practices based on industry acceptable security frameworks such as NIST including, but not limited to, authentication and messaging encryption, encryption of System Confidential and Personal Information over public and/or wireless networks (e.g., email, ftp, etc.), encryption of portable media, laptops, desktops, smartphones, mobile devices, data at-rest, and in-transit encryptions.

5. Secure Code Deployment. Vendor shall establish a secure Systems Development Lifecycle (SDLC) to address *Confidentiality*, *Integrity,* and *Availability* of the System, using industry acceptable secure code development frameworks such as The Open Web Application Security Project (OWASP) and SysAdmin, Audit, Network and Security (SANS), including change management, testing methodology, and annual secure code training to its developers.

6. Technical Vulnerability Management. Vendor shall deploy security controls and processes to identify and remediate vulnerabilities continuously, and to reduce the risk of unauthorized access or modification to System Information, including daily scans of external Internet-Facing systems and weekly internal vulnerability scans.

Vendor shall deploy a process to keep its software, services, platforms, and applicable hardware up to date with the latest security patches, updates, and releases, and to maintain a secure configuration of all hardware and software in compliance with industry-accepted security standards, such as NIST and CIS Benchmarks.

On an annual basis, Vendor shall engage a reputable third-party security firm to perform penetration testing and provide the results to Grove City. Upon receipt of the test result, Vendor shall document any vulnerabilities, evaluate and rank them based on severity, impact, and likelihood, as recommended by the third-party security firm and industry acceptable security standards and practices, and address any high-risk vulnerabilities within 30 days of the vulnerability's identification date.

7. Security Logging and Monitoring. Vendor shall deploy security controls to continuously monitor, in real-time, application, infrastructure, network, firewalls, intrusion detection and prevention systems, endpoint systems, and data storage spaces and systems to identify, prevent, detect, and respond to potential threats and unauthorized access and/or activities to System Information. System logging shall be enabled to capture end-users' and administrators' activities, and the logs shall be reviewed on a periodic basis for

failed and successful login attempts and for suspicious and unauthorized activities. Security logs shall contain details on the date, time, source, and event types and be maintained for forensic purposes for 30 days.

8. Threat Management. Vendor shall deploy network perimeter defense solutions, including firewalls and intrusion detection and prevention systems (IDS/IPS) and monitor boundaries between public and private networks to detect and prevent malicious activities and threats. Supplier shall deploy segmentation to isolate and control access to protect the perimeter, internal, and external networks. Supplier shall deploy mechanisms to prevent social engineering attacks (e.g., phishing, vishing, and smishing).

Vendor shall deploy effective malware protection technology and processes to monitor, detect, and prevent malicious software and actors, including real-time prevention and weekly scanning. Vendor shall deploy technologies and methods to appropriately configure and update firewalls, intrusion detection and prevention, and malware protection software.

9. Physical Security. Vendor shall deploy physical security measures and processes to restrict, monitor, and prevent unauthorized access to its facilities, data centers, and corporate offices, including use of key cards, badges, video cameras, logging, and security personnel.

10. Security Incident Management. Vendor shall deploy security incident management capabilities, plans, and teams to assess, escalate, and respond to identified physical and cyber security incidents that impact Vendor's and Grove City's *Confidentiality*, *Integrity,* and *Availability* of data and information.

Vendor shall have a documented security incident response plan that is reviewed, updated, and tested annually, and updated after lessons learned exercise(s) when applicable, and to incorporate industry developments and changes in data classification and systems. Security incident management shall also be integrated into the business continuity plan.

11. Third Party Security. Vendor shall have a process to assess the risk associated with new vendors prior to onboarding, including an ongoing risk management process for existing vendors. Vendor shall have a method to communicate security and confidentiality requirements, as well as operational responsibilities, to third parties through contractual agreements.

Before using a third party to provide services to Grove City under the Agreement, Vendor shall first obtain Grove City's consent in writing, and Vendor shall require those third parties to agree in writing to provide the same safeguards for System Information as required by this Addendum. Vendor shall be responsible for any such third parties' failure to provide the same safeguards for System Information as required by this Addendum.

12. Oversight and Audit. Vendor shall have a process to conduct internal control assessments to validate that controls are designed and operating effectively. Vendor shall document, track, and remediate issues identified from assessments, as appropriate. Vendor shall also engage an external independent auditor to perform an assessment of internal controls related to security, availability, and confidentiality at least annually, and in accordance with applicable regulatory and industry standards. Independent audit reports shall be provided to Co-op upon completion of the audit.

13. Business Continuity Plan. Vendor shall have a documented plan and strategy to manage significant disruptions to operations and infrastructure, including business impact analysis performed at least annually. The plan shall be reviewed, updated, and tested annually.

14. Human Resources Security. Vendor shall have a program and process for personnel to sign a confidentiality agreement, acknowledge their understanding of security policies during the new employee onboarding process, and receive security awareness training at the time of hire and annually thereafter. Vendor shall perform background verification checks for personnel that will have access to System Information, in accordance with relevant laws and regulations, and commensurate with an individual's job duties, including reference checks, social security verification, and a criminal history check.

15. Compliance with Laws. In the performance of this Agreement, Supplier, and any employees, subcontractors, agents or other personnel of Supplier, shall comply with all applicable federal, state, and local laws, regulations, and codes ("**Applicable Law**"). Applicable Law includes, without limitation, federal, state, and local laws and regulations governing or relating to privacy rights in connection with its performance under this Agreement.

Definitions

1. **"Incident"** means a security event that compromises the integrity, confidentiality, or availability of an information asset.

2. **"Breach"** means an Incident that results in the confirmed disclosure, —not just potential exposure, —of data to an unauthorized party. A Breach is any act or omission that compromises either the security, confidentiality, or integrity of System Information or the physical, technical, administrative, or organizational safeguards put in place by Supplier or Authorized Persons that relate to the protection of the security, confidentiality, or integrity of Personal Information or the receipt of a complaint in relation to the privacy or security practices of the Supplier or a breach or alleged breach of this Addendum relating to such privacy or security practices.

3. **"System Information"** means:

- Personal Information;
- System Client Information; and
- System Confidential Information.

4. **"System Confidential Information"** means:

- Non-public business information of the Co-op, the Servicers, and/or the Selected Buyers or otherwise with respect to the System that a reasonable person would understand is confidential; and
- Any information defined as "Confidential" by the Agreement to which this Addendum is attached.

5. **"Personal Information"** means any information identifying, relating to, describing, reasonably capable of being associated with, or that could reasonably be linked, directly or indirectly, with an identified or identifiable person or household. Any information considered "Personal Data" (or any similar definition) under Applicable Laws shall be considered Personal Information.

6. **"System Client Information"** means any information relating to Vendor's or Grove City's representation of their respective clients. This includes, but is not limited to, the client's name, the

fact that they are a client of any of the foregoing, information provided to any of the foregoing by a client, the advice given to clients, etc.

GovWell Technologies Inc.

By:

Name:

Title: