## COMPANY PAID BENEFIT AGREEMENT

This Company Paid Benefit Agreement ("Agreement") is made and entered into this _____day of March, 2017 ("Effective Date") between Pre-Paid Legal Services, Inc. dba LegalShield ("LS"), One Pre-Paid Way, Ada, Oklahoma 74820, an Oklahoma corporation and City of Delray Beach (Company), 100 NW 1st Avenue, Delray Beach, FL 33444 a(n) municipal corporation. The parties agree as follows:

For mutual consideration, the sufficiency of which is acknowledged by the parties, Company agrees to purchase for their employees, as a Company paid benefit, the LS Plan(s) listed in the attached Exhibit A for a monthly cost to Company as specified in Exhibit Attached as Exhibit B is a LS Security Overview.

The number of employees eligible at the inception of this Agreement is 1,084 of which 680 have an individual plans and 404 have a family plan. Company will provide the necessary information for processing to LS no later than thirty (30) days from the effective date. Enrollment file will be submitted to LS electronically via a template to be supplied to Company by LS.

LS shall invoice Company each month for the membership fees due. Company or Company's Representative shall promptly remit such funds to LS, which shall be no later than thirty (30) days after invoice. Company shall pay a guaranteed minimum fee to LS of $4,065 per month for twelve (12) months, even if the number of enrolled employee members falls below 1,084 members.

If this benefit is being provided to employees in response to a breach situation, Company shall deliver communications to all employees advising them of the breach situation and their purchase of the IDShield product on their behalf and how to activate it. It shall be the responsibility of the member to activate the service.

LS agrees that participants enrolled into this plan will be exempt from any pre-existing condition exclusions or clauses, arising from a breach of the Company's information, as long as they are a qualified, eligible participant, and remain active in the Plan.

This Agreement shall commence on the effective date and shall continue for a term of one (1) year. This Agreement shall not automatically renew. The continuation of this Agreement beyond the end of any fiscal year shall be subject to both the appropriation and the availability of funds in accordance with Florida law. Pricing will be guaranteed for the duration of the one year term. Company shall pay the guaranteed minimum fee to LS of $4,065 per month, for the twelve (12) months. Should the Company fail to make a monthly payment, LS has the right to cancel the services for the enrolled members, and the remaining balance of the fees for the remaining months shall immediately be due from the Company.

Company may only terminate this Agreement if LS fails to perform their obligations under this Agreement and does not cure such failure within fifteen (15) days after Company has given written notice thereof.

In the event this Agreement expires, Company shall allow each LS member to continue a self-pay membership at a rate to be determined by LS and all membership information collected by LS will remain the property of LS.

LS agrees to indemnify and hold Company and its officers, directors, agents and affiliates harmless from any loss, damage, liability, costs or expenses (including reasonable attorney fees) arising from any claim by any employee relating to the employee's membership in LS including, but not limited to, any claim by such member relating to member's acquisition of the membership or receipt of benefits. Company shall give LS written notice of any claim for indemnity hereunder and LS shall defend such claim.

Without the prior written consent of the other Party, neither Party may assign this Agreement.

This Agreement shall be governed by and construed in accordance with the laws of the State of Florida without reference to conflict of laws principles. All parties agree and accept that jurisdiction of any controversies or legal problems arising out of this Agreement, and any action involving the enforcement or interpretation of any rights hereunder, shall be exclusively in the federal or state courts in Palm Beach County, Florida, and venue for litigation arising out of this Agreement shall be exclusively in such courts, forsaking any other jurisdiction which either party may claim by virtue of its residency or other jurisdictional device. If any action at law or in equity is brought to enforce or interpret the provisions of this Agreement, each party is responsible for their own attorney's fees and costs incurred. **BY ENTERING INTO THIS AGREEMENT, LS AND COMPANY HEREBY EXPRESSLY WAIVE ANY RIGHTS EITHER PARTY MAY HAVE TO A TRIAL BY JURY OF ANY CIVIL LITIGATION RELATED TO THIS AGREEMENT. AFTER WRITTEN NOTICE BY THE OTHER PARTY OF VIOLATION OF THIS SECTION, THE PARTY MAKING THE REQUEST FOR JURY TRIAL SHALL BE LIABLE FOR THE REASONABLE ATTORNEYS' FEES AND COSTS OF THE OTHER PARTY IN CONTESTING THE REQUEST FOR JURY TRIAL, AND SUCH AMOUNTS SHALL BE AWARDED BY THE COURT IN ADJUDICATING THE MOTION.**

**IF LS HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO LS'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT CITY OF DELRAY BEACH, CITY CLERK, 100 N.W. 1ST AVE., DELRAY BEACH, FL. THE CITY CLERK'S OFFICE MAY BE CONTACTED BY PHONE AT 561-243-7051 OR VIA EMAIL AT** CITYCLERK@MYDELRAYBEACH.COM.

LS shall comply with all public records laws in accordance with Chapter 119, Florida Statutes. In accordance with state law, LS agrees to:

a. Keep and maintain all records that ordinarily and necessarily would be required by the Company.

b. Provide the public with access to public records on the same terms and conditions that the Company would provide for the records and at a cost that does not exceed the costs provided in Chapter 119, Florida Statutes, or as otherwise provided by law.
c. Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law.
d. Meet all requirements for retaining public records and transfer, at no cost, to the Company all records in possession of LS at the termination of the contract and destroy any public records that are exempt or confidential and exempt from public records disclosure requirements. All records stored electronically must be provided to the Company in a format that is compatible with the information technology systems of the Company. All records shall be transferred to the Company prior to final payment being made to LS.
e. If LS does not comply with this section, the Company shall enforce the contract provisions in accordance with the contract and may unilaterally cancel this contract in accordance with state law.

LS is aware that the Inspector General of Palm Beach County has the authority to investigate and audit matters relating to the negotiation and performance of this contract, and may demand and obtain records and testimony from LS. LS understands and agrees that in additional to all other remedies and consequences provided by law, the failure of LS to fully cooperate with the Inspector General when requested may be deemed by the Company to be a material breach of this Agreement justifying its termination.

Notice under this Agreement shall be to the following individuals:

If to LegalShield:

Pre-Paid Legal Services,
Inc., d/b/a LegalShield
One Pre-Paid
Way Ada,
Oklahoma 74820
Attn: General Counsel
Regulatory@legalshieldcorp.com
(email)

If to City of Delray Beach:

City of Delray Beach
100 NW 1st Avenue
Delray Beach, FL 33444

Attn: Human Resources
radig@mydelraybeach.com
(email)

IN WITNESS WHEREOF, the parties have executed this Agreement to be effective as of the Effective Date set forth above.

PRE-PAID LEGAL SERVICES, INC.,
d/b/a LEGALSHIELD

By: Steve Williamson
Name: Steve Williamson
Title: CFO

ATTEST:

CITY OF DELRAY BEACH

City Clerk

By:
Name: Cary Glickstein
Title: Mayor

APPROVED AS TO FORM:

By:

R. Max Lohman, City Attorney

## Exhibit A

The following Plan(s) at the monthly membership fee rate(s) shall be provided:

Individual IDShield Membership - $3.00 per employee per month.

Minimum employee count per month is 680.

Family IDShield Membership - $5.00 per employee per month.

Minimum employee count per month is 404.

Exhibit B
LegalShield Security Overview

# Security Overview

**Security Overview**
LegalShield values the importance of safeguarding your information and the systems used to store and process your information. Keeping your information safe and secure is the responsibility of everyone. LegalShield encourages everyone to take steps in protecting their personal information.

All information is stored on LegalShield servers located in the United States. Procedural and technical safeguards are in place to protect personal information against loss or theft as well as unauthorized access and disclosure. Information is treated as an asset that must be protected against loss and unauthorized access. Several security technologies are utilized to protect information from unauthorized access by user inside and outside of LegalShield.

Extended Validation Secure Socket Layer certificates are in use when personal information is uploaded or viewed on our website. Each member has a unique user name and password that must be entered every time a user logs on to our website. Firewalls and layered security technologies prevent interference or access from outside intruders. The website is hosted on servers located in a secure data center.

LegalShield takes the privacy of your information very seriously. For specific information regarding our privacy policy, our privacy policy can be viewed at: www.legalshield.com/privacy-policy/.

**Security and Auditing**
LegalShield has implemented a layered security approach to protect your information. Below is a summary of the security and auditing controls. Please note that specific technology details are not disclosed here because releasing such information could jeopardize our security posture.

**Physical Security at Corporate Headquarters**
Security guards and video cameras are present throughout the building grounds and within the building. The buildings and grounds are monitored 24 x 7. The first layer of physical security is the gate at the entrance to the property. The gates are open during normal business hours and visitors are directed to park in visitor parking and then register at the front desk. An intercom system is available at the security gate for questions or off hour usage.

The second layer of physical security are the proximity card key readers, software and badges that control physical access to our buildings and all secured areas within the building. Restricting physical access ensures that our computing assets (servers, network, information, etc.) are not exposed to unwarranted risks. Off-hour access to the gate at the entrance to the property is controlled by card key access.

The third layer of physical security is the restriction of physical access to the data centers to those staff members required to have access to perform their job functions. All other staff members and vendors are required to sign-in to these areas and they must be escorted in these areas for the duration of their visit.

**Logical Security**
Security software and devices are used to protect against unauthorized access, destruction, disclosure or modification of information and applications programs. Logical access controls are layered and govern access to the network, servers, applications and information. Logical access to the network, servers, applications and information is restricted to only those staff members required to have access to complete their job functions.

All employees and contractors are required to login to the internal network first and authenticate. Once network access has been authenticated then an internal user can login to applications which require additional authentication. User access privileges are established on a standard, authorized access request process and are granted in accordance with job-related duties.

**Data Protection**
LegalShield has adopted an information classification system for all information under LegalShield control. When it is necessary to retain information classified as Confidential or Restricted, we store it in a physically secure location.

When documents containing Confidential or Restricted information are disposed of, the documents are placed inside a locked shred bin or shredded immediately. All Confidential information is encrypted when transmitted across public networks.

Credit card information is transmitted to a third-party credit card processing company who clears the transactions and processes the payments. The credit card processing company has security practices in place to protect this information and is independently audited.

Our electronic billing department, within Support Services, verifies encryption methods that meet our requirements are being used when sensitive information is being transmitted or received related to electronic deposits.

**Incident Detection, Response and Reporting**
LegalShield employs a variety of resources to record and analyze system activity for the express purpose of identifying unusual conditions or suspect activity. Any exceptions are logged and investigated. Our incident detection procedures require that any suspected or actual incident be escalated immediately. Management is committed to following our incident response plan and all applicable local, state and federal law.

**Environmental Protections**
Computer operations and services are protected by the following safeguards and environmental control systems:

a. Smoke Detectors
b. Fire alarm system
c. Raised floors
d. Climate conditioning
e. Emergency power-off
f. UPS including battery backup
g. Automatic fire suppression system
h. Hand-held fire extinguishers
i. Water detectors
j. Temperature and humidity control devices
k. Emergency lighting

and diesel generator power

**Disaster Preparedness**
Every business is exposed to a range of threats, events and risks that could cause a disaster declaration. From power failures, fires, hazardous chemical spills, labor unrest, terrorist attacks on the company's facilities or nearby buildings, a disaster can quickly bring an organization's daily business operations to a halt. For this reason, Disaster Recovery (DR) and Business Continuity Planning (BCP) has become an essential element in LegalShield's strategic business plans.

DR and BCP provides LegalShield an increased level of confidence that its business processes and the IT data processing center are prepared to respond to disaster events and recover and resume daily business operations, while preparing to restore operations at a new or repaired business location.

During a declared disaster, senior management will authorize the relocation of Data Center services to an Alternate Site. LegalShield's recovery teams will implement the Alternate Site Recovery Strategy during an actual disaster to restore critical processing. LegalShield maintains, and annually tests, a comprehensive Business Continuity and Disaster Recovery Plan to mitigate the impact of disruptive conditions and major crises.

**Proactive Assessments**
LegalShield manages potential risks to network devices by running weekly vulnerability scans and patching on a monthly basis. All web applications are scanned for cross-site scripting, SQL injections and other common vulnerabilities prior to deployment to the production environment. Security experts conduct annual internal vulnerability assessments and quarterly external vulnerability scans are done by Payment Card Industry Approved Scanning Vendors. The findings provide confirmation of our security practices as well as the opportunity for improvement. Findings and recommendations are discussed and corrective action is taken to address any vulnerabilities. This process provides continual improvement to our security posture.

Testing of internal controls as required by executive management provides additional confirmation of our strong security measures. Best practices have been implemented for security practices, where possible. Third-party auditors and controls experts have been contracted to test and verify that our internal controls for business applications and information technology are designed and operating effectively.

Users of system applications and information technology are recertified quarterly by conducting a review of user access by department to verify access is restricted based upon job duties. The least-privilege concept for providing access to information resources is in use. Each user will have only the access necessary to perform their job duties. Department managers will request appropriate changes to user access for their employees if necessary. When changes are made to user access the department manager is required to review the request to confirm the changes were implemented and then signoff on completed changes.

**Payment Card Industry Data Security Standard**
LegalShield has validated its compliance with the Payment Card Industry Data Security Standard (PCI DSS) through a third-party audit conducted by a Qualified Security Assessor. An audit for compliance with the PCI DSS is performed annually.

**Report on Controls at a Service Organization SOC 2 and 3 Certifications**
LegalShield has maintained effective controls over its Legal Services system, based on the American Institute of Public Accountants ("AICPA") and Chartered Professional Accountants of

Canada ("CPA Canada") for trust services security, availability, processing integrity, and confidentiality criteria to provide reasonable assurance that:

- The system was protected against unauthorized access (both physical and logical);
- The system was available for operation and use, as committed or agreed;
- The system processing was complete, accurate, timely, and authorized; and
- The system information designated as confidential was protected as agreed.

The SOC 3 report can be viewed at: https://cert.webtrust.org/pdfs/soc3_legalshield.pdf

LegalShield has engaged with a Public Company Accounting Oversight Board (PCAOB) registered, licensed Certified Public Accountant (CPA) firm to test the operational effectiveness of controls for the trust services principals; security, availability, confidentiality, and processing integrity, using the American Institute of Certified Public Accountants (AICPA) Guide. An audit is performed annually.

**How you can help**

LegalShield believes it is extremely important for you to share in the responsibility for security. Here are some ways you can protect yourself and your account:

• Select a password that will be difficult to guess. Include letters and numbers and special characters if allowed.

• Never share your password with anyone. Remember that a support representative will never ask you for your password. Your password should not be written on paper or emailed to anyone.

• Change your password on a regular basis. If you think your password has been compromised, change it and contact us immediately.

• Use a personal firewall to prevent hackers from gaining access to your personal computer.

• Install virus protection software and set it up to automatically scan all downloaded software, as well as all email attachments. Also, set the software to auto-update