STATE OF MINNESOTA
JOINT POWERS AGREEMENT

This Joint Powers Agreement ("JPA") is between the State of Minnesota, acting through its Department of Administration ("Admin"), the City of St. Paul ("St. Paul"), and the Metropolitan Airports Commission ("MAC"), collectively ("the Parties").

Recitals

WHEREAS, Under Minnesota Statute §471.59, subdivision 10, the Parties are empowered to enter into this agreement for their collective benefit; and

WHEREAS, the MAC is a party to the Minnesota Unified Certification Program ("MNUCP"), a joint program established under Federal Regulations to administer the Disadvantaged Business Enterprise and Airport Concessions Disadvantaged Business Enterprise Programs ("DBE/ACDBE Programs"), together with the City of Minneapolis ("Minneapolis"), the Metropolitan Council ("Met Council"), and the Minnesota Department of Transportation ("MNDOT") (together, the "MNUCP Partners"); and

WHEREAS, the City of Saint Paul is the lead agency for the Central CERT Program, a regional certification program established under local law to administer the Central CERT certification and outreach program, together with the City of Minneapolis, Hennepin County, and Ramsey County; and

WHEREAS, the MAC currently owns and is responsible for the operation and administration of, and owns exclusive intellectual property rights to, an online application portal for the DBE/ACDBE Programs for the benefit of the MNUCP; and

WHEREAS, St. Paul and Admin each currently operate separate certification programs, namely the CERT program administered by St. Paul and the Targeted Group/Economically Disadvantaged/Veteran-Owned Small Business Program ("TG/ED/VO") operated by Admin (both, together with the DBE/ACDBE Programs, the "Certification Programs"); and

WHEREAS, the Parties desire a single portal for the Certification Programs to streamline application processes and reduce the burden on applicants when submitting information to become certified to participate in the respective programs.

NOW THEREFORE, the Parties agree as follows:

Agreement

1 Term of Agreement

1.1 ***Effective date*****:** January 1, 2017, or the date Admin obtains all required signatures under Minnesota Statutes Section 16C.05, subdivision 2, whichever is later.

1.2 ***Expiration date*****:** This contract will remain in effect until terminated pursuant to Section 10.

2 Agreement between the Parties

1. The Parties agree to utilize a single portal system to collect applicant information to be utilized for purposes of certification into the Certification Programs. To the greatest extent practicable, the shared system shall be the exclusive portal system utilized by the Parties to collect applicant data.

2. To accomplish the goal of a streamlined single certification process for applicants, the Parties will develop and utilize a registration portal system based on the MAC's existing MNUCP registration portal system, as modified according to the terms of this JPA, to meet the information needs of the Parties.

3. The Parties agree to appoint one representative each to serve on a Single Certification Governance Committee ("Governance Committee"). The MNUCP and CERT Partners shall also be permitted to appoint one representative each to serve on the Governance Committee. Each representative shall:

a. Be empowered to make decisions and make commitments on behalf of their organization, subject to approvals of the governing bodies as may be required by law;
b. Assist in defining system requirements, processes and data elements; and
c. Meet regularly to address system and program needs.

The members shall work to reach consensus on matters related to the single portal system. In the event a vote is necessary to reach final decisions, the signators to this JPA comprise the voting members of the Governance Committee.

4. The MAC hereby provides to Admin a limited non-exclusive perpetual license (" License") to software, including source code, related to the MNUCP registration portal (the "Licensed Technology") as described herein. Admin may develop derivative works and otherwise use the Licensed Technology solely for the purpose of developing, operating, and administrating a common registration portal for the Certification Programs for the benefit of the Parties as contemplated by this JPA (the "Purpose"). Admin may reproduce the Licensed Technology only for governmental purposes, including the creation of a redundant system for backup purposes. The License is limited to Admin and may not be used by any other party, except as expressly consented to by the MAC in writing. MAC retains full title to and ownership of the Licensed Technology. Admin's perpetual license to the Licensed Technology and the indemnification provision contained herein survive the termination of this JPA.

   Any and all derivative works developed pursuant to this JPA shall be owned by the MAC and become a part of the Licensed Technology.

   To the extent allowable by law, Admin agrees to indemnify and hold completely harmless the MAC against any claims or causes of action of any kind, including in tort and for infringement, together with the reasonable documented costs for defense of such claims and causes of action, caused by Admin's use or modification of the MAC's Licensed Technology in a manner outside the scope of this JPA.

5. Admin will contract with vendor(s) as necessary to conduct initial system development to implement modifications to the system based on requirements as defined by the Governance Committee. Admin is responsible to develop, test, deploy, maintain, and operate the system. "Help" links and/or telephone numbers for technical assistance shall be directed to Admin and/or its vendor. "Help" links and/or telephone numbers for subject matter assistance shall be directed to the relevant entities.

6. Admin shall provide regular updates to the Governance Committee regarding system activities including, but not limited to, changes in data management practices, all other software and hardware changes, scheduled and unscheduled maintenance, system downtime, etc. All updates to the system shall be first tested in a closed test environment with a reasonable opportunity for the Parties and MNUCP Partners to review and/or test and shall be implemented with full ability to roll updates back in the event that problems occur.

7. MAC shall be granted two administrator-level log-in credentials with respect to all DBE/ACDBE functions. Admin shall be responsible for securing and protecting program applicant data in accordance with federal regulations and Exhibit A. In the event of a conflict, the federal regulations shall apply. Only users designated by the MNUCP Partners, together with technical administrators with the need, shall have access to DBE/ACDBE application information. DBE/ACDBE applicant data shall be expunged from the system 90 days after an application is completed.

8. The registration portal interface shall be maintained according to Web Content Accessibility Guidelines ("WCAG") 2.0, as it may be updated from time to time, except as otherwise agreed to by the Parties.

9. This JPA is entered into, in part, expressly for the benefit of the MNUCP Partners and CERT partners, even if not a party to this JPA. It is intended by the Parties that the MNUCP Partners and CERT partners be intended beneficiaries of this JPA, with all associated rights and privileges inuring to them.

3 Payment

Admin will pay for the initial development of the system in an amount not to exceed $210,000.

Funding required post-implementation to maintain or modify the shared system for the benefit of all Parties ("O&M Costs") will be paid initially by Admin and, by reimbursement, shared equally among the Parties and paid annually. Admin shall provide periodic updates to the Governance Committee regarding O&M Costs and the reasonable justification therefore. O&M Costs shall be calculated on a fiscal calendar ending June 30 and be due and payable by the Parties within 30 days of invoice thereafter. Each Party shall only be committed to annual O&M Costs up to $1,200 (escalating by 5% per fiscal year) unless otherwise agreed to in writing.

Post-implementation costs incurred that substantially benefit fewer than all of the Parties shall be born among the benefiting parties as they shall decide among themselves in writing. Such costs shall not be applied to the annual $1,200 threshold.

The MAC may seek financial contribution from the MNUCP Partners for any of its expenses related to this JPA, and the City of Saint Paul may seek financial contribution from the CERT Collaborative Partners for any of its expenses related to this JPA.

The Parties are responsible to pay for their own internal systems modifications or costs associated with modifying internal business processes necessary to accommodate the shared application.

The total obligation of Admin under this agreement for initial system development and implementation costs will not exceed $210,000 for state fiscal year 2017.

In the event that payments provided for in this JPA are insufficient to complete development of or maintain and operate the system to the reasonable satisfaction of all Parties, and after a reasonable period of time to secure additional funding from the Parties sufficient funding is not provided, this JPA will terminate immediately upon notice by any Party.

4 Single Certification Governance Committee

The representatives authorized to serve on the Governance Committee shall be as follows:

Admin
Dorothy Lovejoy, Assistant Director, 50 Sherburne Avenue, St. Paul, MN 55155, (651) 201-2403, or her successor.

MAC
Anita Bellant, Diversity Manager, 6040 28th Avenue South, Minneapolis, MN 55450, (612) 726-8196, or her successor.

St. Paul
Jessica Brokaw, Deputy Director, 15 Kellogg Boulevard West, 280 City Hall, St. Paul, MN 55102, (651) 266-8966, or her successor.

Minneapolis
Velma Korbel (MNUCP), Director, 350 South 5th Street, City Hall, Minneapolis, MN 55415, (612) 673-3012, or her successor; Mwende Nzimbi (CERT), Assistant Director, Procurement, 330 Second Avenue S., Room 552, Minneapolis, MN 55401, (612) 673-2333, or her successor.

Met Council
Wanda Kirkpatrick, Director, 390 Robert St. North, St. Paul, MN 55101, (651) 602-1085, or her successor.

MNDOT
Kim Collins, Director, 395 John Ireland Blvd., St. Paul, MN 55155, (651) 366-3150, or her successor.

Hennepin County
Michael Rosenfeld, Manager of Negotiated Procurement, Hennepin County Purchasing and Contract Services, A-1730 Hennepin County Government Center – MC 175, 300 South Sixth Street, Minneapolis, MN 55487-0225, (612) 348-5210, or his successor.

Ramsey County
Dana Nofke, Procurement Manager, 210 Courthouse, 15 West Kellogg Blvd., St. Paul, MN 55102, or her successor.

Governance Committee members may be changed by providing written notice to the Parties and MNUCP Partners.

5 Assignment, Amendments, Waiver, and Contract Complete

5.1 ***Assignment.*** The Parties may neither assign nor transfer any rights or obligations under this agreement without the prior consent of the Governance Committee and a fully executed Assignment Agreement, executed and approved by the same Parties who executed and approved this agreement, or their successors in office.

5.2 ***Amendments.*** Any amendment to this agreement must be in writing and will not be effective until it has been executed and approved by the same Parties who executed and approved the original agreement, or their successors in office.

5.3 ***Waiver.*** If a Party fails to enforce any provision of this agreement, that failure does not waive the provision or its right to enforce it.

5.4 ***Contract Complete.*** This agreement contains all negotiations and agreements between the Parties. No other understanding regarding this agreement, whether written or oral, may be used to bind any party.

6 Indemnification

The Parties are responsible for their own respective acts and behavior and the results thereof. The Minnesota Torts Claims Act, Minn. Stat. §3.736 and other applicable law govern the state's liability.

7 State Audits

Under Minnesota Statute § 16C.05, subdivision 5, the Parties' respective books, records, documents, and accounting procedures and practices relevant to this agreement are subject to examination by the State and/or the State Auditor or Legislative Auditor, as appropriate, for a minimum of six years from the end of this agreement, except as otherwise provided by law.

8 Government Data Practices

The Parties must comply with the Minnesota Government Data Practices Act, Minnesota Statute Ch. 13, as it applies to all data provided under this agreement, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the Parties under this agreement. The civil remedies of Minnesota Statute §13.08 apply to the release of the data referred to in this clause by the Parties.

49 CFR Parts 23 and 26 govern the treatment of certain data in the DBE/ACDBE Programs. Each Party agrees to comply with the requirements of those provisions at all times, and to notify the other Parties if it knows or has reason to know of the failure to comply with the terms of this requirement.

See Exhibit A for additional requirements regarding data handling and security.

If any Party receives a request to release the data referred to in this clause, it must immediately notify the other Parties. In any event, no DBE/ACDBE application data shall be disclosed to any party without prior notice to the MAC with reasonable opportunity to object.

9 Venue

Venue for all legal proceedings out of this JPA, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

10 Termination

10.1 ***Termination.*** The Parties may terminate this agreement at any time, with or without cause, upon 90 days' written notice to the other parties. In the event of a breach of this JPA, any non-breaching party may provide notice of the breach to all other parties. The breaching party shall then have 10 business days to cure the breach. If the breach has not been cured within the cure period, any non-breaching party may terminate this JPA effective immediately.

10.2 ***Termination for Insufficient Funding***. Any Party may immediately terminate this agreement if funding cannot be provided at a level sufficient to allow for the payment of the services covered herein. Termination must be by written notice to the other Parties. No Party is obligated to pay for any services for which payment obligations were incurred after notice and effective date of termination. In such event, each Party shall bear its own expenses. No Party shall be assessed any penalty if this JPA is terminated because of the decision of the Minnesota Legislature, or other funding source, not to appropriate funds. Parties must provide the other Parties notice of the lack of funding within a reasonable time of such decision.

10.3 ***Effect of Termination.*** See Exhibit A for additional requirements regarding data handling at termination.

The remainder of this page has been left intentionally blank.

1. STATE ENCUMBRANCE VERIFICATION
Individual certifies that funds have been encumbered as required by Minnesota Statute §§ 16A.15 and 16C.05.

Signed: ____

Date: ____

SWIFT Contract No.__________________________________

2. CITY OF ST. PAUL

By: ____

Title: ____

Date: ____

3. METROPOLITAN AIRPORTS COMMISSION

By: ____

Title: ____

Date: ____

4. STATE OF MINNESOTA

By: ____
(with delegated authority)

Title: ____

Date: ____

5. COMMISSIONER OF ADMINISTRATION
As delegated to Materials Management Division

By: ____

Date: ____

Distribution:
Agency
Governmental Unit

State's Authorized Representative - Photo Copy

Exhibit A

Security and Data Protection

Admin is responsible for the security and protection of any data collected, created, received, maintained or disseminated by it and its contractors under this JPA. The terms of this Exhibit survive the expiration, cancellation, or termination (collectively, "completion") of this JPA. Admin will treat all data received in the same manner and with the same protocols as Admin treats its own data. Admin will make good faith efforts to comply with the following:

1. Definitions

a. **Administering Party:** The Party responsible for the administration of a particular program to which an applicant may apply via the registration portal. For example, with respect to the TGB program and TGB Applicant Data, Admin is the Administering Party.

b. **Applicant Data:** all data submitted by an applicant for one or more programs via the registration portal, regardless of its physical form, storage media or conditions of use.

c. **Cloud Computing:** has the meaning given in the U.S. Department of Commerce, NIST Special Publication 800-145, currently available online at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

d. **Confidential Information:** all information that is or could be not public data under Minnesota Statutes, section 13.02, subdivision 8a. "Confidential Information" may include any information in any medium, regardless of whether the information is marked as "Confidential" or otherwise identified as not public data.

"Confidential Information" does not include data which Admin's written records demonstrate are: (1) rightfully in Admin's possession prior to the effective date of this JPA and free of any confidentiality obligation; or (2) developed or received independently from the Purpose.

e. **Connected Device**: A physical device, sensor, or appliance provided under this JPA that collects data and has any of the following characteristics:

- ability to connect to or exchange data with the internet or a network via Wi-Fi, Ethernet, Bluetooth, cellular, RFID, NFC, ZigBee or other means;
- ability to connect to or exchange data with other devices via Wi-Fi, Ethernet, Bluetooth, cellular, RFID, NFC, ZigBee or other means; or
- an IP address.

The following hardware provided under this JPA are not Connected Devices:

f. **Covered Data**: all data collected, created, received, maintained or disseminated by Admin under this JPA, regardless of its physical form, storage media or conditions of use. Without limiting the foregoing, Covered Data expressly includes the Licensed Technology and Applicant Data.

g. **Industry Standards:** generally recognized industry standards include the following:

i. Center for Internet Security - see http://www.cisecurity.org

ii. Payment Card Industry/Data Security Standards (PCI/DSS) – see http://www.pcisecuritystandards.org/

iii. National Institute for Standards and Technology - see http://csrc.nist.gov

iv. Federal Information Security Management Act (FISMA) - see http://csrc.nist.gov

v. Organization for the Advancement of Structured Information Standards (OASIS) – see http://www.oasis-open.org/

h. **MGDPA:** the Minnesota Government Data Practices Act, Minnesota Statutes ch. 13

i. **Unauthorized Access**: the unauthorized use, disclosure, access, modification, or destruction of data or interference with systems operations, including improper or unauthorized disclosure, access to or alteration of Confidential Information; improper or unauthorized access to or alteration of public data; improper or unauthorized access of a Connected Device; and incidents in which the confidentiality of data maintained by Admin is breached. This includes a violation of the Minnesota Government Data Practices Act (Minnesota statutes ch. 13) or any applicable privacy requirements under state or federal law, rule, or regulation.

2. Ownership. Ownership of Applicant Data, including all rights, title, and interest, whether express or implied, shall reside in the Administering Party for each program. In the event that an applicant applies to more than one program, each Administering Party shall have ownership of the associated Applicant Data as if the data had been submitted directly to that Administering Party without utilizing the registration portal that is the subject of this JPA. With respect to data in Admin's possession but not owned by Admin, such data shall merely be held in trust in favor of the owner of such data.

3. Data Security. Admin agrees to preserve the confidentiality, integrity, and accessibility of the Covered Data with administrative, technical, and physical measures that conform to Industry Standards and best practices. Maintenance of secure storage, processing, production, and development environments by Admin includes Admin timely applying patches, fixes and security updates to operating systems and applications.

4. Data Encryption. Admin must encrypt all Covered Data (including data generated by a Connected Device) at rest and in transit, in compliance with FIPS Publication 140-2 or similar encryption method, or applicable law, regulation or rule, whichever is a higher standard. Admin must use encryption keys that are unique to Covered Data. Admin may only access encryption keys to Covered Data as necessary for performance of this JPA.

5. Data Transmission. Admin agrees that all electronic transmission or exchange of system and application data with the Parties, MNUCP Partners, and any other parties permitted under this JPA must occur using secure means (using HTTPS or SFTP or equivalent). Admin agrees that all data exchanged must be used only for the purposes permitted in this JPA. Admin will not distribute, repurpose, or share Covered Data across other applications, environments, or business units of Admin. Admin further agrees not to transmit, exchange or otherwise share Applicant Data except with the prior written agreement of the Administering Party or Parties.

6. Subcontractors and Third Parties. Except as otherwise agreed to in writing by the Parties, Admin will require any contractors, subcontractors, agents, suppliers or others to whom Admin provides Covered Data to agree in writing to be bound by the terms of this Exhibit B.

7. Return and Destruction of Covered Data. Upon completion, termination, or expiration of this JPA for any

reason, Admin must do the following:

a. Return all Covered Data to the owning entity in a format and media reasonably specified by the owning entity.

b. After receiving written authorization from the owning entity, Admin must within 90 days sanitize and destroy any Covered Data (including backups) according to current Industry Standards, including any Covered Data on a Connected Device in Admin's possession. Within 14 days after any sanitization and destruction of data under this section, Admin must certify in writing to all Parties on the Governance Committee that the sanitization and destruction occurred.

8. Notice of Unauthorized Access. Admin must notify every member of the Governance Committee via email, within 24 hours of discovery, of any instance of Unauthorized Access, attempted unauthorized access, or other compromise of Covered Data or Connected Device.