A G R E E M E N T

THIS AGREEMENT ("Agreement") is made and entered into this 11th day of December, 2018 ("Effective Date"), by and between the COUNTY OF FRESNO, a Political Subdivision of the State of California ("COUNTY"), and CSDC Inc., a Delaware corporation, whose address is 804 Las Cimas Parkway, Suite 100, Austin, Texas 78746 ("CONTRACTOR").

W I T N E S S E T H:

WHEREAS, COUNTY is in need of maintenance and support services and upgrades for the County Building Permit System ("AMANDA"), procured through County Contract No. 04-450, dated September 28, 2004;

WHEREAS, COUNTY currently has an Agreement with CONTRACTOR, Agreement No. 14-069, dated February 25, 2014, and amended on January 26, 2016, for maintenance and licensing services for AMANDA for COUNTY'S Department of Public Works and Planning, and COUNTY desires to supersede and replace that agreement, as amended, with this Agreement;

WHEREAS, COUNTY desires to purchase software license, installation, training, data conversion, and software maintenance of AMANDA from CONTRACTOR for COUNTY'S Department of Public Health and Department of Public Works and Planning, as set forth in the COUNTY's Request for Proposal (RFP) No. 18-011, dated September 29, 2017;

WHEREAS, CONTRACTOR has represented to COUNTY that the software license, installation, training, data conversion, and software maintenance of AMANDA, along with professional services from CONTRACTOR would meet the stated needs of the COUNTY, as provided in the Statement of Work (SOW), attached as Exhibit B and incorporated by this reference;

WHEREAS, COUNTY desires to purchase from CONTRACTOR continuous maintenance and support services for AMANDA; and

WHEREAS, COUNTY and CONTRACTOR desire to execute this Agreement for the purchase of the right to use the software licenses, and maintenance and support of the AMANDA software.

NOW, THEREFORE, in consideration of the mutual covenants, terms and conditions herein contained, the parties agree that the prior Agreement 14-069, as amended, shall be superseded and

replaced in its entirety by this Agreement, and further agree as follows:

1.) **DEFINITIONS:**

The following terms used throughout this Agreement shall be defined as follows:

Acceptance Criteria:

The performance and operating specifications that the System must meet at a minimum, as set out or referred to in this Agreement.

Acceptance Test:

The process of testing a specific function or functions to determine if the operation or operations are as stated in this Agreement.

Application Administrator:

A designated employee or contractor of COUNTY responsible for managing the AMANDA System. This role includes communicating with CONTRACTOR staff for support, troubleshooting problems, and coordinating maintenance tasks.

Change Control Process:

Process used by the Information Technology Services Division of COUNTY's Internal Services Department (ISD) to inform staff of new or updated production use systems.

County System Hardware:

The central processing units owned or leased by COUNTY, on which COUNTY is licensed to use the System Software, any back-up equipment for such central processing units, and any peripheral hardware such as terminals, printers, and Personal Computers, as described in this Agreement.

COUNTY System Software:

The operating system and database software installed on the COUNTY System Hardware.

Final System Acceptance:

When COUNTY determines in writing that all necessary deliverables have been delivered, the data has been converted, the base AMANDA software has been successfully installed and tested, and AMANDA performs all functions in accordance with its specifications.

First Production Use:

Date of first use of the System in a production environment.

License:

The meaning assigned to the term 'License" as defined in Section 2(A) of this Agreement and the rights and obligations it creates under the laws of the United States of America and the State of California including without limitation, copyright and intellectual property law.

Monies:

The terms "Monies", "Charges", "Price", and "Fees" will be considered to be equivalent.

Public Records:

Public Records includes any writing containing information relating to the conduct of the public's business that is prepared, owned, used, or retained by any state or local agency, regardless of physical form or characteristics, with the exclusion of records expressly exempted from disclosure by statute.

Supplier:

The terms "Supplier", "Vendor", and "CSDC Inc." all refer to CONTRACTOR and are considered to be equivalent throughout this Agreement.

System:

The System Software and System Documentation, collectively. Reference to the "System" shall include any component thereof. All modifications and enhancements to the System shall be deemed to be part of the System and shall be subject to all terms and conditions set forth in this Agreement. The System consists of AMANDA, which supports various Fresno County Departments, all interfaces, and third-party software required for the System to function.

System Documentation:

The documentation relating to the System Software, and all manuals, reports, brochures, sample runs, specifications and other materials comprising such documentation provided by CONTRACTOR in connection with the System Software pursuant to this Agreement.

System Operation:

The general operation of COUNTY's hardware and all software including, but not limited to, System restarts, configuration and operation of System peripherals (such as printers, modems, and terminals), installation of new software releases, and other related activities.

System Installation:

All software has been delivered, has been physically loaded on a COUNTY computer, and COUNTY has successfully executed program sessions.

System Software:

AMANDA, that certain computer software described in this Agreement provided by CONTRACTOR, and all interfaces, coding, tapes, disks, modules and similar materials comprising such software or on which it is stored.

User:

The terms "User", "Customer" and "Licensee" all refer to COUNTY and are considered to be equivalent throughout this Agreement.

User Profile:

A record of User-specific data that define the User's working environment. The record can include display settings, application settings, and network connections. What the User sees on his or her computer screen, as well as what files, applications and directories they have access to.

2.) **OBLIGATIONS OF CONTRACTOR:**

A. SOFTWARE LICENSE

I. GRANT OF LICENSE

CONTRACTOR grants to COUNTY and COUNTY accepts a non-exclusive, non-transferable, perpetual license to use AMANDA, subject to the terms and conditions set forth in this Agreement.

II. SCOPE OF LICENSE

The license granted herein shall consist solely of the non-exclusive, non-transferable right of COUNTY to operate the System Software in support of various COUNTY departments, including COUNTY's Department of Public Works and Planning and Department of Public Health.

III. OWNERSHIP

The parties acknowledge and agree that, as between CONTRACTOR and COUNTY, title and full

ownership of all rights in and to the System Software, System Documentation, and all other

materials provided to COUNTY by CONTRACTOR under the terms of this Agreement shall remain

with CONTRACTOR. COUNTY will take reasonable steps to protect trade secrets of the System

Software and System Documentation. Ownership of all copies is retained by CONTRACTOR.

COUNTY may not disclose or make available to third parties the System Software or System

Documentation or any portion thereof. CONTRACTOR shall own all right, title and interest in and to

all corrections, modifications, enhancements, programs, and work product conceived, created or

developed, alone or with COUNTY or others, as a result of or related to the performance of this

Agreement, including all proprietary rights therein and based thereon. Except and to the extent

expressly provided herein, CONTRACTOR does not grant to COUNTY any right or license, express

or implied, in or to the System Software and System Documentation or any of the foregoing. The

parties acknowledge and agree that, as between CONTRACTOR and COUNTY, full ownership of

all rights in and to all COUNTY data, whether in magnetic or paper form, including without limitation

printed output from the System, are the exclusive property of COUNTY.

IV.   POSSESSION, USE AND UPDATE OF SOFTWARE

COUNTY agrees that only COUNTY will use the System Software for its own internal purposes.

CONTRACTOR may, at reasonable times, inspect COUNTY's premises and equipment to verify

that all of the terms and conditions of this license are being observed. CONTRACTOR may create,

from time to time, updated versions of the System Software and System Documentation and

CONTRACTOR shall make such System Updates available to COUNTY. All System Updates shall

be licensed under the terms of this Agreement. COUNTY agrees to follow the prescribed

instructions for updating System Software and System Documentation provided to COUNTY by

CONTRACTOR. COUNTY must authorize all System Updates in writing.

V.   TRANSFER OF SOFTWARE

COUNTY shall not rent, lease, license, distribute, sell, transfer, or assign this license, the System

Software, or the System Documentation, or any of the information contained therein other than

COUNTY data, to any other person or entity, whether on a permanent or temporary basis, and any

attempt to do so will constitute a breach of this Agreement. No right or license is granted under this

Agreement for the use or other utilization of the licensed programs, directly or indirectly, for the benefit of any other person or entity, except as provided in this Agreement.

VI.   POSSESSION AND USE OF SOURCE CODE

Source code and other material that results from custom programming by CONTRACTOR released to COUNTY under this license shall be deemed CONTRACTOR software subject to all of the terms and conditions of the software license set forth in this Agreement. The scope of COUNTY's permitted use of the custom source code under this license shall be limited to maintenance and support of the System Software. For purposes of this Section, the term "maintenance and support" means correction of System Software errors and preparation of System Software modifications and enhancements. If COUNTY creates computer code in the process of enhancing the System Software, that specific new code shall be owned by COUNTY and may be used by COUNTY's employees, officers, or agents for COUNTY's own internal business operations. However, if COUNTY's enhancement results in the creation of a derivative work from the System Software, the copyright to such derivative work shall be owned by CONTRACTOR and COUNTY's rights to use such derivative work shall be limited to those granted with respect to the System Software in this Agreement.

VII.   RESTRICTIONS ON USE

COUNTY shall not (i) license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit or make available to any third-party the System Software or the System Documentation in any way; (ii) modify or make derivative works based upon the System Software or the System Documentation; (iii) create Internet "links" to the System Software or "frame" or "mirror" any System Documentation on any other server or wireless or Internet-based device; (iv) send spam or otherwise duplicative or unsolicited messages in violation of applicable law; (v) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children or violative of third-party privacy rights; (vi) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs; (vii) interfere with or disrupt the integrity or performance of the System Software or the data contained therein, including but not limited to COUNTY Data; (viii) attempt to

gain unauthorized access to the System Software or its related systems or networks; (ix) reverse

engineer or access the System Software in order to (a) build a competitive product or service, (b)

build a product using similar ideas, features, functions or graphics of the System Software, or (c)

copy any ideas, features, functions or graphics of the System Software.

B. SERVICES TO BE PROVIDED BY CONTRACTOR TO COUNTY

I. SYSTEM INSTALLATION

CONTRACTOR shall supply and install AMANDA in accordance with this Agreement. Such

software installation shall include hardware/network review and recommendations, consultation,

software installation and remote technical support.

II. TRAINING

CONTRACTOR will conduct two types of training for COUNTY staff: one for AMANDA Users and

one for AMANDA administrators, as described in Exhibit B. These trainings shall occur at a

COUNTY designated location and at a time approved in writing by COUNTY.

III. USER AND ADMINISTRATOR DOCUMENTATION

CONTRACTOR shall provide to COUNTY AMANDA System Documentation, which shall consist

of electronic media files. The electronic media files must be printable using PC software normally

available at COUNTY. CONTRACTOR shall provide new System Documentation corresponding

to all new Software Upgrades. COUNTY may print additional copies of all documentation. All

System Documentation is to be used by COUNTY only for the purposes identified within this

Agreement.

C. SYSTEM MAINTENANCE AND SUPPORT BY CONTRACTOR

System maintenance and support includes System Updates as they are released by

CONTRACTOR, including updates as required as a result of Federal Regulatory Changes. The first day

of production use will be identified by COUNTY and communicated to CONTRACTOR. CONTRACTOR

will support day-to-day operation of the System as follows:

I. SUPPORT HOURS/SCOPE

During the term of this Agreement, CONTRACTOR shall provide unlimited technical assistance

by phone during normal coverage hours (8:00 a.m. to 5:00 p.m. Eastern Time, Monday through

Friday, except CONTRACTOR and COUNTY holidays), toll-free telephone assistance to keep the System in, or restored to, normal operating condition. The object of this support will be to answer specific questions related to the System Software and the application thereof. Support provided under this Agreement does not include training of new personnel (after initial staff is trained), operation of hardware, or solving other hardware/software problems unrelated to the System Software.

II. SUPPORT RESPONSE

During the term of this Agreement, CONTRACTOR will (a) correct any error or malfunctions in the System as supplied by CONTRACTOR that prevents it from operating in accordance with the specifications set forth in this Agreement or (b) provide a commercially reasonable alternative that will conform to the specifications set forth in this Agreement.

If analysis by CONTRACTOR indicates a reported problem is caused by a reproducible error or malfunction in the then-current release of the System Software as supplied and maintained by CONTRACTOR that significantly impacts effective use of the System by COUNTY, CONTRACTOR will, if the System is inoperable, as reported by COUNTY, provide continuous effort to correct the error or to resolve the problem by providing a circumvention.

In such cases, CONTRACTOR will provide COUNTY with corrective information, such as corrective documentation and/or program code. CONTRACTOR will endeavor to respond to COUNTY's service request no later than four (4) business hours from the time a call has been received by CONTRACTOR. In the event that a person with the necessary expertise is not available when the call is received, CONTRACTOR will endeavor to respond to the service request no later than within one (1) business day from the time of the COUNTY'S service request.

III. REMOTE VIRTUAL PRIVATE NETWORK (VPN) DIAGNOSTICS

Remote VPN Diagnostics Support includes:

a. Diagnostic or corrective actions necessary to restore proper AMANDA operation;

b. Diagnostic actions which attempt to identify the cause of system problem;

c. Correction of data file problem; and

d. AMANDA modifications

CONTRACTOR product specialists will provide diagnostics via VPN on AMANDA. COUNTY will provide any required hardware and equipment necessary at COUNTY for CONTRACTOR VPN support.

IV.   ERROR CORRECTION PROCESS

If during the term of this Agreement COUNTY determines that software error(s) exist, COUNTY will first follow the error procedures specified in the System Documentation. If following the error procedures does not correct the software error, COUNTY shall immediately notify CONTRACTOR, setting forth the defects noted with specificity. Upon notification of a reported software error, CONTRACTOR shall have five (5) days to determine if any actual software error exist and, if so, to correct such software errors. At CONTRACTOR's request, additional time to solve difficult problems will not be unreasonably withheld. Within fifteen (15) days of correction, COUNTY shall retest the System Software and report any other software error(s).

V.   TECHNICAL INFORMATION

CONTRACTOR will provide technical information to COUNTY from time to time. Such information may cover areas such as AMANDA usage, third-party software, and other matters considered relevant to COUNTY by CONTRACTOR. Technical information will be provided at the discretion of CONTRACTOR but will not be unreasonably withheld.

D. ADDITIONAL SYSTEM MAINTENANCE SERVICES BY CONTRACTOR

CONTRACTOR may provide additional maintenance services ("Additional Maintenance and Support Services" or "Additional Maintenance Services") at an additional charge. Charges will be as identified in Section 6 of this Agreement and/or in Exhibit B; or, if not included in this Agreement and/or Exhibit B, the charges will be at CONTRACTOR's then-standard prices in effect at the time the goods or services are provided. Any Additional Maintenance and Support Services requested by COUNTY and determined by CONTRACTOR to be billable by CONTRACTOR must be identified as a chargeable service prior to the service being performed and must be approved in writing in advance by COUNTY's Contract Administrator. Additional Maintenance Services include, but are not limited to, the following:

I. ADDITIONAL TRAINING

A specific amount of training is specified in this Agreement. Additional training at a COUNTY facility is available upon request by COUNTY at an additional charge under the terms of this Agreement. Requests for additional training will be reviewed by CONTRACTOR and must be requested in writing in advance by the COUNTY's Contract Administrator. Charges and terms for additional training are as follows: (a) $650.00 per trainee during the first year of this Agreement (with a 3% annual increase each year thereafter) **plus** (b) CONTRACTOR travel and expenses; provided that any additional training will require a minimum class size of four (4) trainees and a maximum class size of ten (10) trainees.

II. DATA AND SYSTEM CORRECTIONS

Data and System Corrections include any corrective actions accomplished by CONTRACTOR on-site or via VPN that are necessary due to COUNTY errors or unauthorized source code or data access by COUNTY. Unauthorized access to the data is defined as any COUNTY editing of data through other than normal system usage, as defined in System Documentation. Unauthorized access to source code is defined as any COUNTY access whatsoever to System source code. Services provided by CONTRACTOR are not billable to COUNTY when they result from errors caused by AMANDA or instruction provided by CONTRACTOR.

III. CUSTOMER SITE VISITS

Site visits to COUNTY sites, as may be requested in writing by COUNTY and that are within the scope of the project services, are available for reasons such as, but not limited to, (1) additional System training on hardware or software usage; (2) resolution of System difficulties not resulting from actions by, or otherwise the responsibility of CONTRACTOR (as determined by mutual agreement between CONTRACTOR and COUNTY); (3) installation of Software Releases; and (4) assistance in equipment maintenance, movement or diagnosis. Site visits outside of the scope of project services will be reviewed by CONTRACTOR and must be requested in writing in advance by the COUNTY's Contract Administrator. Charges will be at rates identified in this Agreement.

IV. CUSTOM PROGRAMMING

Requests for supplemental programming or customization of system features not covered under this Agreement are available to COUNTY. Such requests will be reviewed by CONTRACTOR and must be requested in writing in advance by the COUNTY's Contract Administrator. These charges will fall under "Services Hours", which is priced at $165 per hour as described in Exhibit B.

E. CONTRACTOR PROJECT COORDINATOR

Upon execution of this Agreement, CONTRACTOR shall appoint a Project Coordinator who will act as the primary contact person to interface with COUNTY for implementation, maintenance and support of AMANDA.

F. SYSTEM UPDATES AND NEW PRODUCTS

I. SYSTEM UPDATES

From time to time CONTRACTOR will develop and provide System Updates to COUNTY for the COUNTY'S licensed CONTRACTOR software. System Updates shall be subject to the terms and conditions of this Agreement and shall be deemed licensed System Software hereunder and will be made available to COUNTY at no additional charge to COUNTY. System Updates will be made available to COUNTY at the discretion of CONTRACTOR but will not be unreasonably withheld.

II. NEW PRODUCTS

CONTRACTOR may from time to time release new software with capabilities substantially different from or greater than the System Software ("New Products") and which therefore do not constitute System Updates. These New Products will be made available to COUNTY at a cost not to exceed CONTRACTOR's then standard rates for customers similarly situated.

G. OPERATING SYSTEM UPDATES

The application must run on a client operating system that is consistently and currently supported by the operating system vendor. Applications under maintenance are expected to always be current in regard to the required client O/S. No outdated or unsupported client O/S will be implemented on the production network. COUNTY will apply patches to both the client O/S and security subsystems on COUNTY PCs as releases are available from O/S vendors.

In order to support a secure environment, the application must run on the latest supported release of any required third-party software, such as JAVA, Flash, etc. COUNTY will notify CONTRACTOR when a critical security patch is released for such products. CONTRACTOR will have 30 days to ensure application can perform in the updated environment.

COUNTY will actively run anti-virus management on all PCs. The application is expected to perform adequately while anti-virus management is active.

COUNTY will notify CONTRACTOR when a critical security patch is released. CONTRACTOR will have 30 days to ensure application can perform in the updated environment. The application is expected to perform in this environment. CONTRACTOR is expected to keep their software current in order to operate in this environment. These patches include critical O/S updates and security patches.

H. ANTI-VIRUS MANAGEMENT

COUNTY will actively run anti-virus management, where appropriate, on all application servers and PCs. The application is expected to perform adequately while anti-virus management is active.

I. ADHERE TO CHANGE CONTROL PROCESS

CONTRACTOR must adhere to COUNTY's Change Control Process, which shall be provided to CONTRACTOR in writing. COUNTY employs a procedure to implement updates, upgrades, and version releases to a system that is in production use. This forum allows ISD to inform staff (Help Desk, Network, Server, Database, Security, and Analysts) of upcoming changes to a production system. CONTRACTOR must inform ISD a minimum of two (2) weeks prior to any planned, non-emergency changes so that the Change Control Process may be followed.

J. OTHER

Unless otherwise specified, for third-party software, CONTRACTOR shall provide standard documentation in electronic form (via the Internet or File Transfer Protocol (FTP).

K. CLIENT INSTALL

Should AMANDA require installation of software on the client PC, AMANDA will not be installed under a specific User Profile, but and it must install available to all Users on the all Users desktop. AMANDA can require an administrator to install AMANDA, but AMANDA must not require administrative

rights in order to operate AMANDA.

L. PROTECTION OF INFORMATION

CONTRACTOR shall be responsible for properly protecting all information used, gathered, received, or developed in performing its obligations under this Agreement in accordance with its security safeguards, which will be made available to COUNTY upon request. CONTRACTOR shall also protect all COUNTY data and equipment used, gathered, or received by CONTRACTOR in performing its obligations under this Agreement by treating such information as sensitive. Data processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure, modification, theft, or destruction in accordance with CONTRACTOR's security safeguards. Such data shall be COUNTY Information subject to the confidentiality provisions of Section 13.

M. SAFEGUARDS

With respect to confidential, personal, or sensitive data received by CONTRACTOR from COUNTY under this Agreement, CONTRACTOR shall utilize a commercial encryption solution that has received Federal Information Processing Standards (FIPS) 140-2 validation to encrypt all confidential, personal, or sensitive data stored on portable electronic media (including, but not limited to, compact disks and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers).

With respect to confidential, personal, or sensitive data received by CONTRACTOR from COUNTY under this Agreement, CONTRACTOR shall not transmit confidential, personal, or sensitive data via e-mail or other internet transport protocol unless the data is encrypted by a solution that has been validated by the National Institute of Standards and Technology (NIST) as conforming to the Advanced Encryption Standard (AES) Algorithm.

3.) **OBLIGATIONS OF COUNTY**

A. COUNTY CONTRACT ADMINISTRATOR

COUNTY appoints its Director of Internal Services/Chief Information Officer (ISD Director/CIO) or his designee, as COUNTY's Contract Administrator ("Contract Administrator") with full authority to deal with CONTRACTOR in all matters concerning this Agreement.

B. CONTRACTOR RESPONSE COMMITMENT

COUNTY shall designate one or more Application Administrator(s), each of whom shall be an employee or contractor of COUNTY. Only a designated Application Administrator may request support. It is the responsibility of COUNTY to instruct Users to route support requests through the Application Administrator. No support shall be provided with respect to any request made by a person who is not an Application Administrator.

C. SAFEGUARDING SYSTEM SOFTWARE

COUNTY will follow its present practices to safeguard System Software delivered to COUNTY by CONTRACTOR. A copy of COUNTY'S "Information Technology (IT) Standards and Preferences" will be made available upon request.

D. BACKUP AND RECOVERY MANAGEMENT

I. COUNTY utilizes a backup and recovery system written and maintained by Commvault Systems. This application requires a backup agent to run on the server.

III. In order for the application to run on COUNTY supported servers, the application must not require the Users to have administrative rights on the servers.

IV. COUNTY, at all times, during and after the performance of the installation of the System Software, is responsible for maintaining adequate data backups to protect against loss of data.

E. ACCEPTANCE TESTING

COUNTY shall approve Final System Acceptance when AMANDA has been successfully tested and satisfactorily performs all functions necessary pursuant to this Agreement, and all deliverables identified in this Agreement as required for acceptance have been received by COUNTY.

F. ACCEPTING TESTING PROCESS

Following delivery and installation, CONTRACTOR shall test AMANDA, along with COUNTY personnel.

G. FACILITIES AND PREPARATION

COUNTY will at its own expense provide all necessary labor and materials for site preparation, electrical services, and cabling required for System Installation. COUNTY shall receive the System Software and will follow instructions provided by CONTRACTOR to load it on COUNTY's System Hardware to prepare the System for processing.

H. SYSTEM HARDWARE AND SYSTEM SOFTWARE

COUNTY will at its own expense provide and properly maintain and update on an ongoing basis all necessary COUNTY System Software and County System Hardware required to operate AMANDA. COUNTY System Software and County System Hardware shall meet or exceed CONTRACTOR's recommendations.

As part of COUNTY's responsibility for computer infrastructure, COUNTY is responsible for ensuring that data is secure and protected at all times. CONTRACTOR is not responsible for and cannot be held liable for inadvertent data disclosure or theft from COUNTY facilities.

I. COUNTY PROJECT MANAGER

Upon execution of this Agreement, COUNTY's Contract Administrator shall designate one individual from ISD who will function as Project Manager with responsibility for day-to-day management of the project for implementation of AMANDA. The Project Manager and COUNTY personnel shall have the necessary and appropriate training and experience to implement the terms of this Agreement. COUNTY acknowledges CONTRACTOR'S reliance on same.

J. OTHER COUNTY OBLIGATIONS

Technical assistance from COUNTY's ISD staff will be provided during the performance of the installation of the System Software. In particular, COUNTY will provide:

a.   Network connectivity and troubleshooting assistance.

b.   Ability to monitor network traffic and isolate bottlenecks.

c.   Technical assistance concerning the integration with existing COUNTY systems (if applicable).

d.   Expertise to handle issues with PCs, printers, and cabling before, during, and after rollout.

4.) **TERM**

The term of this Agreement shall be for a period of five (5) years, commencing on Effective Date through and including December 3, 2023. This Agreement may be extended for five (5) additional consecutive twelve (12) month periods upon written approval of both parties no later than thirty (30) days prior to the first day of the next twelve (12) month extension period. The ISD Director/CIO or his or her designee is authorized to execute such written approval on behalf of COUNTY based on CONTRACTOR'S satisfactory performance.

5.) **TERMINATION**

A. <u>Non-Allocation of Funds</u> - The terms of this Agreement, and the services to be provided hereunder, are contingent on the approval of funds by the appropriating government agency. Should sufficient funds not be allocated, the services provided may be modified, or this Agreement terminated, at any time by giving the CONTRACTOR thirty (30) days advance written notice.

B. <u>Breach of Contract</u> - The COUNTY may immediately suspend or terminate this Agreement in whole or in part, where in the determination of the COUNTY there is:

    I.   An illegal or improper use of funds by CONTRACTOR;

    II.   A failure to comply with any term of this Agreement by CONTRACTOR;

    III.   A substantially incorrect or incomplete report submitted by CONTRACTOR to the COUNTY;

    IV.   Improperly performed service by CONTRACTOR.

In no event shall any payment by the COUNTY constitute a waiver by the COUNTY of any breach of this Agreement or any default which may then exist on the part of the CONTRACTOR. Neither shall such payment impair or prejudice any remedy available to the COUNTY with respect to the breach or default. CONTRACTOR shall promptly refund upon demand any funds disbursed to CONTRACTOR in contravention of this Agreement.

C. <u>Without Cause</u> - Under circumstances other than those set forth above, this Agreement may be terminated by COUNTY by giving thirty (30) days advance written notice of an intention to terminate to CONTRACTOR.

6.) **COMPENSATION/INVOICING:** COUNTY agrees to pay CONTRACTOR and

CONTRACTOR agrees to receive compensation as follows: $2,248,062.98 for the initial five (5) year term, and $1,036,450.11 for the five-year renewal term, for a total of $3,284,513.09 for the entire potential ten (10) year term. CONTRACTOR shall submit monthly invoices referencing the provided contract number, either electronically or via mail, in triplicate to the County of Fresno, Internal Services Department, ATTN: Business Office, 333 W. Pontiac Way, Clovis, CA 93612, (isdbusinessoffice@fresnocountyca.gov).

Optional Additional Maintenance Service hours shall be billed at $165.00 per hour as described in Exhibit B, not to exceed two thousand (2,000) hours for the term of this Agreement for future possible service needs. These hours will only be billed if they are used and there is no minimum requirement for hours that must be used. In no event shall the cumulative cost to COUNTY for such Optional Additional Maintenance Services exceed $330,000.00. CONTRACTOR may provide additional products for additional fees. Pricing for additional products will be based on the prices listed in "Appendix B: Future Software Costs" of Exhibit B. In no event shall all services performed under this Agreement exceed $4,000,000.00 during the term of this Agreement. This amount limit of $4,000,000.00 includes an approximate ten percent (10%) buffer for the provision of additional products throughout the term of this Agreement. The cost summary in "Appendix C: Cost Summary" of Exhibit B contains further details on pricing. It is understood that all expenses incidental to CONTRACTOR'S performance of services under this Agreement shall be borne by CONTRACTOR. COUNTY will pay CONTRACTOR within forty-five (45) days of receipt of an approved invoice.

7.)   **SOFTWARE LICENSE TERMS**

A. General License Terms

The executable version of the Software is licensed to COUNTY on a non-exclusive basis solely for use in connection with the licensing, permitting, regulatory compliance, docket management, information requests, or other government activities that COUNTY is authorized by law to provide. The term of each Software license is stated in the Order or, if no term is stated, is one (1) year. The license may not be assigned except as part of an assignment of the Agreement as set forth herein. COUNTY may permit the use of the Software only by COUNY Users and Public Users and may not otherwise sublicense or permit the use of the Software by any other Person. Unless stated in the Product Specific Terms or the Order, the license is worldwide, subject to applicable export law. The license is subject to the following conditions and

restrictions:

        (i)   Fee Metric. COUNTY may not permit the use of the Software in excess of the applicable licensing metric, such as User "seats";

        (ii)   High Risk Use. COUNTY may not use the Software in any situation where failure or fault of the Software could lead to death or serious bodily injury of any Person or damage to tangible property or environmental damage;

        (iii) Reverse Engineering. COUNTY may not reverse engineer, disassemble, or decompile the Software or attempt to discover any underlying algorithm or method embodied by the Software except to the extent applicable law permits such activity notwithstanding this limitation, and then only on advance written notice to CONTRACTOR of at least thirty (30) days;

        (iv) Modifications. Except as expressly authorized under a separate written agreement, COUNTY may not modify the Software, combine the Software with other software, or create any derivative works of the Software;

        (v)   Competing Services. COUNTY may not use, and may not permit any Person to use, the Software for the purpose of developing a competing software program or service; and

        (vi) Performance Analysis. COUNTY may not publish any benchmarking results or other performance analysis.

        B. Product Specific License Terms

The license is subject to the following additional "Product-specific" conditions and restrictions:

(i)   Per User Fee. If the System Software is licensed on a per user basis, then COUNTY must pay a license fee for each individual who has access to the administrative features of the System Software (each a "seat"). A seat may not be used by more than one individual. A seat may be transferred from one individual user to another provided that the transfer is intended to be a permanent transfer and not a means of sharing a single seat. COUNTY must require each individual to establish a unique log in name and password. If user seats are licensed on a subscription basis for annual periods and COUNTY wishes to add seats

during an annual period, COUNTY may purchase additional user seats for a pro-rated

annual fee based on the number of partial or full months remaining in the then-current

annual period, provided that COUNTY commits to purchasing a full annual subscription for

the additional seats on the renewal of the annual period.

(ii)   Warranty Period. The warranty period for the System Software for purposes of the

Agreement is ninety (90) days beginning on the date of delivery to the COUNTY.

(iii)   Delivery. Unless otherwise expressly stated in this Agreement, CONTRACTOR shall deliver

the System Software electronically by making the System Software and enabling

information available on CONTRACTOR's Internet accessible download site. Delivery is

deemed complete as of the second (2nd) business day that CONTRACTOR has made the

System Software and enabling information available to COUNTY.

(iv)   Records and Audit. COUNTY must keep complete and accurate records showing the

location where each copy of the System Software has been installed or stored, and the

relevant information necessary to verify its compliance with the license metric (such as

users, transactions, number of servers, CPUs, etc.) and with any Support Plan

requirements. CONTRACTOR may audit COUNTY's records and facilities provided that:

(i) it gives reasonable advance notice of the audit and conducts the audit without undue

interference in COUNTY's operations; (ii) it conducts an audit no more than once per 12

months unless it discovers non-compliance, in which case it may conduct an audit as often

as once per 3 months until there have been no findings of non-compliance for a period of 12

months. In the alternative, CONTRACTOR may require COUNTY to conduct a self-audit on

reasonable terms and provide an attestation of COUNTY's officer or like official reporting the

results. If CONTRACTOR requests a self-audit, COUNTY shall complete the audit and

return the results and attestation within 30 days of CONTRACTOR's request.

8.)   SOFTWARE WARRANTY

A.   PRODUCT WARRANTY AND REMEDIES:

For the applicable warranty period, subject to the conditions and exclusions described below in this

Section 8, CONTRACTOR warrants that: (i) the general release version of Software will substantially

conform to the applicable Documentation; and (ii) the media on which the Software is provided will be free

from material defects. The applicable warranty period is stated on the Product-specific license. As

COUNTY's sole and exclusive remedies, and CONTRACTOR's sole and exclusive obligations, for a breach

of the warranty stated in this Section 8, CONTRACTOR will repair or replace the non-conforming element

of the Software or re-deliver the Software on non-defective media, as applicable, provided that if repair or

replacement is not commercially feasible then CONTRACTOR may terminate the applicable Order and

related licenses and refund any license fees paid by COUNTY.

B. Conditions and Exclusions

As a condition to the warranty remedy under Section 8(A), COUNTY must give notice of the

warranty breach during the warranty period or within thirty (30) days after the end of the warranty period

and must cooperate with CONTRACTOR's reasonable requests for information and assistance, including

information necessary to reproduce the defect. The warranty does not apply to the extent a failure is due to:

(i) COUNTY's failure to comply with the installation, operation, environmental, and other requirements or

specifications stated in the Order or the Documentation; (ii) fire, flood, or other casualty; (iii) any non-

standard configuration or implementation of the Software implemented by COUNTY or implemented by

CONTRACTOR at COUNTY's request; or (iv) the interoperation between the general release version of the

Software and any custom modules, non-standard extensions, or Unsupported technology element. In

addition, the warranty does not apply if the failure is due to the interoperation between the Software and

any Third-Party Technology unless otherwise expressly agreed in the Order.

9.) **SUPPORT, SUPPORT WARRANTY**

A. Software Support

CONTRACTOR will provide Support in accordance with its Support Terms.

B. Software Support Warranty.

CONTRACTOR warrants that it will provide Support in a professional manner using personnel who

have appropriate education, experience, and skill. COUNTY's exclusive remedy for CONTRACTOR's

failure to meet its Support warranty stated in this Section 9(B) is to require CONTRACTOR to correct or

re-perform the deficient Support, or, if CONTRACTOR fails to correct or re-perform the deficient Support,

to terminate the Support Plan and receive a refund of any unused pre-paid Support fees. In addition, if

CONTRACTOR's failure to meet the Support warranty materially impairs the use of the Software or results in a material security vulnerability, COUNTY may terminate the Product license covered by the Support Plan and receive a refund of any prepaid, unused license fees (which for a perpetual license shall be based on an assumed five (5) year license life) as well as any prepaid, unused fees for related hosting services if the Software Product is a Hosted Software Service. To be eligible for a refund of fees described in this Subsection COUNTY must: (i) give CONTRACTOR reasonably prompt notice describing the warranty breach in reasonable detail; (ii) cooperate with any requests for information and cooperation by CONTRACTOR to diagnose the issue, including any effort to reproduce a Software failure; and (iii) give CONTRACTOR a reasonable period of at least thirty (30) days to correct or re-perform the deficient Support.

C. Infrastructure Elements of Hosted Software Service

If CONTRACTOR provides Hosted Software Services, then in addition to the Software Support described above, CONTRACTOR will provide technical assistance for the infrastructure services element of the Product as described in the Product-specific license. CONTRACTOR does not provide any warranty or service level commitment in connection with the infrastructure elements of the Hosted Software Services but will make reasonable efforts to pass through any warranty or service level commitments made by the infrastructure services provider as further described on Product-specific license.

D. Other Services

Unless otherwise expressly stated in the applicable Order, CONTRACTOR is not obligated to provide any technical assistance, maintenance, or other services for software delivered pursuant to an Order for Professional Services. If CONTRACTOR provides any services it is not required to provide, the services are provided AS IS and AS AVAILABLE, with no representation or warranty whatsoever.

10.) **UNSUPPORTED SOFTWARE AND SERVICES:** If COUNTY asks CONTRACTOR to provide a non-standard configuration or implementation of Software or Services, CONTRACTOR may refuse, or may designate the non-standard Software or Services as "non-standard", "reasonable endeavors," "unsupported," "best efforts," or with like designation in the Order, support ticket or other agreement or correspondence (collectively "Unsupported" Software or Services). Unsupported Software

and Services are not covered by warranties, service level agreements, security commitments, maintenance or support commitments, or indemnities, and may not be used to process or store Personal Data. If COUNTY requests assistance with Unsupported Software or Services, CONTRACTOR will provide good faith technical assistance using its available personnel who have generalized skill and training in information technology systems. Otherwise Unsupported Software or Services are provided AS IS and AS AVAILABLE with no representation or warranty whatsoever. CONTRACTOR is not responsible to COUNTY for any loss or damage arising from the provision of Unsupported Software or Services.

11.)   **INTELLECTUAL PROPERTY (IP), TRADEMARK, AND COPYRIGHT:**

CONTRACTOR retains ownership of the System Software, any portions or copies thereof, and all rights therein. CONTRACTOR reserves all rights not expressly granted to COUNTY. This License does not grant COUNTY any rights in connection with any trademarks or service marks of CONTRACTOR, its suppliers or licensors. All right, title, interest and copyrights in and to the System Software and the accompanying System Software Documentation and any copies of the System Software are owned by CONTRACTOR, its suppliers or licensors. All title and intellectual property rights in and to the content which may be accessed through use of the System Software are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This License grants COUNTY no rights to use such content.

A. COUNTY IP

COUNTY retains all right, title, and interest in and to the COUNTY Information and all related intellectual property rights, including the content of reports and other output generated by COUNTY by using the Software or the Services, and any modifications to the COUNTY Information that result from the use of the Software or Services. CONTRACTOR may use COUNTY Information solely for the purpose of providing Services in accordance with the Agreement.

B. CONTRACTOR IP

Except for any deliverables expressly identified in an Order for Professional Services as "Customer-Owned Deliverables," CONTRACTOR retains all right, title, and interest in and to its Software and Services technology, and any and all information and processes used to deliver or provide the Software or the Services, whether existing prior to the date of the Agreement, or conceived, discovered, developed,

-22-

authored, reduced to practice, or otherwise created as part of providing the Software or Services.

C. Feedback

COUNTY hereby licenses to CONTRACTOR any feedback or suggestions that it provides regarding the Software, Services or CONTRACTOR's other existing or proposed products or services on a perpetual, irrevocable, royalty free, worldwide, unconditional, fully sublicensable and transferable basis, including the right to make, have made, use, sell, offer to sell, import, copy, display, perform, modify, distribute in modified or unmodified form, and commercialize any intellectual property, without accounting to COUNTY. COUNTY agrees that it will not assert, or authorize, assist, or encourage any third-party to assert, against COUNTY or any of its affiliates, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding the Software, Services, or any other products or services that COUNTY uses.

D. General Reservation of Rights

Except for the rights and licenses expressly granted in the Agreement, each party retains all right, title, and interest in and to its information and technology and all related intellectual property rights. The parties agree that no license may arise by estoppel or course of conduct.

12.) **INDEPENDENT CONTRACTOR:** In performance of the work, duties and obligations assumed by CONTRACTOR under this Agreement, it is mutually understood and agreed that CONTRACTOR, including any and all of the CONTRACTOR'S officers, agents, and employees will at all times be acting and performing as an independent contractor, and shall act in an independent capacity and not as an officer, agent, servant, employee, joint venturer, partner, or associate of the COUNTY. Furthermore, COUNTY shall have no right to control or supervise or direct the manner or method by which CONTRACTOR shall perform its work and function. However, COUNTY shall retain the right to administer this Agreement so as to verify that CONTRACTOR is performing its obligations in accordance with the terms and conditions thereof.

CONTRACTOR and COUNTY shall comply with all applicable provisions of law and the rules and regulations, if any, of governmental authorities having jurisdiction over matters the subject thereof.

Because of its status as an independent contractor, CONTRACTOR shall have absolutely no right to employment rights and benefits available to COUNTY employees. CONTRACTOR shall be solely liable

and responsible for providing to, or on behalf of, its employees all legally-required employee benefits. In addition, CONTRACTOR shall be solely responsible and save COUNTY harmless from all matters relating to payment of CONTRACTOR'S employees, including compliance with Social Security withholding and all other regulations governing such matters. It is acknowledged that during the term of this Agreement, CONTRACTOR may be providing services to others unrelated to the COUNTY or to this Agreement.

13.) **CONFIDENTIALITY:** A Party receiving Information (defined below) of the other will not disclose such Information other than to persons in its organization who have a need to know and who will be required to comply with this Section. The Party receiving Information will not use such Information for a purpose inconsistent with the terms of this Agreement. "Information" means the Software, Documentation and all information and intellectual property related thereto (including, but not limited to all databases provided to COUNTY by CONTRACTOR whether created by CONTRACTOR or its third-party licensors such as, without limitation, the mapping product databases) as well as information related to the business of CONTRACTOR or COUNTY. Information will not include: (i) information publicly known prior to disclosure; (ii) information coming into the lawful possession of the recipient without any confidentiality obligation; and (iii) information required to be disclosed pursuant to regulatory action or court order, provided adequate prior written notice of any request to disclose is given to the Party whose information is to be disclosed. Each Party will exercise at least the same degree of care to safeguard the confidentiality of the other's Information as it does to safeguard its own proprietary confidential information, but not less than a reasonable degree of care.

14.) **MODIFICATION:** Any matters of this Agreement may be modified from time to time by the written consent of all the parties without, in any way, affecting the remainder.

15.) **NON-ASSIGNMENT:** With the exception of Vision33, an IT professional services consultancy that CONTRACTOR uses for comprehensive end-to-end implementation services, neither party shall assign, transfer or sub-contract this Agreement nor their rights or duties under this Agreement without the prior written consent of the other party, which consent shall not be unreasonably withheld.

16.) **HOLD HARMLESS:** Except with respect to IP Claims (as defined below), in respect of which CONTRACTOR'S exclusive obligations are set forth in the immediately following paragraph, CONTRACTOR agrees to indemnify, save, hold harmless, and at COUNTY'S request, defend the

COUNTY, its officers, agents, and employees from any and all costs and expenses (including costs and fees of litigation), damages, liabilities, claims, and losses occurring or resulting to COUNTY in connection with the performance, or failure to perform, by CONTRACTOR, its officers, agents, or employees under this Agreement, and from any and all costs and expenses (including costs and fees of litigation), damages, liabilities, claims, and losses occurring or resulting to any person, firm, or corporation who may be injured or damaged by the performance, or failure to perform, of CONTRACTOR, its officers, agents, or employees under this Agreement.

In the event of a claim of alleged infringement of patent rights, copyright, trade secret rights, or intellectual property rights by an unaffiliated third party with respect to the software or services provided by CONTRACTOR under this Agreement (an "IP Claim"), CONTRACTOR shall pay any resulting judgment that is finally awarded to the third party by a court or other tribunal of competent jurisdiction, including any award of attorney fees and court costs. Notwithstanding the foregoing, CONTRACTOR has no obligation with respect to an IP Claim that is based on COUNTY's unauthorized combination of such software or services with third-party technology or its own technology, COUNTYs unauthorized change to the software or services, CONTRACTOR's compliance with COUNTY's specific directives that are not standard for COUNTY, or COUNTY's use of the software or services more than a reasonable period of time after CONTRACTOR has provided an updated version that is functionally equivalent but free from the IP Claim (the "Exclusions"). If an IP Claim is asserted, or if CONTRACTOR reasonably believes that an IP Claim is likely to be asserted, then CONTRACTOR may do either of the following at its expense: (i) obtain the right to use the software or services free from the claimed infringement; or (ii) modify the software or service so that they are no longer subject to the claimed infringement. If CONTRACTOR is not able to do either on commercially reasonable terms, then CONTRACTOR may terminate the license for the software or the order for the services, as applicable, that is the subject of the IP Claim on ninety (90) days advance written notice.

Payments by CONTRACTOR to COUNTY in respect of CONTRACTOR'S indemnification obligations set forth herein are limited to the amount of liability or damage that remains to COUNTY after deducting any insurance proceeds received by COUNTY in respect of CONTRACTOR'S insurance policies described herein.

The provisions of this Section 16 shall survive the termination of this Agreement.

17.) **INSURANCE:** Without limiting the COUNTY's right to obtain indemnification from CONTRACTOR or any third parties, but subject to the provisions of Section 16, CONTRACTOR, at its sole expense, shall maintain in full force and effect, the following insurance policies or a program of self-insurance, including but not limited to, an insurance pooling arrangement or Joint Powers Agreement (JPA) throughout the term of the Agreement:

A. Commercial General Liability

Commercial General Liability Insurance with limits of not less than Two Million Dollars ($2,000,000) per occurrence and an annual aggregate of Four Million Dollars ($4,000,000). This policy shall be issued on a per occurrence basis.

B. Automobile Liability

Comprehensive Automobile Liability Insurance with limits for bodily injury of not less than One Million Dollars ($1,000,000.00) per accident for bodily injury and for property damages. Coverage should include any auto used in connection with this Agreement.

C. Technology Professional Liability (Errors and Omissions)

Technology Professional Liability (Errors and Omissions) Insurance appropriate to CONTRACTOR's profession, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CONTRACTOR in this Agreement and may include, but not be limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy may provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

D. Cyber Liability

CONTRACTOR shall obtain cyber liability insurance with limits not less than Two Million Dollars ($2,000,000) per claim. CONTRACTOR's cyber liability insurance will cover claims involving Cyber Risks ONLY TO THE EXTENT SET FORTH IN SUCH POLICY, as included in Exhibit C.

Definition of Cyber Risks. "Cyber Risks" include but are not limited to (i) security breaches, which may include disclosure of personal information to an unauthorized third-party; (ii) breach of any of the CONTRACTOR's obligations under Section 2 of this Agreement; (iii) infringement of intellectual property including, but not limited to infringement of copyright, trademark, and trade dress; (iv) invasion of privacy, including release of private information; (v) information theft; (vi) damage to or destruction or alteration of electronic information; (vii) extortion related to the CONTRACTOR's obligations under this Agreement regarding electronic information, including personal information; (viii) network security; (ix) data breach response costs, including security breach response costs; (x) regulatory fines and penalties related to the CONTRACTOR's obligations under this Agreement regarding electronic information, including personal information; and (xi) credit monitoring expenses.

E. Claims Made Policies

If any of the required policies provide claims-made coverage:

> (i) The Retroactive Date must be shown, and must be before the date of the contract or the beginning of contract work.
>
> *(ii)* Insurance must be maintained and evidence of insurance must be provided *for at least five (5) years after completion of the contract of work.*
>
> (iii) If coverage is cancelled or non-renewed, and not replaced *with another claims-made policy form with a Retroactive Date prior to* the contract effective date, the CONTRACTOR must purchase "extended reporting" coverage for a minimum of five (5) years after completion of work.

F. Worker's Compensation

A policy of Worker's Compensation insurance as may be required by the California Labor Code.

Additional Requirements Relating to Insurance

CONTRACTOR shall obtain a broad form endorsement to the insurance policies required under this

Agreement.

CONTRACTOR hereby waives its right to recover from COUNTY, its officers, agents, and employees any amounts paid by the policy of worker's compensation insurance required by this Agreement. CONTRACTOR is solely responsible to obtain any endorsement to such policy that may be necessary to accomplish such waiver of subrogation, but CONTRACTOR's waiver of subrogation under this paragraph is effective whether or not CONTRACTOR obtains such an endorsement.

Within Thirty (30) days from the date CONTRACTOR signs and executes this Agreement, CONTRACTOR shall provide a certificate of insurance and endorsement with respect to the insurance policies required under this Agreement as stated above to the County of Fresno, Internal Services Department, ATTN: Business Office, 333 W. Pontiac Way, Clovis, CA 93612.

In the event CONTRACTOR fails to keep in effect at all times insurance coverage as herein provided, the COUNTY may, in addition to other remedies it may have, suspend or terminate this Agreement upon the occurrence of such event.

All policies shall be issued by companies possessing a current A.M. Best, Inc. rating of A FSC VII or better.

18.)   **AUDITS AND INSPECTIONS:** The CONTRACTOR shall at any time during business hours, and as often as the COUNTY may deem necessary, make available to the COUNTY for examination all of its records and data with respect to the matters covered by this Agreement. The CONTRACTOR shall, upon request by the COUNTY, permit the COUNTY to audit and inspect all of such records and data necessary to ensure CONTRACTOR'S compliance with the terms of this Agreement.

If this Agreement exceeds ten thousand dollars ($10,000.00), CONTRACTOR shall be subject to the examination and audit of the California State Auditor for a period of three (3) years after final payment under contract (Government Code Section 8546.7).

19.)   **NOTICES:** The persons and their addresses having authority to give and receive notices under this Agreement include the following:

COUNTY	CONTRACTOR
COUNTY OF FRESNO	CSDC Inc.
Internal Services Director/Chief	Attn: Legal Department
Information Officer	
333 W. Pontiac Way	804 Las Cimas Pkwy, Suite 100
Clovis, CA 93612	Austin, Texas 78746

All notices between the COUNTY and CONTRACTOR provided for or permitted under this Agreement must be in writing and delivered either by personal service, by first-class United States mail, by an overnight commercial courier service, or by telephonic facsimile transmission. A notice delivered by personal service is effective upon service to the recipient. A notice delivered by first-class United States mail is effective three COUNTY business days after deposit in the United States mail, postage prepaid, addressed to the recipient. A notice delivered by an overnight commercial courier service is effective one COUNTY business day after deposit with the overnight commercial courier service, delivery fees prepaid, with delivery instructions given for next day delivery, addressed to the recipient. A notice delivered by telephonic facsimile is effective when transmission to the recipient is completed (but, if such transmission is completed outside of COUNTY business hours, then such delivery shall be deemed to be effective at the next beginning of a COUNTY business day), provided that the sender maintains a machine record of the completed transmission. For all claims arising out of or related to this Agreement, nothing in this section establishes, waives, or modifies any claims presentation requirements or procedures provided by law, including but not limited to the Government Claims Act (Division 3.6 of Title 1 of the Government Code, beginning with section 810).

20.) **GOVERNING LAW:** Venue for any action arising out of or related to this Agreement shall only be in Fresno County, California.

The rights and obligations of the parties and all interpretation and performance of this Agreement shall be governed in all respects by the laws of the State of California.

21.) **DISCLOSURE OF SELF-DEALING TRANSACTIONS:** This provision is only applicable if the CONTRACTOR is operating as a corporation (a for-profit or non-profit corporation) or if during the term of the agreement, the CONTRACTOR changes its status to operate as a corporation.

Members of the CONTRACTOR's Board of Directors shall disclose any self-dealing transactions that they are a party to while CONTRACTOR is providing goods or performing services under this

agreement. A self-dealing transaction shall mean a transaction to which the CONTRACTOR is a party and in which one or more of its directors has a material financial interest. Members of the Board of Directors shall disclose any self-dealing transactions that they are a party to by completing and signing a Self-Dealing Transaction Disclosure Form, attached hereto as Exhibit A and incorporated herein by reference, and submitting it to the COUNTY prior to commencing with the self-dealing transaction or immediately thereafter.

   22.) **<u>ENTIRE AGREEMENT</u>:** This Agreement constitutes the entire agreement between CONTRACTOR and COUNTY with respect to the subject matter hereof and supersedes all previous Agreement negotiations, proposals, commitments, writings, advertisements, publications, and understanding of any nature whatsoever unless expressly included in this Agreement. Furthermore, this Agreement specifically supersedes and replaces Agreement No. 14-069, dated February 25, 2014, and amended on January 26, 2016.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first hereinabove written.

CONTRACTOR

(signature)

(Authorized Signature)
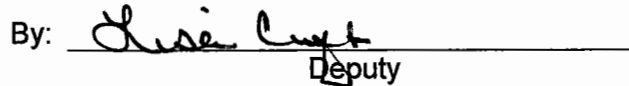
John B. Hanby, III & SVP Sales
CSDC Inc.

804 Las Cimas Pkwy, Suite 100
Austin, TX 78746
Mailing Address

COUNTY OF FRESNO

(signature)

Sal Quintero, Chairperson of the Board of
Supervisors of the County of Fresno

ATTEST:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: _(signature)_
Deputy

FOR ACCOUNTING USE ONLY:

ORG No.: 8905
Account No.: 7311
Requisition No.: 8905190378

-31-

EXHIBIT A

SELF-DEALING TRANSACTION DISCLOSURE FORM

In order to conduct business with the County of Fresno (hereinafter referred to as "County"), members of a contractor's board of directors (hereinafter referred to as "County Contractor"), must disclose any self-dealing transactions that they are a party to while providing goods, performing services, or both for the County. A self-dealing transaction is defined below:

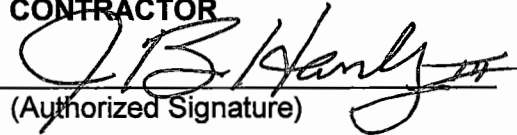*"A self-dealing transaction means a transaction to which the corporation is a party and in which one or more of its directors has a material financial interest"*

The definition above will be utilized for purposes of completing this disclosure form.

<u>INSTRUCTIONS</u>

(1)   Enter board member's name, job title (if applicable), and date this disclosure is being made.

(2)   Enter the board member's company/agency name and address.

(3)   Describe in detail the nature of the self-dealing transaction that is being disclosed to the County. At a minimum, include a description of the following:

        a.   The name of the agency/company with which the corporation has the transaction; and

        b.   The nature of the material financial interest in the Corporation's transaction that the board member has.

(4)   Describe in detail why the self-dealing transaction is appropriate based on applicable provisions of the Corporations Code.

(5)   Form must be signed by the board member that is involved in the self-dealing transaction described in Sections (3) and (4).

(1) Company Board Member Information:		
Name:		Date:
Job Title:		

(2) Company/Agency Name and Address:

(3) Disclosure (Please describe the nature of the self-dealing transaction you are a party to):

(4) Explain why this self-dealing transaction is consistent with the requirements of Corporations Code 5233 (a):

(5) Authorized Signature

Signature:		Date:	

1 **EXHIBIT B**

2 **STATEMENT OF WORK**

3 (See attached)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Statement of Work

Public Works A7 Upgrade &
Public Health Implementation

Prepared by CSDC Inc. for:

County of Fresno

CSDC Inc.
804 Las Cimas Parkway, Suite 100,
Austin, TX 78746
Prepared By:

Chris Westervelt
Director, Business Development
1-888-661-1933 x276
c.westervelt@csdcsystems.com

CSDC
ENTERPRISE SOLUTIONS

LICENSING
GRANTS
COURTS & JUSTICE
PERMITTING & COMPLIANCE
FREEDOM OF INFORMATION

Table of Contents

1   Definitions

This section identifies key terms used throughout this Statement of Work

Table 1: Terms and Definitions Used within SOW

Term	Definition
	None defined

2   Introduction

The following document will serve as a Statement of Work between CSDC ("CSDC") and the County of Fresno to work on the Amanda Implementation for the Public Works and Public Health Departments.

The purpose of the first Project is to complete the Upgrade of the current A6 AMANDA environment at the County of Fresno for the Department of Public Works to AMANDA 7, implement a new Amanda Public Portal and implement Amanda Inspector App.

The purpose of the second Project is to implement the Department of Public Health – Environmental Health for a Data Management System in response to RFP #18-011.

Total 10-year Contract Value Table

Work Package	Fixed Price Cost	Comments
Public Works Software and Maintenance	$ 761,527.16	Detail summary in Section 3
Public Health Software and Maintenance	$1,661,985.93	Detail summary in Section 3
Total Services Cost	$1,191,000.00	Detail summary in Section 7
Totals	**$3,614,513.09**	

3   Software Summary

As a commitment to the County of Fresno in providing a County-wide contract and combining the Public Works and Public Health projects. CSDC has given credits/discounts of $134,710.00 (20%) when compared to the two projects being purchased separately.

Separate Model	Initial Cost
Public Health Software	$ 512,218.00
Public Works Software	$ 152,180.00
TOTAL	$ 664,398.00
GRAND TOTAL	

Combined Model w/discounts	
	Initial Cost
Combined Software	$ 529,688.00
TOTAL	$ 529,688.00
GRAND TOTAL	
DISCOUNT DOLLARS	$ 134,710.00
DISCOUNT PERCENTAGE	20%

Software will be delivered to the Client FTP and invoiced upon contract signature. Year 1 Maintenance charges will be prorated to the County's current schedule as necessary.

3.1   Fresno County Public Health

Description	Unit Price	Quantity	Total	Year 1 Maintenance
Concurrent users - first 15	$ 4,500.00	15	$ 67,500.00	$ 13,500.00
Concurrent users - next 40	$ 3,625.00	40	$ 145,000.00	$ 29,000.00
License - Business	$ 12,000.00	1	$ 12,000.00	$ 2,400.00
RFS	$ 15,000.00	1	$ 15,000.00	$ 3,000.00
Enhanced Inspection (Deficiency)	$ 12,000.00	1	$ 12,000.00	$ 2,400.00
Multiple Merge Documents	$ 12,000.00	1	$ 12,000.00	$ 2,400.00
EDMS Adapter (general)	$ 15,000.00	1	$ 15,000.00	$ 3,000.00
Mobile Inspection Server	$ 16,000.00	1	$ 16,000.00	$ 3,200.00
Enterprise Authentication Adaptor	$ 5,500.00	1	$ 5,500.00	$ 1,100.00
Webservices Toolkit	$ 50,000.00	1	$ 50,000.00	$ 10,000.00
Batch Scheduler	$ 15,000.00	1	$ 15,000.00	$ 3,000.00
AMANDA Analytics Server	$ 7,500.00	1	$ 7,500.00	$ 1,500.00
Amanda Public Portal**	$ 13,800.00	1	$ 0	$ 13,800.00
52 Amanda Inspector App Users- first 5	$ 1,600.00	5	$ 8,000.00	$ 1,600.00
52 Amanda Inspector App Users - next 15	$ 1,472.00	15	$ 22,080.00	$ 4,416.00
52 Amanda Inspector App Users - next 25	$ 1,344.00	25	$ 33,600.00	$ 6,720.00
52 Amanda Inspector App Users - next 7	$ 1,216.00	7	$ 21,888.00	$ 4,377.60

Time and Activity Tracking	$ 12,000.00	1	$ 12,000.00	$ 2,400.00
Total			**$ 456,692.00**	**$ 105,138.40**
			Year 2 Maint.	$108,292.55
			Year 3 Maint.	$111,541.33
			Year 4 Maint.	$114,887.57
			Year 5 Maint.	$118,334.20
			Year 6 Maint.	$121,884.22
			Year 7 Maint.	$125,540.75
			Year 8 Maint.	$129,306.97
			Year 9 Maint.	$133,186.18
			Year 10 Maint.	$137,181.76
		10 YR Software and Maintenance Totals		**$1,661,985.93**

**The Amanda Public Portal Module is sold as a subscription rather than perpetual software. For this reason, the maintenance cost is the same as year 1 cost rather than 20% maintenance. Subscription software and maintenance on perpetual software are subject to a 3% per year increase and will be pro-rated with the Client's existing maintenance cycle.

3.2   Fresno County Public Works

Description	Unit Price	Quantity	Total	Year 1 Maintenance
20 Inspector App Users	$ 1,216.00	20	$ 24,320.00	$ 4,864.00
Mobile Inspection Server	No cost	1	No cost	No cost
Analytics Maintenance**	$ 1,700.00	1	$ 0	$ 1,700.00
Trust Account	$ 12,000.00		$ 12,000.00	$ 2,400.00
Amanda Public Portal**	$ 7,800.00	1	$ 0	$ 7,800.00
Web Services Toolkit	No cost	1	No cost	No cost
Existing Amanda Module maintenance Concurrent User Licenses - 35 Row Level Security and Audit – 35 Amanda Cashier Amanda Permit Scan Station Amanda iMap Public Portal				$ 46,496.19
TOTAL			**$ 36,320.00**	**$ 63,260.19**
			Year 2 Maint.	$ 65,157.99
			Year 3 Maint.	$ 67,112.73

				Year 4 Maint.	$ 69,126.12
				Year 5 Maint.	$ 71,199.90
				Year 6 Maint.	$ 73,335.90
				Year 7 Maint.	$ 75,535.97
				Year 8 Maint.	$ 77,802.05
				Year 9 Maint.	$ 80,136.11
				Year 10 Maint.	$ 82,540.20
			10 YR Software and Maintenance Totals		**$ 761,527.16**

**The Amanda Public Portal Module is sold as a subscription rather than perpetual software. For this reason, the maintenance cost is the same as year 1 cost rather than 20% maintenance. Subscription software and maintenance on perpetual software are subject to a 3% per year increase and will be pro-rated with the Client's existing maintenance cycle.

Services costs are in Section 7 and correspond to the Work Packages and Deliverables described in Sections 4 and 5

4   AMANDA 7 Upgrade, Public Portal and Inspector App – Public Works - Work Packages and Deliverables

This section describes the specific Work Packages and Deliverables that will be provided to County and the associated tasks that will be completed by the end of the engagement described in this Statement of Work.

The project will take on 3 major components: A7 upgrade and adhoc services, Amanda Citizen Access Portal implementation, and Amanda Inspector App implementation.

Deliverables will be considered "complete" when all the Acceptance Criteria set forth in this Statement of Work, or mutually agreed to subsequently in writing have been met, or the prescribed review period for each Deliverable or task has expired without written response from County.

Key Deliverables will require a Certificate of Acceptance (CoA) form signed by the County. These are denoted with a "(CoA Form required)" annotation in the detailed Deliverables list in each subsection of this Statement of Work. A sample form is shown in Appendix A: Sample Certificate of Acceptance Document.

The task/Deliverable numbers are referred to in subsequent sections throughout this Statement of Work.

Table 2: Summary of Work Packages and High-Level Deliverables

Work Package Number	Work Package	High Level Deliverable(s) / Milestones
4.1	A7 Upgrade	1. Services as needed 2. KMC Amanda User Training Course 3. KMC Amanda Admin Bridge A6 to A7 Training Course
4.2	Public Portal Deliverables	4. Microsoft Project Schedule 5. Portal Mapping Worksheets 6. Portal Installation 7. Configure Portal for Test 8. Portal Training 9. Final Configured Portal for Deployment 10. Go Live 11. Post Go Live Support
4.3	Inspector App Deliverables	12. Inspector App Requirements Worksheet 13. Configured Inspector App for Test 14. Final Configured Inspector App for Deployment 15. Inspector App Training 16. Go Live 17. Post Go Live support

A7 Upgrade and Ad hoc Services

4.1 Upgrade Activities and hours

The County of Fresno is undertaking an upgrade from the current Amanda 6 with Oracle database to Amanda 7 with SQL Server database. Most tasks will be completed by County staff. Assistance can be provided by CSDC through Vision33 as delivery partner as needed. Below is a list of activities that the County may need assistance with:

4.1.1 A7 Upgrade Services

- Deliverable Description: Service hours to be used at Fresno County's discretion.
- Assumptions and Constraints:
  - None
- Acceptance Criteria:
  - Monthly summary of hours consumed

4.1.2 KMC Amanda User Training Course

- Deliverable Description: Formal CSDC Training course and hard copy training material for each attendee
- Assumptions and Constraints:
  - One (1) day training course
  - Onsite delivery
  - CSDC Training Instructor will deliver the course
  - Four (4) – Ten (10) attendees per training session
  - Attendees will include staff that will be
    - Performing User Acceptance Testing
    - Providing long term internal support to the system
- Acceptance Criteria:
  - Completion of Training Course

4.1.3 KMC Amanda Bridge A6 to A7 Administration Training Course

- Deliverable Description: Formal CSDC Training course and hard copy training material for each attendee
- Assumptions and Constraints:
  - Two (2) day training course
  - Onsite delivery
  - Training Instructor will deliver the course
  - Four (4)
  - Attendees will include staff that will be

- Performing User Acceptance Testing
- Providing long term internal support to the system
- Acceptance Criteria:
  - Completion of Training Course

Amanda Citizen Access Portal

4.2 Public Portal Deliverables

4.2.1 Microsoft Project schedule

- Deliverable Description: Mutually agreed upon draft Project schedule to commence the Project
- Assumptions and Constraints: With resource requirements and task completion schedule that addresses all Project tasks and Deliverables
- Acceptance Criteria: County Project Manager Acceptance of Schedule

4.2.2 Portal Mapping Worksheets

Deliverable Description: Word or Excel document describing for each Portal screen, which Folder fields are presented and exchange data elements.

Assumptions and Constraints:
- Portal will include scope for the following
  - Home Page or Landing Page
  - Page Master
    - Default master page for all subsequent pages
  - Public Search Page
    - Search for [Folder] by property address
    - Search for [Folder] by permit/license information
    - View [Folder] search results in table or on map (Google map)
    - View [Folder] details
      - Folder Details (i.e. folder)
      - Property Details (if applicable)
      - Application Details (i.e. Folder Info's)
  - User Registration (2-step verification) Page
  - Registered User Login page
  - User Profile Management Page
  - Password Reset Page
  - User Dashboard
    - View data & status of all permits, licenses and other applications/folder types
      - Folder Details (i.e. folder)
      - Property Details (if applicable)
      - Application Details (i.e. Folder Info's)
      - Attachments

- o Certifications
- o Process list with Status
- o Application Fee
- o Schedule Inspections
- Edit data of all permits, licenses and other applications
- Schedule & manage inspections requests
- Download approved permits or license
- Submit New Applications
- Submit/renew an application (Folder)
- o Application Wizard & Anchors for (client-authored) Help/Guiding Text
- o Property Search
- o Application Detail (i.e. Folder info's)
- o Upload attachments (multiple file, drag & drop)
- o Pay application fees
- Save and withdraw applications
- Payment interface

Acceptance Criteria:
- o (DA form required): Client Business SME and PM signed acceptance of the Portal Mapping Worksheets

4.2.3 Portal Installation

- Deliverable Description: Installation assistance on up to three environments
- Assumptions and Constraints: Resources will need proper access to infrastructure to complete tasks
- Acceptance Criteria: County verification of installed software.

4.2.4 Configured Portal(s) for Test

Deliverable Description: Portal module configured in Client's Test Environment
Assumptions and Constraints:
- o Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:
- o Pre-Test configured Portal(s) released to Client Test Environment, and Client notified about release

4.2.5 Portal Training

Deliverable Description: Knowledge transfer and training on the Citizen Access Module for administrators
Assumptions and Constraints:
- o None
Acceptance Criteria:
- o Completed Training session

4.2.6   Final Configured Portal for Deployment

- Deliverable Description: Configured Portal(s) with corrected defects arising from UAT
- Assumptions and Constraints:
    o   Within UAT environment prior to Production deployment
- Acceptance Criteria:
    o   (DA form required): Client Business SME and Project Manager signoff

4.2.7   Go Live

- Deliverable Description: Client begins using the system in Production with live data.
- Assumptions and Constraints:
    o   Go Live may not be immediately after Production Deployment
    o   Usage of the system with live production data constitutes Go Live even if formal notification has not been provided.
- Acceptance Criteria:
    o   Client notification of Go-Live or Client usage of the system for live Production data.

4.2.8   Post Go Live Support

- Deliverable Description: CSDC support to address issues arising in the first week of usage in Production.
- Assumptions and Constraints:
    o   Limited timeframe: one (1) calendar weeks after Go-Live to raise issues
    o   CSDC resolves issues before considering the deliverable closed.
    o   After completion of Post Go Live support deliverable, any new issues are handled under either Warranty or Production Support as appropriate to the issue.
- Acceptance Criteria:
    o   Completion of one (1) calendar week period
    o   Closure of incidents raised during first calendar week of operation

Amanda Inspector App

4.3   Inspector App Deliverables

The AMANDA Inspector App is a cross-platform (iOS, Android, Window 10), store-and-forward app that allows inspectors in the fields to complete scheduled and unscheduled inspections.

This section describes the specific Work Packages and Deliverables that CSDC will provide to County and the associated tasks that CSDC will complete by the end of the engagement described in this Statement of Work. Deliverables will be considered "complete" when all the Acceptance Criteria set forth in this Statement of Work, or mutually agreed to subsequently in writing have been met, or the prescribed review period for each Deliverable or task has expired without written response from County.

Key Deliverables will require a Certificate of Acceptance (CoA) form signed by the County. These are denoted with a "(CoA Form required)" annotation in the detailed Deliverables list in each subsection of this Statement of Work. A sample form is shown in Appendix A: Sample Certificate of Acceptance Document.

County Responsibilities: The County is expected to provide the following:

- County SMEs participate in Needs Analysis session(s)
- Sign-off on the requirements analysis documentation
- Leading User Acceptance Testing

4.3.1   Inspector App Requirements Worksheets

- Deliverable Description: Word or Excel document defining the inspection folders, processes to be exchanged through the Inspector application, any mobile specific reports if applicable, and user groups that will utilize Inspector App.
- Assumptions and Constraints:
  o   None
- Acceptance Criteria:
  o   (CoA form required): County Business SME and PM signed Acceptance of the Inspector App Requirements Worksheets

4.3.2   Configured Inspector App for Test

- Deliverable Description: Inspector App module configured in County's Test Environment, and Inspector App Software install on Inspector's remote units for Soft Launch program.
- Assumptions and Constraints:
  o   Five (5) inspectors (maximum) will participate in the Soft Launch program / Inspector App UAT
- Acceptance Criteria:
  o   Pre-Test Inspector App module released to County Test Environment, and County notified about release
  o   Inspector App Software installed on Soft Launch program Inspector's remote units

4.3.3   Final Configured Inspector App for Deployment

- Deliverable Description: Inspector App with corrected defects arising from UAT
- Assumptions and Constraints:
  o   Within UAT environment prior to Production deployment
- Acceptance Criteria:
  o   (CoA form required): County Business SME and Project Manager signoff

4.3.4   Inspector App Training

Deliverable Description: Knowledge transfer and training on the Inspector for administrators and End
     user training for the app
Assumptions and Constraints:
   o   None
Acceptance Criteria:
   o   Completed Training session

4.3.5   Go Live

- Deliverable Description: County begins Using the System in Production with live data.
- Assumptions and Constraints:
   o   Go Live may not be immediately after Production Deployment
   o   Use of the System with live production data constitutes Go Live even if formal notification has
        not been provided.
- Acceptance Criteria:
   o   County notification of Go-Live or County Use of the System for live Production data.

4.3.6   Post Go Live Support

- Deliverable Description: CSDC support to address issues arising in the first two weeks of Use in
  Production.
- Assumptions and Constraints:
   o   Limited timeframe: one (1) calendar week after Go-Live to raise issues
   o   CSDC resolves issues before considering the Deliverable closed.
   o   After completion of Post Go Live support Deliverable, any new issues are handled under
        Production Support as appropriate to the issue.

- Acceptance Criteria:
   o   Completion of one (1) calendar week period
   o   Closure of incidents raised during first week of operation

5   Department of Public Health - Work Packages and Deliverables

This section describes the specific Work Packages and Deliverables that CSDC will provide to Client and
the associated tasks that CSDC will complete by the end of the engagement described in this Statement of
Work. Deliverables will be considered "complete" when all the acceptance criteria set forth in this Statement
of Work, or mutually agreed to subsequently in writing have been met, or the prescribed review period for
each deliverable or task has expired without written response from Client.

Key deliverables will require a Deliverable Acceptance (DA) form signed by the Client. These are denoted with a "(DA Form required)" annotation in the detailed deliverables list in each subsection of this Statement of Work. A sample form is shown in Appendix A: Sample Deliverable Acceptance Document.

The task/deliverable numbers are referred to in subsequent sections throughout this Statement of Work.

Table 2: Summary of Work Packages and High Level Deliverables

Work Package Number	Work Package	High Level Deliverable(s) / Milestones
5.1	Prepare	1. Project Kickoff Session and Slides 2. Microsoft Project schedule
5.2	Scope Verification & Prototype	3. Solution Design Document (SDD) 4. Requirements Traceability Matrix 5. Amanda Folder Prototype
5.3	Needs Analysis	6. Folder(s) Specification Report's (FSRs) 7. Report(s) Output Mapping Worksheets 8. Merge Document Mapping Worksheets 9. Batch Mapping Worksheets 10. Interface Mapping Worksheets 11. Data Conversion Mapping Worksheets 12. Inspector App Mapping Worksheets 13. Portal Mapping Worksheets 14. Updated Traceability Matrix
5.4	Configuration	15. Configured Folders for Test 16. Configured Output Reports for Test 17. Configured Merge Documents for Test 18. Configured Batch Jobs for Test 19. Configured Interfaces for Test 20. Configured Data Conversion for Test 21. Configured Inspector App for Test 22. Configured Portal for Test

Work Package Number	Work Package	High Level Deliverable(s) / Milestones
5.5	Train and Test	23. KMC Amanda User Training Course
		24. KMC Amanda Administration Training Course
		25. Configuration Based Train the Trainer Knowledge Transfer
		26. Final Configured Folders for Deployment
		27. Final Configured Output Reports for Deployment
		28. Final Configured Merge Documents for Test
		29. Final Configured Batch Jobs for Deployment
		30. Final Configured Interfaces for Deployment
		31. Final Configured Data Conversion for Deployment
		32. Final Configured Inspector App for Deployment
		33. Final Configured Portal for Deployment
5.6	Go Live and Closure	34. Production Deployment Package and Instructions
		35. Deployed Essential Configuration Elements
		36. Go Live
		37. Post Go Live Support
5.7	Project Management	38. Services as per section 9.2
5.8	Travel for Program Activities	39. As defined in section 5.8

5.1   Prepare

The Preparation Phase is designed to set the foundation for the subsequent phases. This phase includes detailed project planning, Client resource planning, project management and hardware and software infrastructure preparation and installation. Initial kick–off meetings are held during this phase to officially begin the project and present the project schedule and objectives to all interested parties.

Planning involves a SOW review and confirmation of Scoping Document template after Project Kickoff.

CSDC and Client PMs will jointly publishing the baseline Project schedule based on the contents of the RFP, Contract and Statement of Work

The Client prepares their environment(s) for software installation, and CSDC delivers the required software modules and licenses to the Client.

CSDC conducts pre-analysis tasks, which include collecting documentation of current business processes based on a CSDC provided checklist of information for Client to gather; and viewing a demo of the Clients existing system.

The Client develops a Business Requirements Document (BRD) containing the necessary details sufficient for CSDC to define a solution either in their own format, or based on a template provided by CSDC.

Client Responsibilities: The Client is expected to provide the following:

    Preparation of environment and infrastructure in preparation for software install
    Documentation of existing business processes
    Delivery to CSDC of a Business Requirements Document (BRD)
    Demonstration of the existing system(s) to CSDC staff

 Detailed Milestone Deliverables: CSDC will deliver the following:

5.1.1   Project Kickoff Session

Deliverable Description: Project Kickoff meeting completed, and slide package delivered
Assumptions and Constraints:
   o   Kickoff may be in conjunction with the Scope Verification workshop to facilitate a single session
   o   Kickoff / Slides include project scope, goals and expectations, risks, PM process, high level schedule
Acceptance Criteria: Completion of Kickoff Session and delivery of slide package

5.1.2   Microsoft Project schedule

Deliverable Description: Mutually agreed upon draft project schedule to commence the project

Assumptions and Constraints: With resource requirements and task completion schedule that addresses all project tasks and deliverables

Acceptance Criteria: Client Project Manager Acceptance of Schedule

5.2   Scope Verification & Prototype

The Scope Verification & Prototype phase establishes the initial "to-be" AMANDA Folders that will be fully elaborated in subsequent phases, and confirms e list of output documents, interfaces/integrations, conversion sources, mobile needs and portal services are.

During this phase, CSDC conducts a Scope Verification session that is a high level review of AMANDA Folder Types with Client business Subject Matter Experts (SMEs). As part of this review the list of Folder Types and their relationships with each other are confirmed which become the basis of detailed Needs Analysis that occurs in later phases.

The prototype Folder Types are reviewed with key stakeholders to ensure they accurately represent (at a high-level) to-be Folder Types. The functional understanding conveyed during the prototype walkthrough is documented within the project's Solution Design Document (SDD) for Client review and reference throughout the project. The SDD provides the customer with general architecture, high-level module walkthrough guides, and listings of the high-level folder types, outputs, interfaces, data conversion sources, and/or the portal and mobile scope.

Using information gathered from Pre-Analysis documents, and the Scope Verification sessions Prototype Folder Types may be modified further in preparation for more detailed requirements definition at the subsequent Needs Analysis step.

Client Responsibilities: The Client is expected to provide the following:

    List and sample of reports to generated from the system
    List of interfaces to be built with available documentation
    List of source system for data conversion
    Client SME(s) work with CSDC Solution Architect and Business Analyst to decide on the Folder Type list

5.2.1   Solution Design Document (SDD)

Deliverable Description: Word Document with contents as defined below

Assumptions and Constraints:

- Listing and high-level definition of Folder Types to be developed. Below is a list of all program actives listed in the RFP. These will be grouped into 5 Amanda Folder types with Sub Types.
  - Body Art
  - Consumer Food
  - Milk and Dairy
  - Recreational Health
  - Institutional Health
  - Hazardous Materials/Certified Unified Program Agency (CUPA)
  - Solid Waste
  - Liquid Waste
  - Waste Tire Enforcement
  - Land Use
  - Water Wells
  - Water System
  - Noise
  - Rabies Control
  - Vector Control
  - Substandard Housing
  - Solid Waste
  - Lead Hazard Remediation and Surveillance

- List of 20 merge documents and 30 reports
- High level listing of portal scope
- High level listing of Inspector App scope
- High level listing of the Interface scope
- High level listing of the data conversion scope

Acceptance Criteria:
- (DA form required): Client Business SME and PM signoff of the SDD Document

5.2.2   Requirements Traceability Matrix

Deliverable Description: Word or Excel document
- Cross reference table between Client Business Requirements Document (BRD) and Solution Design Document (SDD) elements

Assumptions and Constraints:
- Initial references to SDD document only
- Subsequent deliverables will update content to FSR and other Requirements doc deliverables

Acceptance Criteria:
- (DA form required): Signoff of Requirements Traceability

5.2.3   Amanda Folder Prototype

Deliverable Description: Prototype Amanda Folders ready for Needs Analysis, and associated Folders List

Assumptions and Constraints:

- o The Prototype Folder may be in the Client's Development environment or a zedIT Sandbox if the Development environment has not yet been prepared
- o Folder list is an export from Prototype and includes all Folders that are to be developed as defined in the Client's BDR and CSDC SDD documents.

Acceptance Criteria:
- o (DA form required): Signoff of Folder List

5.3 Needs Analysis

In this phase business requirements are analyzed including detailed analysis of Folders, Reports, Batches, Interfaces/Integrations, Portal, Mobile and Data Conversion requirements.

CSDC conducts Product Orientation Training to familiarize SMEs and other Client staff with AMANDA interface and terminology using the prototype Folder Types. CSDC leads "business fit" workshops, demonstrating and using the prototype Folder Types as a baseline. Detailed Folder Type business and configuration requirements (data validation rules, workflow business rules, fee calculations, etc.) are captured in the AMANDA Administration Console to form the basis of the Folder Specification Report (FSR), which is generated from AMANDA.

FSR's are approved by the Client, after which Folder configuration can begin. Needs Analysis of the remaining elements may continue in parallel with Folder Configuration based on the project schedule as agreed by the CSDC and Client PMs. Requirements of remaining elements may drive minor changes to the Folder requirements to ensure completeness, and efficient interoperation of elements. These include:

Output Documents including Folder related outputs, merge documents, system-wide reports and batch reports.
Batch Routines for system automation
AMANDA Public Portal online services
Amanda Inspector App

The product of this phase is also an updated version of the Prototype Folder Types, enhanced with setup data and all setup requirements documented in the FSRs, documenting the final design of each Folder Type.

Client Responsibilities: The Client is expected to provide the following:

Client SMEs participate in Product Orientation session
Client SMEs participate in Needs Analysis session(s)
Sign-off on the Folder Type design documented in FSRs
Client SMEs will produce samples of output documents and reports needed, either copies of existing reports, or mock ups of planned reports.
Signoff on Analysis/Requirements documents for Output Reports, Batch Routine, and Portal.

Detailed Milestone Deliverables: CSDC will deliver the following:

5.3.1   Folder(s) Specification Report (FSR)

Deliverable Description: Word document generated from export of AMANDA Folder requirement and configuration details

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o   5 folder types

  - ▪   Facility Folder – main facility record

  - ▪   Program Folder (2) – each permit that a facility has associated with it. We will have two separate types of these to be able to group the records logically.

  - ▪   Complaints

Acceptance Criteria:

- o   (DA form required): Client Business SME and PM signed acceptance of the FSR Report

5.3.2   Report(s) Output Mapping Worksheets

Deliverable Description: Word or Excel document capturing which configured fields that will be used in each output report.

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o   30 reports are in scope

Acceptance Criteria:

- o   (DA form required): Client Business SME and PM signed acceptance of the Report Output Mapping worksheet.

5.3.3   Merge Document Mapping Worksheets

Deliverable Description: Word or Excel document capturing which configured fields that will be used in each Word merge document.

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o   20 merge documents are in scope

Acceptance Criteria:

- o   (DA form required): Client Business SME and PM signed acceptance of the Report Output Mapping worksheet.

5.3.4   Batch Routine Worksheets

Deliverable Description: Word or Excel document describing all automatic batch routines required, their functionality, and any automated modifications to data elements

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o   Up to 10 batch jobs

Acceptance Criteria:

- o   (DA form required): Client Business SME and PM signed acceptance of the Batch Mapping Worksheets

5.3.5   Interface Mapping Worksheets

Deliverable Description: Word or Excel document describing all interfaces required, their functionality, and any automated modifications to data elements

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o   2 interfaces
    - ▪   CERS – Tiers 1-5 for electronic data transfer (EDT) with CERS
    - ▪   Laserfiche – Amanda will be able to push attachments and documents as well as meta data to Laserfiche for storage. When a user then opens an attachment or document in Amanda the interface will open the document with Laserfiche API.

Acceptance Criteria:

- o   (DA form required): Client Business SME and PM signed acceptance of the Batch Mapping Worksheets

5.3.6   Data Conversion Mapping Worksheets

Deliverable Description: Word or Excel document describing all data conversion required, their functionality, and any automated modifications to data elements

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o   1 data conversion source – Envision Connect

Acceptance Criteria:

- o   (DA form required): Client Business SME and PM signed acceptance of the Batch Mapping Worksheets

5.3.7   Inspector App Mapping Worksheets

Deliverable Description: Word or Excel document describing all data conversion required, their functionality, and any automated modifications to data elements

Assumptions and Constraints:

- o   Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.

Acceptance Criteria:

- o (DA form required): Client Business SME and PM signed acceptance of the Inspector App Mapping Worksheets

5.3.8 Portal Mapping Worksheets

<u>Deliverable Description</u>: Word or Excel document describing for each Portal screen, which Folder fields are presented and exchange data elements.

<u>Assumptions and Constraints</u>:
- o Requirements are backwards traceable to Clients BRD, and CSDC's System Design Document (SDD) from the Scope Verification phase.
- o Portal will include scope for the following… We need to discuss what we will be sending customers to the State CERS portal for and what is in scope for the Amanda Portal.
  - Home Page or Landing Page
  - Page Master
    - Default master page for all subsequent pages
  - Public Search Page
    - Search for [Folder] by property address
    - Search for [Folder] by permit/license information
    - View [Folder] search results in table or on map (Google map)
    - View [Folder] details
      - o Folder Details (i.e. folder)
      - o Property Details (if applicable)
      - o Application Details (i.e. Folder Info's)
  - User Registration (2-step verification) Page
  - Registered User Login page
  - User Profile Management Page
  - Password Reset Page
  - User Dashboard
    - View data & status of all permits, licenses and other applications
      - o Folder Details (i.e. folder)
      - o Property Details (if applicable)
      - o Application Details (i.e. Folder Info's)
      - o Attachments
      - o Certifications
      - o Process list with Status
      - o Application Fee
      - o Schedule Inspections
    - Edit data of all permits, licenses and other applications
    - Schedule & manage inspections requests
    - Download approved permits or license
  - Submit New Applications
    - Submit/renew an application (Folder)
      - o Application Wizard & Anchors for (client-authored) Help/Guiding Text
      - o Property Search
      - o Application Detail (i.e. Folder info's)
      - o Upload attachments (multiple file, drag & drop)
      - o Pay application fees
  - Save and withdraw applications
  - Payment interface

Acceptance Criteria:
- o (DA form required): Client Business SME and PM signed acceptance of the Portal Mapping Worksheets

5.3.9   Updated Traceable Matrix

<u>Deliverable Description</u>: Updated version of original Word or Excel document spreadsheet
<u>Assumptions and Constraints</u>:
- o Updated to show the traceability from Client BRD, and CSDC SDD, to
  - FSR report version and any specific requirements
  - Reports Output mapping worksheet version and any specific requirement
  - Batch Routine Worksheet version and any specific requirement
  - Portal Mapping Worksheet version and any specific requirement
  - Mobile Requirements version and any specific requirement
  - Data Conversion Mapping worksheet version and any specific requirement

<u>Acceptance Criteria</u>:
- o (DA form required): Client Business SME and PM signed acceptance of the Traceability Matrix

5.4   Configuration

Configuration and unit testing of the AMANDA system is executed during the Configuration phase. The new system is ready for User Acceptance Testing (UAT) at the end of this phase.

CSDC configures and updates the Folder Types to reflect business rules and requirements finalized in the FSRs. CSDC also develops Output Documents, Batch Routines, Custom Interfaces, and Portal views that interact with the Folders.

Upon completion of each configurable component CSDC performs a QA Review on each to ensure that all requirements are met and functionality is as expected. The QA Review includes

"Unit Level Testing" for individually configured Folders and other elements against documented requirements, including boundary conditions and error handling for any data validation requirements

"Pairs Testing" for the interaction of Folders with other configured elements where appropriate (ie. Batch Routines, Reports, Interfaces, Portals, Mobile updates and synchronization)

"Systems testing" for full end to end interaction of multiple configured elements. Testing of custom interfaces to Client systems may be limited or not possible from the Development environment.

Upon completion of QA Review, the solution is moved to the Client's Testing Environment to begin User Acceptance Testing.

During the configuration phase, the Client may begin development of test cases and procedures in preparation for User Acceptance Testing (see Section 5.5 Train and Test).

Client Responsibilities: The Client is expected to provide the following:

Additional input or clarification as requested related to configuration requirements

Development of a User Acceptance Testing environment

Optionally begin development of User Acceptance Test Plans, Cases, and Procedures in alignment with approved documented requirements.

Detailed Milestone Deliverables: CSDC will deliver the following:

5.4.1   Configured Folders for Test

Deliverable Description: Configured Folders in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-test Folders released to Client Test Environment, and Client notified about release.

5.4.2   Configured Output Reports for Test

Deliverable Description: Output Reports in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test Output Reports released to Client Test Environment, and Client notified about release

5.4.3   Configured Merge Documents for Test

Deliverable Description: Merge Documents in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test Merge Documents released to Client Test Environment, and Client notified about release

5.4.4   Configured Batch Jobs for Test

Deliverable Description: Batch Job Routines in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test Batch Job Routines released to Client Test Environment, and Client notified about release

5.4.5   Configured Interfaces for Test

Deliverable Description: Interfaces in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test Interfaces released to Client Test Environment, and Client notified about release

5.4.6   Configured Data Conversion for Test

Deliverable Description: Data Conversion in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test Data Conversion released to Client Test Environment, and Client notified about release

5.4.7   Configured Inspector App for Test

Deliverable Description: Inspector App in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test Inspector App released to Client Test Environment, and Client notified about release

5.4.8   Configured Portal(s) for Test

Deliverable Description: Portal module configured in Client's Test Environment

Assumptions and Constraints:

- o   Configuration is completed as defined in the approved Analysis documentation

Acceptance Criteria:

- o   Pre-Test configured Portal(s) released to Client Test Environment, and Client notified about release

5.5   Train and Test

CSDC will provide formal Amanda Training to prepare Client's staff for User Acceptance Testing and long term support of the configuration. CSDC provides support to, and correction of defects identified during the Client's User Acceptance Testing. The Client provides End User Training to the extended business team.

Training and Knowledge Transfer

The objective of the training is to provide Client staff with product knowledge, and knowledge of the configured solution to prepare them for development and execution of a User Acceptance Test, as well as other longer term Client activities including rollout of End User training to the planned business users of the system, and long term end user support of the system.

CSDC Knowledge Management Centre (KMC) provides two (2) formal training courses: Amanda User, and Amanda Administration. The Amanda User Training course is a prepared general training course, and not specific to the Client's configuration. The training is scheduled according to the project plan developed by the Client and CSDC PM's, typically after Needs Analysis during the Build phase, prior to UAT

CSDC will also provide knowledge transfer to key Client staff on the configured AMANDA application. This occurs through Client staff participation in Scope Verification and Needs Analysis, as well as informal (non-KMC) training of the Client Staff on the "as configured" solution ("Train the Trainer"), immediately prior to User Acceptance Testing (UAT Kickoff). Train the trainer content includes

- Use of Back Office Folders, Batch Submissions, Output documents (Admin covered by KMC)
- Use of configured Portal

User Acceptance Test

Test cases are developed by the Client in this phase, in alignment with the Folder Requirements (FSRs) and other analysis/mapping Requirements documents approved in the Needs Analysis phase. Client Test Case development is considered part of the Testing task, but can be started concurrently as early as Needs Analysis and during the Configuration based on the Client's readiness, and overall schedule. Upon request, CSDC can provide a Test Case template that the Client can use. Test Cases are reviewed with the CSDC Business Analyst for potential recommendations or alignment with approved Requirements documents. The configured system is run through testing cycles, using the test cases, to execute User Acceptance Test (UAT).

User Acceptance Test Cases and Execution should address:

- Folders
- Batch jobs
- Output Reports
- Portal
- "Pairs" testing for configured elements that interact (eg. Reports with Folders)
- Full end to end Systems Testing of the configured solution

CSDC recommends that the testing and production rollout strategy be such that all configured elements are tested and approved for production deployment at the same time. Staged approval and deployment

of elements could result in previously approved and released elements requiring additional configuration changes that may be considered Out of Scope and require a Change Order to address.

As issues arise during UAT, it is the responsibility of the Client to report them via an AFIL (AMANDA Folder Issue Log) request, which supports the tracking, disposition, correction and closure of issues. AFIL walkthrough guides are available, and the process for generating an AFIL request is reviewed during UAT kickoff.

CSDC will investigate and resolve issues arising from UAT testing. Issues that are related to test cases that don't reflect the approved requirements documents may be considered new requirements and Out of Scope for the project. Any Issue that is jointly agreed to be a New Requirement will be rationalized with the Client and either dropped if not needed, or addressed through a Change Order if the program cannot move forward without the new requirement.

The Client will approve the various high level elements of the system with signed Deliverable Acceptance (DA) documents, releasing them to be deployed to Production. Additional modifications to configuration elements after deployment to Production that are not considered defects covered under the Warranty Period, will be Out of Scope for the project and will require a Change Order to address. This includes any new requirements that may arise from a staged testing and production rollout strategy.

Following Client approval of the system, the configuration elements are frozen. The Client will provide any internal business user training sessions either in the Test environment prior to deployment, or in the Production environment after deployment, prior to Go-Live.

Client Responsibilities: The Client is expected to provide the following:

- Attend CSDC Knowledge Management Centre (KMC) formal training sessions
- Attend "As Configured" Train the Trainer sessions
- Create Test Cases using FSR and other requirements documents
- Execute Test Cases
- Execute Final System Test
- Log Test Issues in Amanda Folder Issue Log (AFIL)
- Approve configured elements and full solution for deployment to Production
- Develop End User Guides
- Train all end users

Detailed Milestone Deliverables: CSDC will deliver the following:

5.5.1   KMC Amanda User Training Course

- Deliverable Description: Formal CSDC Training course and hard copy training material for each attendee
- Assumptions and Constraints:
    - One (1) day training course

- o Onsite delivery
- o CSDC Training Instructor will deliver the course
- o Four (4) – Ten (10) attendees per training session
- o Attendees will include staff that will be
    - ▪ Performing User Acceptance Testing
    - ▪ Providing long term internal support to the system
- Acceptance Criteria:
    - o Completion of Training Course

5.5.2   KMC Amanda Administration Training Course

- Deliverable Description: Formal CSDC Training course and hard copy training material for each attendee
- Assumptions and Constraints:
    - o Four (4) day training course
    - o Onsite delivery
    - o CSDC Training Instructor will deliver the course
    - o Four (4) – Ten (10) attendees per training session
    - o Attendees will include staff that will be
        - ▪ Performing User Acceptance Testing
        - ▪ Providing long term internal support to the system
- Acceptance Criteria:
    - o Completion of Training Course

5.5.3   Configuration Based "Train the Trainer" Knowledge Transfer

- Deliverable Description: Brief detail about what the deliverable is… should be 1 item
- Assumptions and Constraints:
    - o Two, One (1) day training courses. One for CP and one for CUPA/SW.
    - o Onsite delivery
    - o CSDC Business Analyst, Solution Architect, and/or Technical Consultant may provide the training as appropriate.
    - o Use of Back Office Folders, Batch Submissions, Output documents
    - o Use of configured Portal
- Acceptance Criteria:
    - o Completion of Training session

5.5.4   Final Configured Folders for Deployment

- Deliverable Description: Folders with corrected defects arising from UAT
- Assumptions and Constraints:
    - o Within UAT environment prior to Production deployment

- Acceptance Criteria:
  - (DA form required): Client Business SME and Project Manager signoff

5.5.5 Final Configured Output Reports for Deployment

- Deliverable Description: Output Reports with corrected defects arising from UAT
- Assumptions and Constraints:
  - Within UAT environment prior to Production deployment
- Acceptance Criteria:
  - (DA form required): Client Business SME and Project Manager signoff

5.5.6 Final Configured Merge Documents for Deployment

- Deliverable Description: Merge Documents with corrected defects arising from UAT
- Assumptions and Constraints:
  - Within UAT environment prior to Production deployment
- Acceptance Criteria:
  - (DA form required): Client Business SME and Project Manager signoff

5.5.7 Final Configured Batch Jobs for Deployment

- Deliverable Description: Batch Jobs with corrected defects arising from UAT
- Assumptions and Constraints:
  - Within UAT environment prior to Production deployment
- Acceptance Criteria:
  - (DA form required): Client Business SME and Project Manager signoff

5.5.8 Final Configured Interfaces for Deployment

- Deliverable Description: Interfaces with corrected defects arising from UAT
- Assumptions and Constraints:
  - Within UAT environment prior to Production deployment
- Acceptance Criteria:
  - (DA form required): Client Business SME and Project Manager signoff

5.5.9 Final Configured Data Conversion for Deployment

- Deliverable Description: Data Conversion with corrected defects arising from UAT
- Assumptions and Constraints:
  - Within UAT environment prior to Production deployment
- Acceptance Criteria:
  - (DA form required): Client Business SME and Project Manager signoff

5.5.10 Final Configured Inspector App for Deployment

- <u>Deliverable Description</u>: Inspector App with corrected defects arising from UAT
- <u>Assumptions and Constraints</u>:
  - Within UAT environment prior to Production deployment
- <u>Acceptance Criteria:</u>
  - (DA form required): Client Business SME and Project Manager signoff

5.5.11 Final Configured Portal for Deployment

- <u>Deliverable Description</u>: Configured Portal(s) with corrected defects arising from UAT
- <u>Assumptions and Constraints</u>:
  - Within UAT environment prior to Production deployment
- <u>Acceptance Criteria:</u>
  - (DA form required): Client Business SME and Project Manager signoff

5.6   Go Live and Closure

Go-Live and Closure is the last phase of the project where the system is rolled out to production after approval and signoff of User Acceptance Testing, and training of intended end users has been completed. A single rollout of all configured elements is recommended to de-risk the possibility of requiring updates to previously deployed elements in a staged rollout strategy.

The production infrastructure is verified by the Client, with support from CSDC, against Contracted specifications and Amanda platform specifications to ensure readiness for deployment. Approved elements are promoted from the Test Environment to the Production environment. Final data conversion is typically executed over a weekend or other planned updates to minimize the downtime between freezing the existing system and switching on the new Amanda system.

All steps needed to perform the appropriate deployment are provided within CSDC's Production Deployment Instructions which is developed by CSDC staff and provided (along with any necessary change control documents) to the Client for verification, mock go-live testing, and promotion to Production.

CSDC leads a mock Go-Live session where the Client is walked through and executes to the extent possible the deployment procedure. The mock Go-Live will determine any final clarifications required to the documented instructions and gain an understanding of the downtime that will be required during cutover. Depending on the extent of changes required, the deployment instructions may be updated and re-released, or simply "red line" modified for small modifications by the Client.

The Production Deployment and final conversion/migration of legacy data is performed by the Client, with CSDC support. Final checks are performed on the converted data, and the system is released for Go-Live.

The Client installs the Mobile software on the remote devices of the remaining Inspectors that were not part of the pilot program. CSDC may provide support if and as requested.

Post go-live assistance for a period of one (1) week is also included in this phase to stabilize the system.

Project closure activities and final handover of the system will mark the end of the project.

Client Responsibilities: The Client is expected to provide the following:

- Set up the production environment.
- Assist CSDC staff to perform all steps during Mock Go Live.
- Deploy configured elements to the Production environment
- Convert final Production migration data from source to intermediate tables
- Installation of Mobile software on all Inspectors remote devices

Detailed Milestone Deliverables: CSDC will deliver the following:

5.6.1 Production Deployment Package and Instructions

- Deliverable Description: Word document detailing the deployment procedures
- Assumptions and Constraints:
  - CSDC staff will not have access to Client Production environment
  - May or may not include a physical deployment package of configured elements depending on whether Client prefers to have instructions to move elements between environments, or instructions for install elements from a package (eg. Zip file)
  - Final version may be "red line" updated by the Client at mock Go-Live prior to actual deployment.
- Acceptance Criteria:
  - Client email or verbal approval of the Deployment Instructions

5.6.2 Deployed Essential Configuration Elements

- Deliverable Description: Configured Elements are deployed to Production Environment.
- Assumptions and Constraints: Includes:
  - Folders
  - Batch Jobs
  - Output Reports

- o   Portal
- o   Client performs deployment with CSDC support
- Acceptance Criteria:
    - o   Elements Deployed to Production

5.6.3   Go Live

- Deliverable Description: Client begins using the system in Production with live data.
- Assumptions and Constraints:
    - o   Go Live may not be immediately after Production Deployment
    - o   Usage of the system with live production data constitutes Go Live even if formal notification has not been provided.
- Acceptance Criteria:
    - o   Client notification of Go-Live or Client usage of the system for live Production data.

5.6.4   Post Go Live Support

- Deliverable Description: CSDC support to address issues arising in the first week of usage in Production.
- Assumptions and Constraints:
    - o   Limited timeframe: two (2) calendar weeks after Go-Live to raise issues
    - o   CSDC resolves issues before considering the deliverable closed.
    - o   After completion of Post Go Live support deliverable, any new issues are handled under either Warranty or Production Support as appropriate to the issue.
- Acceptance Criteria:
    - o   Completion of two (2) calendar week period without incident
    - o   Closure of incidents raised during first calendar week of operation

5.7   Project Management

Throughout the project, CSDC shall complete all Project Management activities as described Section 9.2 of this SOW.

5.8   Travel for Program Activities

CSDC may travel onsite for key meetings and activities related to the project (on request). Travel is initially included in the fixed price amount, based on the assumed travel indicated below to a maximum of twenty (20) trips. A Change Order and/or Amendment will be required to add funding for Travel, should additional travel be deemed necessary.

6 Out of Scope Services

The following items are outlined as out-of-scope:

- Proof of Concept activities
- Core Product Enhancement requirements or development
- Additional requirements raised after signoff of Needs Analysis Requirements documents
- New or derived requirements raised during UAT testing
- Customized Training or Training materials
- IT or Product support for non-hosted environments
- Extensive CSDC Test Plan or Test Procedures, or Test Report beyond what is described in Section 5.4 Configuration

7 Services Costs

The services are to be provided on a Fixed Price Milestone basis as defined in Tables 5.1 and 5.2: Payment Milestones. Payment milestones are based on specific deliverables of the project, and their associated acceptance criteria as defined in Work Packages and Deliverables

Change Orders may be introduced as new Fixed Price elements as mutually agreed,and identified in the Change Order documentation.

Change Orders or Amendments may not unilaterally decrease the overall value of the contract. Modifications to planned scope of work may increase, or introduce alternate activities of equable work in order to utilize the full amount of planned funding; except by mutual consent to decrease the overall contract value.

Table 4: Summary of Implementation Costs

Work Package	Fixed Price Cost	Comments
Public Works Services	$ 210,000	
Public Health Services	$ 605,000	
Travel for Public Works Activities	$ 6,000	
Travel for Public Health Activities	$40,000	
Public Works - Services Hours Contingency (1000 hrs @ $165/hr for the life of the agreement)	$165,000	

Work Package	Fixed Price Cost	Comments
Public Health - Services Hours Contingency (1000 hrs @ $165/hr for the life of the agreement)	$165,000	
Totals	**$1,191,000**	

*These hours are set aside to handle future possible services needs. They will only be billed as consumed and there is no minimum hours that must be used.

Table 5.1: Public Works Payment Milestones

Milestone	Deliverable	Fixed Price Cost	Timing
1.	4.1.1 Services as needed	$131,000	
2.	4.1.2 KMC Bridge to Amanda 7 End User training course	$8,500	Month 2
3.	4.1.3 KMC Bridge to Amanda 7 Admin training course	$6,000	Month 2
4.	4.2.1 Microsoft Project Schedule	$2,500	Month 1
5.	4.2.2 Portal Mapping Worksheets	$5,000	Month 1
6.	4.2.3 Portal Installation	$4,000	Month 1
7.	4.2.4 Configure Portal for Test	$10,000	Month 2
8.	4.2.5 Portal Training	$3,500	Month 2
9.	4.2.6 Final Configured Portal for Deployment	$5,000	Month 3
10.	4.2.7 Go Live	$5,000	Month 4
11.	4.2.8 Post Go Live Support	$2,500	Month 5
12.	4.3.1 Inspector App Requirements Worksheet	$5,000	Month 1
13.	4.3.2 Configured Inspector App for Test	$10,000	Month 2
14.	Inspector App Training	$3,000	Month 2
15.	4.3.3 Final Configured Inspector App for Deployment	$9,000	Month 3
16.	4.3.5 Go-Live	*included	Month 4

Milestone	Deliverable	Fixed Price Cost	Timing
17.	4.3.6 Post Go-Live support	*included	Month 5
18.	Travel	$6,000.00	Months 1-6
	Totals	**$216,000**	

Table 5.2: Public Health Payment Milestones

Milestone	Deliverable	Fixed Price Cost	Comments
1.	5.1.1 Project Kickoff Session	$5,000.00	Month 1
2.	5.1.2 Microsoft Project schedule	$5,000.00	Month 1
3.	5.2.1 Solution Design Document (SDD)	$25,000.00	Month 1
4.	5.2.2 Requirements Traceability Matrix	$10,000.00	Month 1
5.	5.2.3 Amanda Folder Prototype	$25,000.00	Month 2
6.	5.3.1 Folder(s) Specification Report (FSR)	$35,000.00	Month 3
7.	5.3.2 Report(s) Output Mapping Worksheets	$20,000.00	Month 2
8.	5.3.3 Merge Document Mapping Worksheets	$15,000.00	Month 2
9.	5.3.4 Batch Routine Worksheets	$7,500.00	Month 2
10.	5.3.5 Interface Mapping Worksheets	$20,000.00	Month 2
11.	5.3.6 Data Conversion Mapping Worksheets	$20,000.00	Month 3
12.	5.3.7 Inspector App Mapping Worksheets	$5,000.00	Month 3
13.	5.3.8 Portal Mapping Worksheets	$15,000.00	Month 3
14.	5.3.9 Updated Traceable Matrix	$5,000.00	Month 3
15.	5.4.1 Configured Folders for Test	$40,000.00	Month 4
16.	5.4.2 Configured Output Reports for Test	$25,000.00	Month 4
17.	5.4.3 Configured Merge Documents for Test	$15,000.00	Month 4
18.	5.4.4 Configured Batch Jobs for Test	$10,000.00	Month 4

Milestone	Deliverable	Fixed Price Cost	Comments
19.	5.4.5 Configured Interfaces Test	$30,000.00	Month 5
20.	5.4.6 Configured Data Conversion for Test	$25,000.00	Month 5
21.	5.4.7 Configured Inspector App for Test	$10,000.00	Month 5
22.	5.4.8 Configured Portal for Test	$10,000.00	Month 5
23.	5.5.1 KMC Amanda User Training Course	$8,250.00	Month 6
24.	5.5.2 KMC Amanda Administration Training Course	$12,000.00	Month 6
25.	5.5.3 Configuration Based "Train the Trainer" Knowledge Transfer	$5,000.00	Month 6
26.	5.5.4 Final Configured Folders for Deployment	$35,000.00	Month 7
27.	5.5.5 Final Configured Output Reports for Deployment	$15,000.00	Month 7
28.	5.5.6 Final Configured Merge Documents for Deployment	$10,000.00	Month 7
29.	5.5.7 Final Configured Batch Jobs for Deployment	$10,000.00	Month 7
30.	5.5.8 Final Configured Interfaces for Deployment	$20,000.00	Month 7
31.	5.5.9 Final Configured Data Conversion for Deployment	$20,000.00	Month 8
32.	5.5.10 Final Configured Inspector App for Deployment	$10,000.00	Month 8
33.	5.5.11 Final Configured Portal for Deployment	$14,250.00	Month 8
34.	5.6.1 Production Deployment Package and Instructions	$8,000.00	Month 8
35.	5.6.2 Deployed Essential Configuration Elements	$10,000.00	Month 8
36.	5.6.3 Go Live	$25,000.00	Month 9
37.	5.6.4 Post Go Live Support	$25,000.00	Month 9
38.	Travel	$40,000.00	
Totals		**$645,000**	

*Timing of the above milestones is contingent on the final project plan that will take into account resource availability for both the Fresno and Vision33 teams. Changes in scope may also impact project timeline.

8 Roles and Responsibilities

The following key roles and responsibilities are defined for this project. They are not all inclusive of the potential roles or specific responsibilities that may be necessary, but reflect the most significant ones that are required and that impact the project execution.

8.1 Client Roles and Responsibilities

Table 6: Client Roles and Responsibilities

Resource Category	Responsibility
Project Manager	• See section 9.1
Business Subject Matter Experts	• Input to all Requirements definition • Acceptance of scope and requirements documents • Direct and Participate in User Acceptance Test Plans, Procedures and execution
Infrastructure and IT SME	• Establish and maintain AMANDA environments
Database Administrator	• Input to Data Migration Requirements and data mapping • Export and data cleanup from current systems, and input to intermediate database
Interface and Extensions SME	• Input to Custom Interface Requirements definition • Acceptance of scope and requirements documents related to Custom Interfaces • Direct and Participate in Custom Interface User Acceptance Test Plans, Procedures and execution

8.2 CSDC Roles and Responsibilities

Table 7: CSDC Roles and Responsibilities

Role	Responsibility
Project Manager (PM)	• See Section 9.2
Solution Architect (SA)	• Design of overall technical solution • Leads or supports Scope Verfication and Needs Analysis • Oversite of Configuration Development • May support QA testing prior to UAT • Supports or leads configuration based "Train the Trainer" sessions • Supports or Leads Legacy Data Conversion and Migration • Supports or leads Deployment
Business Analyst (BA)	• Supports or leads Scope Verification and Needs Analysis • Prototype Folder Development • Requirements documentation • Leads Configuration Development • QA testing prior to UAT • Leads or supports configuration based "Train the Trainer" sessions\ • Supports or Leads Legacy Data Conversion and Migration • Leads or supports Deployment
Technical Consultants (TC)	• Support Prototye Folder Development • Configuration and Development as directed by BA and SA • Development of legacy data migration scripts as directed by BA, SA, and DBA • Unit level testing
Training Specialist (TR)	• Formal KMC Training sessions

9   Project Management

Project management of this engagement will be performed by both the Client and CSDC.

9.1 Client Project Manager

The Client's project manager will:

- Work closely with CSDC Project Manager to ensure successful completion of the project.
- Consult with CSDC Project Manager to develop the Project Management Schedule for CSDC's development, and Client's supporting activities of the program.
- Assist with risk identification and risk mitigation strategies.
- Develop and maintain any internal, higher level Program Schedule that may be needed for Client executives, in consultation with the Client Project Manager if so required.
- Acquire Client project team members, and other subcontracted resources if appropriate, as needed.
- Chair weekly status meetings with CSDC and project team members to receive and provide status updates.
- Drive the closure of Client actions and deliverables pursuant to the definition of business needs
- Be responsible for Deliverable Work Package Acceptance
- Coordinate Client's review of the project document and software deliverables, and obtain signoff of an approval form to signify acceptance for each deliverable.

9.2 CSDC Project Manager

CSDC Project Manager will:

- Serve as an interface between the Client Project Manager and all CSDC personnel participating in this engagement.
- Be responsible for the management and deployment of CSDC project resources, work packages, and deliverables, and drive closure of CSDC team actions as necessary
- Consult with the Client Project Manager to develop the Project Management Schedule for CSDC's development, and Client's supporting activities of the program.
- Facilitate regular communication with the Client Project Manager, including weekly status update meetings, and review the project performance against the project plan.
- Generate monthly status reports including an updated CSDC Project Management Schedule.
- May attend and participate in key project meetings and workshops including Kick-Off, EPA and PPA; Data Migration, Customizations, and Product Enhancement Requirements workshops; Iteration Reviews, and UAT
- May contribute to the delivery of work packages
- Manage time tracking and cost allocation for CSDC project resources
- Provide Timesheet Reports to support invoicing
- Review and deliver final invoices to Client

- Maintain ongoing financial tracking and summary of budget and costs incurred on the project
- Manage project budget and reporting according to the Statement of Work.
- Support key meetings as needed through logistical support, and the generation of meeting materials.
- May provide internal review of Document Deliverables prior to submission to the Client
- Manage work package deliverable acceptance
- Assist with risk identification and risk mitigation strategies.

10   Assumptions and Constraints

CSDC has made the following assumptions in the activities and estimates provided in this Statement of Work:

- Assumptions and Constraints previously identified in the detailed deliverables for each work package identified in Sections 4 and 5 Work Packages and Deliverables
- Out of Scope activities are identified in Section 6 Out of Scope Services
- Project start date and other identified project dates is dependent on contract approval and mutual resource availability
- Activities and costs presented in this Statement of Work are based on continuous execution without material interruption.
- Estimates and fees are for work performed by CSDC or their sub-CSDCs resources.
- Client resource efforts are not assumed for the purposes of deliverable costing
- Contracted procedures will be followed, including the change order procedure to manage any identified deviation in project scope, schedule, or budget
- Client has not made any direct changes to the core product operational database
- Client will not participate in Amanda development and/or configuration for the initial implementation. Subsequent Client modifications of developed solution may void warranty.

11   Client Responsibilities

In order to maintain the proposed schedule, estimates, and quality of work, CSDC and the Client agree that the Client accepts the following responsibilities:

- Client Responsibilities identified in the specific Task Descriptions of Sections 4 and 5: Work Packages and Deliverables
- Individual Roles and Responsibilities as defined in Table 6: Client Roles and Responsibilities
- The Client shall assign an internal Project Manager, to support the activities as identified in section 9.1 Client Project Manager for each Client deployment.
- Timely review of CSDC delivered documentation, with consolidated feedback received within two (2) weeks of document delivery, or sooner upon mutual agreement to achieve desired overall project schedule.
- Provide appropriate venues, logistics, and media equipment for on-site meetings,
- Ensure appropriate attendance of key Client Stakeholders at all key project meetings

- As a non-hosted solution; purchase, install and support the necessary IT hardware and infrastructure for Client Development, User Acceptance Test, and Production environments, as well as associate Business Intelligence environments.
- As a non-hosted solution; provide the appropriate and secure access rights and tools necessary for CSDC staff to remotely work in the Client's Development and UAT environments.
- Sign off on acceptance of the deliverables and confirmation to proceed prior to the release to Production. Deliverables released to Production under Client direction without formal sign off or acceptance will be considered formally accepted.

13 Appendix A: Sample Deliverable Acceptance Document

Deliverable Acceptance Request

Project Name:		Date Requested:	
Reference:		Requested Return Date:	
Requested By:		Telephone: FAX:	
Requested Of:		Telephone: FAX:	

Deliverable Name:	
Date and Version:	

Deliverable Disposition		
Accepted No Conditions O	Accepted With Conditions O	Rejected O

Comments	
Signature: (Indicating Acceptance)	
Returned On:	

Page 1 of 1

Accept Request Template.v2 June 05, 2013

14   Appendix B: Future Software Costs

Future Amanda Back Office and Amanda Inspector App Licenses in the combined Fresno County Amanda instance can be purchased at volume discount prices listed below:

Amanda Back Office Concurrent User Licenses	Per User Cost	Per User Yearly Maintenance
Any future license purchases up to a total license count of 200 County-wide	$ 3,000.00	$ 600.00
Any future license purchases with a total license count above 200 County-wide	$ 2,437.50	$ 487.50

Amanda Inspector App Named User Licenses	Per User Cost	Per User Yearly Maintenance
Any future license purchases up to a total user count of 200 County-wide	$ 1,088.00	$217.60
Any future license purchases with a total user count above 200 County-wide	$ 944.00	$188.80

15   Appendix C: Cost Summary

Year	Public Health Initial Software and Maintenance	Public Health Services	Public Works Initial Software and Maintenance	Public Works Services	Combined Per Year Sum
Year 1	$ 561,830.40	$ 661,500.00	$ 99,580.19	$ 232,500.00	$ 1,555,410.59
Year 2	$ 108,292.55	$ 16,500.00	$ 65,157.99	$ 16,500.00	$ 206,450.55
Year 3	$ 111,541.33	$ 16,500.00	$ 67,112.73	$ 16,500.00	$ 211,654.06
Year 4	$ 114,887.57	$ 16,500.00	$ 69,126.12	$ 16,500.00	$ 217,013.68
Year 5	$ 118,334.20	$ 16,500.00	$ 71,199.90	$ 16,500.00	$ 222,534.09
Total 5 Yr	$ 1,014,886.04	$ 727,500.00	$ 372,176.93	$ 298,500.00	$ 2,413,062.97
Year 6	$ 121,884.22	$ 16,500.00	$ 73,335.90	$ 16,500.00	$ 228,220.12
Year 7	$ 125,540.75	$ 16,500.00	$ 75,535.97	$ 16,500.00	$ 234,076.72
Year 8	$ 129,306.97	$ 16,500.00	$ 77,802.05	$ 16,500.00	$ 240,109.02
Year 9	$ 133,186.18	$ 16,500.00	$ 80,136.11	$ 16,500.00	$ 246,322.29
Year 10	$ 137,181.76	$ 16,500.00	$ 82,540.20	$ 16,500.00	$ 252,721.96
Total 6-10	$ 647,099.88	$ 82,500.00	$ 389,350.23	$ 82,500.00	$ 1,201,450.11
Total All 10 Yr	$ 1,661,985.93	$ 810,000.00	$ 761,527.16	$ 381,000.00	$ 3,614,513.09

EXHIBIT C

CERTAIN CONTRACTOR INSURANCE

(See attached)

CERTIFICATE OF INSURANCE   Date: November 7, 2018

The Insurer(s) hereby states that it has issued to the insured named herein a policy or policies of insurance providing the type of insurance and limits of liability set forth herein. This certificate of insurance neither affirmatively nor negatively amends, extends or alters the coverage, limits, terms or conditions of the policy it certifies.

Certificate Holder:	Named Insured:
County of Fresno, Internal Services Department Attn: Business Office, 333 W. Pontiac Way, Clovis, CA 93612	CSDC, Inc (DE Corporation), CSDC Systems Inc (BC Corporation), CSDC India Technologies Pvt Ltd., 3500 Jefferson St, Suite 303, Austin, TX 78731

COVERAGE PROVIDED ONLY FOR THE FOLLOWING SECTIONS: A B C D E F G H O P & Q

SECTION	TYPE OF POLICY	INSURER & POLICY NO.	POLICY PERIOD M / D / Y	LIMITS OF LIABILITY	
A	Commercial General Liability	Sovereign General Insurance Company Policy No. INT79848136	06/06/18 - 06/06/19	Each Occurrence	$2,000,000
B	Products and Completed Operations				
C	Cross Liability - Severability of Interests Clause			Aggregate	$2,000,000
D	Blanket Contractual Liability				
E	Occurrence Bodily Injury & Property Damage			Tenant's Legal Liability	$2,000,000
F	Personal Injury				
G	Non-Owned and Hired Automobile Liability			Non-Owned and Hired Automobile Liability	$2,000,000
H	Owners and Contractors protective				
I	Property			Office Contents	
J	Certificate Holder Loss Payee			Building	
K	• All Risks, subject to exclusions			Equipment	
L	• Replacement Cost			Stock	
M	• Stated Amount of Co-insurance			Property of Others	
N	• Other:			Tenants Improvement	
O	Excess/Umbrella Liability (Professional Liability EXCLUDED)	Sovereign General Insurance Company Policy No. INT79848136	06/06/18 - 06/06/19	Limits	$4,000,000
P	Professional Liability (Technology Errors & Omissions)	Sovereign General Insurance Company Policy No. INT79848137	06/06/18 - 06/06/19	Limits	$2,000,000
Q	County of Fresno, its officers, agents, and employees, individually and collectively, as additional insured but only with respect to General liability arising out of the operations/negligence of the Named Insured. Professional Liability to include Technology Products Errors & Omissions, Information Security and Privacy Liability for Service Provided to others.				

Should any of the above described policies be cancelled before the expiration date thereof, the issuing insurer will endeavor to mail <u>30</u> days written notice to the holder of this certificate, but failure to do so shall impose no obligation or liability of any kind upon the insurer, its agents or representatives.

Teenakohi

Authorized Representative
THOMAS I. HULL INSURANCE LIMITED
220 Bay Street, Suite 600, Toronto, ON M5J 2W4

Form #	Coverage		Deductible	Amount or Limit of Insurance
S70005.2	**Intellect Professional Liability Claims Made**			
		Per Claim :	$ 25,000	
	Aggregate Limit			$ 5,000,000
	Professional Services Liability			$ 5,000,000
		Retroactive Date: June 30, 1999 ; Per Claim :	$ 25,000	
	E-Media Liability			$ 5,000,000
		Retroactive Date: June 30, 1999 ; Per Claim :	$ 25,000	
	Network Security & Privacy Breach Liability			$ 5,000,000
		Retroactive Date: June 30, 1999 ; Per Claim :	$ 25,000	
	Privacy Breach Coverage			$ 250,000
		Per Claim :	$ 10,000	
S70005-E.1	Business Interruption Loss			$ 250,000
		Time Period per Loss (hours) :	24	
S70005-G.1	Cyber Extortion Threat			$ 250,000
		Per Credible Threat :	$ 5,000	
S70005-F.1	Digital Asset Loss			$ 250,000
		Per Loss :	$ 5,000	

SECTION I - INSURING AGREEMENTS

In consideration of the payment of the premium, in reliance upon the statements made in the "Proposal", for this insurance which are made a part thereof, the Insurer agrees to provide insurance as follows:

1. **LIABILITY COVERAGES**
   A. **Professional Services Liability**
      The Insurer will pay on behalf of the "Insured(s)" all sums which the "Insured(s)" shall become legally obligated to pay as "Damages" resulting from "Claim(s)" first made against the "Insured(s)" during the "Policy Period" alleging a:
      (a) "Technology Professional Services Wrongful Act";
      (b) "Technology Products Wrongful Act";
      (c) "Intellectual Property Wrongful Act";
      (d) "Miscellaneous Professional Services Wrongful Act"; by the Insured, to which this Insurance applies.
   B. **E-Media Liability**
      The Insurer will pay on behalf of the "Insured(s)" all sums which the "Insured(s)" shall become legally obligated to pay as "Damages" resulting from "Claim(s)" first made against the "Insured(s)" during the "Policy Period" alleging an "E-Media Wrongful Act", by the Insured, to which this Insurance applies.
   C. **Network Security And Privacy Breach Liability**
      The Insurer will pay on behalf of the "Insured(s)" all sums which the "Insured(s)" shall become legally obligated to pay as "Damages" resulting from "Claim(s)" first made against the "Insured(s)" during the "Policy Period" alleging a "Network Security Wrongful Act" or a "Privacy Breach Wrongful Act", by the Insured, to which this Insurance applies.

2. **EXPENSE COVERAGES**
   D. **Privacy Breach Expense**
      The Insurer will reimburse the "Insured(s)" for "Privacy Breach Expense" resulting from a "Privacy Breach Wrongful Act" that occurs during the "Policy Period"; provided the "Privacy Breach Expense" is incurred within one (1) year of the expiration of the "Policy Period".

3. **FIRST PARTY COVERAGES**
   E. **Business Interruption Loss**
      The Insurer will reimburse the "Insured(s)" for "Business Interruption Loss" subject to the "Waiting Period" set forth in the Declarations Page, the "Company" incurs during the Period of Restoration directly resulting from a "Network Outage" that first occurs during the "Policy Period". The "Failure Of Security" causing the "Network Outage" and the "Business Interruption Loss" must each first occur during the "Policy Period".
   F. **Digital Asset Loss**
      The Insurer will reimburse the "Insured(s)" for "Digital Asset Loss" the "Company" sustains that first occurs during the "Policy Period". The "Digital Asset Loss" must result from a "Failure Of Security" of the "Computer System" during the "Policy Period".
   G. **Cyber Extortion Threat**
      The Insurer will reimburse the "Insured(s)" for "Extortion Expense" and "Extortion Monies" resulting directly from any "Credible Threat" or series of "Credible Threats" that includes a demand for "Extortion Monies" that first occurs during the "Policy Period". "Extortion Expense" and "Extortion Monies" will not be paid without prior consultation with the Insurer and express written consent of the Insurer.

POLICY DEFINITIONS RELEVANT TO "TECH E&O" and "CYBER RISK" including but not limited to:

"Technology Professional Services Wrongful Act": actual or alleged error, omission, negligent act, breach of duty, or negligent misstatement committed by the "Insured" solely in the conduct of the "Insured's" "Technology Professional Services".

"Technology Professional Services": one or more of the following provided for others for compensation:
(a) the development, design, assembly, manufacture, sale, leasing, licensing, distribution, installation, modification, integration, servicing, supporting or repairing of computers, computer hardware, firmware and/or software, computerized networks, or similar electronic information systems or telecommunications equipment;
(b) the provision of computer systems, network related or telecommunication related consulting, analysis, programming, training or support;
(c) data processing;
(d) services provider (ASP), domain name registration services, Internet hosting services, Internet service provider (ISP services), web portal services or search engine services; or
(e) any other related computer services, but will not include "Technology Products".

"Network Security Wrongful Act": actual or alleged breach of duty, negligent, act, error or omission by the "Insured" that results in a "Failure Of Security". Any failures, interruptions, suspensions and delays of a "Company's Computer System" that results in the same or interrelated "Network Security Wrongful Act" will be considered a single "Wrongful Act", regardless of the number of such failures, interruptions, suspensions or delays or dates when such failures, interruptions, suspensions or delays happened.

"Failure Of Security:" the actual failure or inability:
(a) of the "Security" of the "Company's" "Computer System" to prevent "Unauthorized Access" or "Unauthorized Use" of the "Company's" "Computer System", receipt or transmission of a "Malicious Code" or attack of the "Company's" "Computer System"; or
(b) to prevent the physical theft of hardware or firmware controlled by a "Company" on which electronic data is stored, by a person other that an "Insured", from a premises occupied and controlled by a "Company". "Failure Of Security" will also include actual failure and inability above, resulting from the theft of a password or access code by non-electronic means in direct violation of a "Company's" specific written security policies and procedures.

"Computer System": computer hardware, software, firmware, and components thereof, including electronic data stored thereon, which are linked together through a network or two or more computers, including such networks accessible through the Internet, intranets, extranets or virtual private networks.

"Unauthorized Access": the gaining of access to a "Computer System" by an unauthorized person(s), or by an authorized person(s) in an unauthorized manner.

"Unauthorized Use": the use of "Computer Systems" by a person unauthorized by the "Insured" or a person authorized by the "Insured" that used the "Computer System" for a purpose not intended by the "Insured".

"Malicious Code": unauthorized corrupting or harmful piece of code, including, but not limited to, computer viruses, Trojan horses, worms, time or logic bombs, spy ware, malware or spider ware.

"Privacy Breach Wrongful Act": any actual or alleged breach of duty, negligent act, error or omission by the "Insured" that results in:
(a) the disclosure of "Protected Personal Information"; or
(b) breach or violation by the "Insured" of any "Privacy Law".

"Protected Personal Information": a person's first name and/or last name in combination with any one or more of the following:
(a) social insurance number or social security number;
(b) medical or healthcare information or data;
(c) drivers license number; or
(d) financial account information that would permit access to that individual's financial account.

"Privacy Law":
(a) the Personal Information Protection and Electronic Documents Act (PIPEDA); or
(b) other similar federal, provincial, state or local identity theft and privacy protection laws requiring commercial entities that collect personal information to post privacy policies, adopt specific privacy controls, or notify individuals in the event that personal information has potentially been compromised.

AXIS REINSURANCE COMPANY (CANADIAN BRANCH)
Administrative Office – 70 York Street, Suite 1010, Toronto, Ontario M5J1S9
Telephone 416.361.7200 | Fax 416.361.7225

SECUREXCESS LIABILITY – DECLARATIONS FORM SXS300A | Edition 04/13

SUBJECT TO THE PROVISIONS OF THE FOLLOWED POLICY, THIS POLICY MAY APPLY ONLY TO CLAIMS FIRST MADE OR CLAIMS FIRST MADE AND REPORTED DURING THE POLICY PERIOD OR EXTENDED REPORTING PERIOD, IF APPLICABLE, AND THE LIMIT OF LIABILITY AVAILABLE TO PAY JUDGMENTS OR SETTLEMENT AMOUNTS MAY BE REDUCED AND EXHAUSTED BY PAYMENT OF DEFENSE COSTS OR CLAIMS EXPENSES. PLEASE READ THIS POLICY CAREFULLY.

ITEM 1: INSURER:
AXIS Reinsurance Company (Canadian Branch)

ITEM 2: PRODUCER
Thomas I. Hull Insurance Limited - Toronto

ITEM 3: POLICY NUMBER:
CTN/630768/01/2018

ITEM 4: POLICYHOLDER AND ADDRESS:
CSDC Systems Inc. (BC Incorporated) and CSDC Inc. (DE) and CSDC India Technologies Pvt Ltd.
255 Longside Drive, Unit-102, Mississauga, Ontario L5W 0G7

ITEM 5: POLICY PERIOD: (Both dates as at 12:01 a.m. at the address listed in Item 4)
June 6, 2018   Inception Date
June 6, 2019   Expiration Date

ITEM 6: LIMIT OF LIABILITY:
$5,000,000   Per **Loss** Limit
$5,000,000   Annual Aggregate

ITEM 7: UNDERLYING INSURANCE:
See attached schedule of Underlying Insurance

ITEM 8: FORMS AND ENDORSEMENTS AT INCEPTION:
1. Schedule of Underlying Insurance - SXS 302A (06-12)
2. Sublimit coverage extension Endorsement - SXS 386A (06-16)
3. Prior Acts Exclusion - SXS 353A (04-13)

ITEM 9: NOTICES TO INSURER:
Notice of Claim or Circumstance:
AXIS Reinsurance Company (Canadian Branch), Office of the Chief Agent
70 York Street, Suite 1010, Toronto, Ontario   M5J1S9
Email: ClaimNoticeCAN@axiscapital.com
Facsimile: 1-866-348-8103
Phone: 1-866-518-4153
All other Notice:
AXIS Reinsurance Company (Canadian Branch), Office of the Chief Agent
70 York Street, Suite 1010, Toronto, Ontario   M5J1S9

ITEM 10: TOTAL POLICY PREMIUM:
$15,000

ITEM 11: PRODUCER COMMISSION: (Included)
Included

ITEM 12: CURRENCY: (Amounts reference in this Policy are shown in the following currency)
CAD

All other terms and conditions remain unchanged.

The Insurer has caused this Policy to be issued and signed in Toronto, Ontario and attested by its authorized officers, but it shall not be valid unless also signed by another duly authorized representative of the Insurer.

_____   July 26, 2018
Authorized Representative: Date:

AXIS REINSURANCE COMPANY (CANADIAN BRANCH)
Administrative Office – 70 York Street, Suite 1010, Toronto, Ontario M5J1S9
Telephone 416.361.7200 | Fax 416.361.7225

SECUREXCESS LIABILITY – POLICY FORM SXS301A | Edition 06/12

POLICY NUMBER: CTN/630768/01/2018

In consideration of the paid Premium and in reliance upon all information and representations provided or made available by the **Insureds** to the Insurer in connection with the underwriting of this Policy and to the insurers of the **Underlying Insurance** in connection with the underwriting of the **Underlying Insurance**, and subject to the provisions of this Policy and the Declarations and any Schedules and Endorsements attached hereto, all of which are made a part of this Policy, the Insurer and **Policyholder**, on behalf of all **Insureds**, agree as follows:

I. INSURING AGREEMENT

This Policy shall provide insurance excess of the respective **Underlying Insurance**. Liability for any covered **Loss** shall attach to the Insurer only after (i) the insurers of the **Underlying Insurance**, the **Insureds** or others on behalf of the **Insureds** shall have paid **Loss** covered under the respective **Underlying Insurance** equal to the full amount of the **Underlying Limit**, and (ii) the retention or deductible, if any, applicable under the **Underlying Insurance** has been satisfied. Except as specifically set forth herein, coverage under this Policy shall apply in conformance with all provisions of the **Followed Policy**.

II. DEFINITIONS

When used in this Policy, whether in the singular or the plural:

A.   **Insureds** means all persons and entities covered under the **Followed Policy**.

B.   **Followed Policy** means the insurance policy(ies) identified as such in the Schedule of Underlying Insurance attached hereto.

C.   **Loss** means all amounts covered under the **Underlying Insurance**.

D.   **Policy Period** means the period set forth in Item 5 of the Declarations.

E.   **Policyholder** means the person(s) or entity(ies) set forth in Item 4 of the Declarations.

F.   **Underlying Insurance** means the **Followed Policy** and all other policies, if any, identified as such in the Schedule of Underlying Insurance attached hereto.

G.   **Underlying Limit** means an amount equal to the aggregate of all limits of liability set forth in the Schedule of Underlying Insurance attached hereto.

III. CONDITIONS AND LIMITATIONS

A.   The Limit of Liability set forth in Item 6 of the Declarations shall be the maximum amount payable by the Insurer for all **Loss** in excess of the **Underlying Limit**.

B.   If any **Loss** is subject to a sublimit of liability under any **Underlying Insurance**, this Policy shall not apply to such **Loss**, but the Insurer shall recognize payment of such **Loss** in any manner described in Section I. Insuring Agreement as reducing the **Underlying Limit** by the amount of such payment.

C.   The **Insureds** shall give written notice to the Insurer if any **Underlying Insurance** is changed or terminated or if any insurer of the **Underlying Insurance** becomes financially unable to pay **Loss**. No such event shall affect coverage under this Policy, unless the Insurer so agrees in writing.

D.   Notice to the Insurer shall be given at the respective address shown in Item 9 of the Declarations. Notice to any other insurer shall not constitute notice to the Insurer unless also given to the Insurer as provided above.

E.   The Insurer may, at its sole discretion, elect to participate in the investigation, defense and settlement of any claim or other matter to which the coverage under this Policy could apply even if the **Underlying Limit** has not been exhausted. The **Insureds** shall provide the Insurer with information, assistance and cooperation as the Insurer reasonably requests and shall do nothing to prejudice the Insurer's position or potential rights of recovery. No action by any other insurer shall bind the Insurer under this Policy.

IV. GOVERNING LAW

A.   It is agreed that any interpretation of the coverage afforded by this Policy, including by reference any terms, conditions and provisions contained herein, will be governed by the laws of the province in Canada in which this Policy is issued.

B.   For the purposes of the Insurance Companies Act (Canada), this document was issued in the course of AXIS Reinsurance Company (Canadian Branch)'s insurance business in Canada.

SIGNATURE PAGE FOLLOWS.

SIGNATURE PAGE

In witness whereof, this policy has been executed and attested by the undersigned in Toronto, Canada; however, this policy will not be valid unless countersigned on the Declarations Page by one of our duly authorized representatives.

<u>Andrew M. Weissert</u>

Secretary

<u>Robert Looney</u>

President & CEO

<u>Brad Randell</u>

Chief Agent

SECUREXCESS LIABILITY

AXIS REINSURANCE COMPANY (CANADIAN BRANCH)
Administrative Office – 70 York Street, Suite 1010, Toronto, Ontario M5J1S9
Telephone 416.361.7200 | Fax 416.361.7225

SECUREXCESS LIABILITY – SCHEDULE OF UNDERLYING INSURANCE FORM SXS302A | Edition 06/12

(SINGLE TOWER)

<u>**ENDORSEMENT 1**</u>

Issued to:	CSDC Systems Inc. (BC Incorporated) and CSDC Inc. (DE) and CSDC India Technologies Pvt Ltd.
Issued by:	AXIS Reinsurance Company (Canadian Branch)
Producer:	Thomas I. Hull Insurance Limited - Toronto
Effective:	June 6, 2018

This endorsement is attached to, and forms part of Policy Number: CTN/630768/01/2018

<u>**FOLLOWED POLICY**</u>

	<u>Insurer Name:</u>	<u>Policy Number:</u>	<u>Limit of Liability:</u>
A.	The Sovereign General Insurance Company	INT79848137	$5,000,000

ALL OTHER PROVISIONS OF THIS POLICY REMAIN UNCHANGED.

_____   July 26, 2018
Authorized Representative   Date

SECUREXCESS LIABILITY – Sublimit Coverage Extension Endorsement **FORM SXS** 386A **| Edition** 06-16

ENDORSEMENT 2

Issued to:	CSDC Systems Inc. (BC Incorporated) and CSDC Inc. (DE) and CSDC India Technologies Pvt Ltd.
Issued by:	AXIS Reinsurance Company (Canadian Branch)
Producer:	Thomas I. Hull Insurance Limited - Toronto
Effective:	June 6, 2018

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement is attached to, and forms part of Policy Number: CTN/630768/01/2018

It is hereby understood and agreed that:

FOLLOW SUBLIMIT COVERAGE ENDORSEMENT

SCHEDULE

Coverage Section/Description of the **Followed Policy**	Sublimit of Liability under this Policy
Privacy Breach Coverage	$250,000 xs $250,000
Business Interruption Loss	$250,000 xs $250,000
Cyber Extortion Loss	$250,000 xs $250,000
Digital Asset Loss	$250,000 xs $250,000

The following is added to paragraph B. in the CONDITIONS AND LIMITATIONS Section:

Notwithstanding the above, liability for amounts covered under the coverage section/description of the **Followed Policy** set forth in the above schedule shall attach to the Insurer after the full amount of such sublimit has been paid in accordance with the terms of Section I. INSURING AGREEMENT, subject to a Sublimit of Liability under this Policy set forth in the above schedule, which is part of, and not in addition to, the Limit of Liability set forth in Item 6. of the Declarations.

ALL OTHER PROVISIONS OF THIS POLICY REMAIN UNCHANGED.

_____   July 26, 2018
Authorized Representative   Date

AXIS REINSURANCE COMPANY (CANADIAN BRANCH)
Administrative Office – 70 York Street, Suite 1010, Toronto, Ontario M5J1S9
Telephone 416.361.7200 | Fax 416.361.7225

SECUREXCESS LIABILITY – PRIOR ACTS EXCLUSION ENDORSEMENT FORM SXS353A | Edition 04/13

<u>**ENDORSEMENT 3**</u>

Issued to:	CSDC Systems Inc. (BC Incorporated) and CSDC Inc. (DE) and CSDC India Technologies Pvt Ltd.
Issued by:	AXIS Reinsurance Company (Canadian Branch)
Producer:	Thomas I. Hull Insurance Limited - Toronto
Effective:	June 6, 2018

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement is attached to, and forms part of Policy Number: CTN/630768/01/2018

In consideration of the premium charged, it is agreed that, the Insurer shall not be liable for **Loss** arising from any Claim made against any **Insured** based upon, arising out of, directly or indirectly resulting from, in consequence of or in any way involving any Wrongful Act actually or allegedly occurring before June 6, 2018 (hereinafter "Prior Acts") or any Wrongful Act whenever occurring, which together with any Prior Acts constitutes Interrelated Wrongful Acts.

ALL OTHER PROVISIONS OF THIS POLICY REMAIN UNCHANGED.

(signature)	July 26, 2018
Authorized Representative	Date

Sovereign

Declarations

Policy Number: INT79848137

Policy Period:
Effective Date: June 06, 2018
Expiry Date: June 06, 2019
12:01 A.M. Standard Time at the mailing address of the Named Insured as stated herein

Named Insured and Mailing Address:
CSDC Systems Inc. and CSDC Inc. and CSDC India Technologies Pvt Ltd. and CSDC Holdco Inc.
Unit 102, 255 Longside Drive
Mississauga ON
L5W 0G7

Renewal

Broker:
Ontario Non-Contracted Broker Arrangement (Central Region)
1400, One York Street
Toronto ON
M5J 0B6
Phone: (416) 365-1818

Premium for this Transaction: $ 25,643

Policy Minimum Retained Premium: $ 12,822

The policy contains a clause that may limit the amount payable.

Various provisions in this policy may restrict coverage. Please read your policy carefully to determine what is and is not covered. If you have any questions, please contact your broker.

Valid only if countersigned by an authorized representative of the Insurer.

Robert Wesseling
President and Chief Executive Officer

Countersigned _____
Authorized Representative

POLICY CANCELLATION REQUEST

In consideration of the return of unearned premium to follow (if any) and in accordance with the terms of the policy, this policy (Policy No. INT79848137) is hereby cancelled and surrendered effective 12:01 AM Standard time on _____ and the renewal policy (if any has been issued for same), acknowledged to be of no effect.

_____   _____
Signature of Authorized Representative for Named Insured   Dated

_____
Print name and title

Liability

Operations of Insured: Enterprise Platform for Governments

Form #	Coverage	Deductible	Amount or Limit of Insurance	Premium
S70005.2	**Intellect Professional Liability Claims Made**			
	Per Claim :	$ 25,000		
	Aggregate Limit		$ 5,000,000	
	Professional Services Liability		$ 5,000,000	
	Retroactive Date: June 30, 1999 ; Per Claim :	$ 25,000		
	E-Media Liability		$ 5,000,000	
	Retroactive Date: June 30, 1999 ; Per Claim :	$ 25,000		
	Network Security & Privacy Breach Liability		$ 5,000,000	
	Retroactive Date: June 30, 1999 ; Per Claim :	$ 25,000		
	Privacy Breach Coverage		$ 250,000	
	Per Claim :	$ 10,000		
S70005-E.1	Business Interruption Loss		$ 250,000	
	Time Period per Loss (hours) :	24		
S70005-G.1	Cyber Extortion Threat		$ 250,000	
	Per Credible Threat :	$ 5,000		
S70005-F.1	Digital Asset Loss		$ 250,000	
	Per Loss :	$ 5,000		
SM502.1	INTELLECT ERRORS AND OMISSIONS LIABILITY – SPECIFIED CLAIM EXCLUSION			
SM503.1	INTELLECT PROFESSIONAL LIABILITY – INCREASE IN LIMITS ENDORSEMENT			
S70315.1	Unlicensed Software Exclusion			

Policy Conditions and Endorsements

S10005.1	Short Rate Table			
S10006.2	Policy and Statutory Conditions			
S10013.1	Declaration of Emergency			

Intellect
Data Breach Services

Sovereign General Insurance Company has partnered with IDT911 to provide you with Data Breach Services that will help you prepare your business for the complexities and nuances of data security—without the expense of hiring in-house expertise. This benefit will help you:

• **Reduce the chances of a data breach in the first place**

• **Prepare for those that might occur**

• **Respond appropriately if they do**

Proactive Breach Preparation Services

As an educational resource, our proactive breach preparedness site can provide you with the tools you need to better protect your sensitive data and teach you how to respond appropriately in the event of a data breach.

• **Learning Management System -** On-demand, web-based training platform on important data breach issues such as Compliance, Data Security and Privacy

• **Notification Laws and Regulations -** Information on consumer, regulatory and third party requirements

• **Incidence Response Plan Template -** Establish procedures for handling a breach and working with IDentity Theft 911 to minimize the impact and potential fallout

• **Educational Resources -** Data protection tips, breach scenarios, articles and best practices

To access the breach preparedness site:

• Go to **www.sovereigngeneral.breachresponse.ca** and log in using the following credentials:

• Username: **Sovgen01**

• Password: **Sovgen01**

After your initial login you will be required to create your own, unique credentials for future use.

Breach Response Services

In the unfortunate event of a breach, IDentity Theft 911's experts can help you quickly develop a clear breach response strategy and incident management plan.

• **Breach Counseling -** Help determine whether a breach has occurred and assess the severity of the incident

• **Crisis Management -** Time-saving professional service in handling a breach

• **Notification Assistance -** Help in preparing notification letters that comply with regulatory requirements

• **Remediation Services -** Recommendations on remediation services for impacted individuals

• **Media Relations Consulting -** Public relations assistance to help restore your business' reputation

• **Legal Support -** Documentation of steps taken and remediation services provided

Intellect
Data Breach Services

 Sovereign

Privacy Breach Expense Coverage

These services are included as part of your Privacy Breach Expense Coverage:

- Proactive monitoring
- Data breach notification
- Third party data breach notification
- Forensic investigation
- Limited legal service
- Public relations

ABOUT IDT911

Covering more than 45 million individuals, IDT911 is North America's premier identity management and data risk management services provider.

Since 2005, the company has provided data breach services to more than 600,000 business and has helped more than 2,000 deal with actual data breaches.

WHAT IS A DATA BREACH

A data breach is a security incident in which sensitive, protected or confidential data is intentionally or unintentionally released to an un-trusted environment.

Lost data may involve personally identifiable information (PII), such as Social Security numbers, credit card or bank details, and personal health information (PHI).

WHAT BACKGROUND DOES THE BREACH RESPONSE TEAM HAVE

The breach response team has multidisciplinary backgrounds in:

- Data Security
- Computer Forensics
- Privacy Law
- Information Technology
- Business Administration

If you think you've had a data breach or have any questions, call 1.866.824.9940 today.

Powered by

 IDT 911

Manuscript wording for: SM502.1 - INTELLECT ERRORS AND OMISSIONS LIABILITY – SPECIFIED CLAIM EXCLUSION
APPLICABLE TO THE INTELLECT ERRORS AND OMISSIONS LIABILITY FORM

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

It is stated and agreed that this Policy does not apply to any "Claim(s)" based upon, arising out of or in any way related to:

City of Ottawa Claim as documented in the 2017 submission information

Except as otherwise provided in this endorsement all terms, provisions and conditions of the Policy shall have full force and effect.

Manuscript wording for: SM503.1 - INTELLECT PROFESSIONAL LIABILITY – INCREASE IN LIMITS ENDORSEMENT
It is stated and agreed that the retroactive dates are as follows:

1) Professional Services Liability for $1,000,000 excess $3,000,000 is November 26, 2011.

2) Professional Services Liability for $1,000,000 excess $4,000,000 is December 10, 2012.

3) E-Media Liability for $1,000,000 excess $3,000,000 is November 26, 2011.

4) E-Media Liability for a $5,000,000 Limit is as stated on the declarations.

5) Network Security and Privacy Breach Liability for $1,000,000 excess $3,000,000 is November 26, 2011.

6) Network Security and Privacy Breach Liability for $1,000,000 excess $4,000,000 is December 10, 2012.

Except as otherwise provided in this endorsement all terms, provisions and conditions of the Policy shall have full force and effect.

SHORT RATE TABLE

Attached to and forming part of this policy. The following Table applies when termination of the policy is requested by the Insured.

Days to Expiry	% of Premium Returned	Days to Expiry	% of Premium Returned	Days to Expiry	% of Premium Returned
365-362	92	245-243	61	126-123	30
361-358	91	242-239	60	122-120	29
357-354	90	238-235	59	119-116	28
353-350	89	234-231	58	115-112	27
349-346	88	230-227	57	111-108	26
345-342	87	226-223	56	107-104	25
341-339	86	222-219	55	103-100	24
338-335	85	218-216	54	99-97	23
334-331	84	215-212	53	96-93	22
330-327	83	211-208	52	92-89	21
326-323	82	207-204	51	88-85	20
322-319	81	203-200	50	84-81	19
318-316	80	199-196	49	80-77	18
315-312	79	195-193	48	76-73	17
311-308	78	192-189	47	72-69	16
307-304	77	188-185	46	68-66	15
303-300	76	184-181	45	65-62	14
299-296	75	180-177	44	61-58	13
295-292	74	176-173	43	57-54	12
291-289	73	172-170	42	53-50	11
288-285	72	169-166	41	49-47	10
284-281	71	165-162	40	46-43	9
280-277	70	161-158	39	42-39	8
276-273	69	157-154	38	38-35	7
272-269	68	153-150	37	34-31	6
268-266	67	149-146	36	30-27	5
265-262	66	145-143	35	26-24	4
261-258	65	142-139	34	23-20	3
257-254	64	138-135	33	19-16	2
253-250	63	134-131	32	15-12	1
249-246	62	130-127	31	11-0	0

POLICY CONDITIONS
(Applicable only to Alberta and British Columbia)

The following applies where the Insured is domiciled or where the insured property is located in Alberta or British Columbia.

LIMITATION OF ACTION
Every action or proceeding against an insurer for the recovery of insurance money payable under the contract is absolutely barred unless commenced within the time set out in the *Insurance Act.*

RECOVERY BY INNOCENT PERSONS
(1) Where this policy contains a term or condition excluding coverage for loss or damage to property caused by a criminal or intentional act or omission of an Insured or any other person, the exclusion applies only to the claim of a person:
  (a) whose act or omission caused the loss or damage,
  (b) who abetted or colluded in the act or omission,
  (c) who
    (i) consented to the act or omission, and
    (ii) knew or ought to have known that the act or omission would cause the loss or damage, or
  (d) who is in a class prescribed by regulation.
(2) Nothing in section (1) allows a person whose property is insured under the contract to recover more than their proportionate interest in the lost or damaged property.
(3) A person whose coverage under a contract would be excluded but for section (1) must comply with any requirements prescribed by regulation.
Coverage provided by this condition only applies to the extent of coverage provided under the relevant legislation set out in the applicable provincial *Insurance Act.*

STATUTORY CONDITIONS
(Applicable only to Alberta and British Columbia)

These Statutory Conditions apply where the Insured is domiciled or where the insured property is located in Alberta or British Columbia.
If any condition below or in the policy, contains a variation, omission or an addition to the Statutory Condition established by the applicable provincial statute, then the interpretation most favourable to the Insured shall prevail.

1. PROPERTY OF OTHERS
The Insurer is not liable for loss or damage to property owned by a person other than the Insured unless:
(1) otherwise specifically stated in the contract, or
(2) the interest of the Insured in that property is stated in the contract.

2. CHANGE OF INTEREST
The Insurer is liable for loss or damage occurring after an authorized assignment under the Bankruptcy and Insolvency Act (Canada) or a change of title by succession, by operation of law or by death.

3. MATERIAL CHANGE IN RISK
(1) The Insured must promptly give notice in writing to the Insurer or its agent of a change that is:
  (a) material to the risk, and
  (b) within the control and knowledge of the Insured.
(2) If an Insurer or its agent is not promptly notified of a change under subparagraph (1) of this condition, the contract is void as to the part affected by the change.
(3) If an Insurer or its agent is notified of a change under subparagraph (1) of this condition, the Insurer may:
  (a) terminate the contract in accordance with Statutory Condition 4, or
  (b) notify the Insured in writing that, if the Insured desires the contract to continue in force, the Insured must, within 15 days after receipt of the notice, pay to the Insurer an additional premium specified in the notice.
(4) If the Insured fails to pay an additional premium when required to do so under subparagraph (3) (b) of this condition, the contract is terminated at that time and Statutory Condition 4 (2) (a) applies in respect of the unearned portion of the premium.

4. TERMINATION OF INSURANCE
(1) This contract may be terminated,
  (a) by the Insurer giving to the Insured 15 days' notice of termination by registered mail or 5 days' written notice of termination personally delivered, or
  (b) by the Insured at any time on request.
(2) If the contract is terminated by the Insurer,
  (a) the Insurer must refund the excess of premium actually paid by the Insured over the prorated premium for the expired time, but in no event may the prorated premium for the expired time be less than any minimum retained premium specified in the contract, and
  (b) the refund must accompany the notice unless the premium is subject to adjustment or determination as to amount, in which case the refund must be made as soon as practicable.
(3) If the contract is terminated by the Insured, the Insurer must refund as soon as practicable the excess of premium actually paid by the Insured over the short rate premium for the expired time specified in the contract, but in no event may the short rate premium for the expired time be less than any minimum retained premium specified in the contract.
(4) The 15 day period referred to in subparagraph (1) (a) of this condition starts to run on the day the registered letter or notification of it is delivered to the Insured's postal address.

5. NOTICE

(1) Written notice to the Insurer may be delivered at, or sent by registered mail to, the chief agency or head office of the Insurer in the province.

(2) Written notice to the Insured may be personally delivered at, or sent by registered mail addressed to, the Insured's last known address as provided to the Insurer by the Insured.

N.B. To the extent that the Civil Code of the Province of Quebec is applicable to this contract General Conditions and Provisions as set out in the Civil Code of the Province of Quebec apply. These General Conditions and Provisions apply to all coverages insured by this policy, except where such conditions and provisions may be modified or supplemented by forms or endorsements attached to this policy. A copy of the General Conditions and Provisions is available on request from the Insurer.

DECLARATION OF EMERGENCY ENDORSEMENT
EXTENSION OF TERMINATION or EXPIRY DATE

This endorsement changes the policy.

The effective date of termination of this policy by the Insurer or the expiry date of this policy is extended, subject to the conditions and definitions set out below, as follows when an "emergency" is declared by a Canadian public authority designated by statute for the purpose of issuing such an order.

1. The "emergency" must have a direct effect or impact on:
   (i) the Insured, the insured site or insured property located in the declared emergency area; or
   (ii) the operations of the Insurer or its agent/broker located in the declared emergency area.

2.A. Any time limitation described in the Termination condition of this policy, with respect to termination of this policy by the Insurer, will not continue to run until the "emergency" is terminated plus the lesser of:
   (i) 30 days; or
   (ii) the number of days equal to the total time the "emergency" order was in effect.

2.B. If this policy is due to expire during an "emergency", it will continue in force until the "emergency" is terminated plus the lesser of:
   (i) 30 days; or
   (ii) the number of days equal to the total time the "emergency" order was in effect.

3. In no event shall the total term of this extension exceed 120 consecutive days.

The Insured agrees to pay the pro rata premium earned for the additional time the Insurer remains on risk as a result of the above.

"**Emergency**" means the first statutory "declaration" of an emergency:
(a) with respect to a situation or an impending situation that constitutes a danger of major proportions that could result in serious harm to persons or substantial damage to property and that is caused by the forces of nature, a disease or other health risk, an accident or an act whether intentional or otherwise; or
(b) as provided for by the relevant governing legislation if different from a),
but does not include any subsequent statutory "declaration(s)" that may be issued relating to the same event.

All other terms and conditions of the policy remain unchanged.

INTELLECT PROFESSIONAL LIABILITY - CLAIMS MADE

THIS IS A CLAIMS-MADE. Various provisions in this Policy restrict coverage. Read the entire Policy carefully to determine rights, duties and what is and is not covered. Words and phrases that appear in quotation marks have special meaning.

SECTION I - INSURING AGREEMENTS

In consideration of the payment of the premium, in reliance upon the statements made in the "Proposal", for this insurance which are made a part thereof, the Insurer agrees to provide insurance as follows:

1. **LIABILITY COVERAGES**
    A. **Professional Services Liability**
        The Insurer will pay on behalf of the "Insured(s)" all sums which the "Insured(s)" shall become legally obligated to pay as "Damages" resulting from "Claim(s)" first made against the "Insured(s)" during the "Policy Period" alleging a:
        (a) "Technology Professional Services Wrongful Act";
        (b) "Technology Products Wrongful Act";
        (c) "Intellectual Property Wrongful Act";
        (d) "Miscellaneous Professional Services Wrongful Act"; by the Insured, to which this Insurance applies.
    B. **E-Media Liability**
        The Insurer will pay on behalf of the "Insured(s)" all sums which the "Insured(s)" shall become legally obligated to pay as "Damages" resulting from "Claim(s)" first made against the "Insured(s)" during the "Policy Period" alleging an "E-Media Wrongful Act", by the Insured, to which this Insurance applies.
    C. **Network Security And Privacy Breach Liability**
        The Insurer will pay on behalf of the "Insured(s)" all sums which the "Insured(s)" shall become legally obligated to pay as "Damages" resulting from "Claim(s)" first made against the "Insured(s)" during the "Policy Period" alleging a "Network Security Wrongful Act" or a "Privacy Breach Wrongful Act", by the Insured, to which this Insurance applies.

2. **EXPENSE COVERAGES**
    D. **Privacy Breach Expense**
        The Insurer will reimburse the "Insured(s)" for "Privacy Breach Expense" resulting from a "Privacy Breach Wrongful Act" that occurs during the "Policy Period"; provided the "Privacy Breach Expense" is incurred within one (1) year of the expiration of the "Policy Period".

3. **FIRST PARTY COVERAGES**
    E. **Business Interruption Loss**
        The Insurer will reimburse the "Insured(s)" for "Business Interruption Loss" subject to the "Waiting Period" set forth in the Declarations Page, the "Company" incurs during the Period of Restoration directly resulting from a "Network Outage" that first occurs during the "Policy Period". The "Failure Of Security" causing the "Network Outage" and the "Business Interruption Loss" must each first occur during the "Policy Period".
    F. **Digital Asset Loss**
        The Insurer will reimburse the "Insured(s)" for "Digital Asset Loss" the "Company" sustains that first occurs during the "Policy Period". The "Digital Asset Loss" must result from a "Failure Of Security" of the "Computer System" during the "Policy Period".
    G. **Cyber Extortion Threat**
        The Insurer will reimburse the "Insured(s)" for "Extortion Expense" and "Extortion Monies" resulting directly from any "Credible Threat" or series of "Credible Threats" that includes a demand for "Extortion Monies" that first occurs during the "Policy Period". "Extortion Expense" and "Extortion Monies" will not be paid without prior consultation with the Insurer and express written consent of the Insurer.

4. **DEFENCE AND SETTLEMENT**
    With respect to "Claim(s)" covered under Section I, Item 1 the Insurer shall have the right and duty to:
    (a) defend any legal proceedings or arbitration proceedings against the "Insured(s)" seeking "Damages" payable under the terms of this Policy even if any of the allegations of the suit are groundless, false or fraudulent;
    (b) investigate and negotiate the settlement of any "Claim(s)" or suit as it deems expedient.

    The Insurer shall not settle any "Claim(s)" without the consent of the "Insured(s)". If, however, the "Insured(s)" shall refuse to consent to any settlement recommended by the Insurer and shall elect to contest the "Claim(s)" or continue any legal proceedings in connection with such "Claim(s)", then the Insurer's liability for the "Claim(s)" shall not exceed the amount for which the "Claim(s)" could have been so settled with the "Insured's" consent up to the date of such refusal.

5. **SUPPLEMENTARY PAYMENTS**
    With respect to "Claim(s)" covered under Section I, Item 1, the Insurer shall pay or reimburse:
    (a) all premiums on bonds to release attachments for an amount not in excess of the Limit of Liability shown in the Declarations Page;
    (b) all premiums on appeal bonds required in any defended suit, but without any obligation to apply for or furnish such bonds;
        all costs taxed against the "Insured(s)" in any civil action defended by the Insurer and any interest accruing after entry of judgment upon that part of the judgment which is within the Limit of Liability.

6. **LIMIT OF LIABILITY & DEDUCTIBLE**
    A. **Combined Aggregate Limit**
        The Policy Aggregate Limit stated in the Declarations Page is the most the Insurer will pay as "Damages" for all "Claim(s)" made against the "Insured(s)" during the "Policy Period", regardless of the number of "Insured's" or the number of claimants.

B. Liability Coverage – Limit of Liability
The Limit of Liability for each Liability Insuring Agreement stated in the Declarations Page is the most the Insurer will pay under such Insuring Agreement as "Damages" for all "Claim(s)" made against the "Insured(s)" during the "Policy Period", regardless of the number of "Insured's" or the number of Claimants. The Limit of Liability will be part of and not in addition to the Policy Aggregate Limit.

C. Expense Coverage
The sub limit of Insurance for COVERAGE D – PRIVACY BREACH EXPENSE stated in the Declarations Page is the maximum aggregate amount the Insurer will pay for such expenses. The Limit of Insurance will be part of and not in addition to the Limit of Liability for COVERAGE C – NETWORK SECURITY AND PRIVACY BREACH LIABILITY INSURANCE. The Limit of Liability will be part of and not in addition to the Policy Aggregate Limit.

D. First Party Coverage
The Limit of Insurance for each First Party Coverages stated in the Declarations Page will be the maximum aggregate amount that the Insurer will pay under such Insuring Agreements for "Damages" for all "Claim(s)" covered under such Insuring Agreement. The Limit of Insurance will be part of and not in addition to the Limit of Liability for COVERAGE C – NETWORK SECURITY AND PRIVACY BREACH LIABILITY INSURANCE. The Limit of Liability will be part of and not in addition to the Policy Aggregate Limit.

Amounts payable under Section I, Items 4 and 5, will be part of and not in addition to the Limit of Liability applicable to each "Claim(s)".

The Deductible stated in the Declarations Page will apply to "Damages" for each "Claim(s)" under Section I, Item 1,Item 2 and Item 3, and the Insurer will only be responsible in excess of this amount. The full Limit of Liability will apply over the Deductible.

The Deductible will not apply to Section I, Items 4, and 5.

One or more "Claim(s)" arising out of the same or related "Wrongful Acts" or "Interrelated Wrongful Acts" will be considered a single "Claim", first reported in the "Policy Period" in which the earliest "Claim" was reported and subject to that single Limit of Liability.

In the event a "Claim(s)" triggers more than one Deductible amount, the highest Deductible amount will be deemed the Deductible amount applicable to "Damages" from the "Claim(s)". A single Deductible will apply to all "Claim(s)" alleging the same "Wrongful Act" or "Interrelated Wrongful Acts".

7. TERRITORY & RETROACTIVE DATE
This Policy applies to "Claim(s)" arising out of "Wrongful Acts", which occur:
(a) within the "Coverage Territory" and,
(b) after the Retroactive Date shown on the Declarations Page and before the expiration of the "Policy Period"; and provided always that the "Claim(s)" is first made against the "Insured(s)" during the "Policy Period" and notice given to the Insurer in accordance with Section IV, Item 12.

8. AUTOMATIC EXTENDED REPORTING PERIOD
This Policy shall provide the "Insured(s)" an automatic extended reporting period of sixty (60) days, without additional charge, following the termination of this Policy, for the reporting of any "Claim(s)", but only with respect to any "Wrongful Act" committed after the Retroactive Date and prior to such termination date. This automatic extended sixty (60) day reporting period will not apply if the Policy is cancelled because of non-payment of the premium by the "Insured(s)" or if replacement coverage is obtained from the Insurer. It is further understood and agreed that this automatic extension shall not apply with respect to knowledge by the "Insured(s)" of any fact or circumstance which could reasonably be expected to give rise to any verbal or written demand against the "Insured(s)" for monetary damages.

9. DISCOVERY PERIOD
If the Insurer or the "Named Insured(s)" shall cancel or refuse to renew this Policy and provided that the premium has been fully paid, the "Insured(s)" shall have the right, upon payment of an additional premium, to an extension of the coverage granted by this Policy in respect of any "Claim" or "Claim(s)" which are made against the "Insured(s)" during one (1), three (3) or six (6) years after the termination of the Policy, but only with respect to a "Wrongful Act" committed after the Retroactive Date and prior to such termination date. Such period of time is hereinafter referred to as the Discovery Period. The additional premium to be charged will be determined upon request of this extension and will remain at the discretion of the Insurer, however, such additional premium shall not exceed:
(a) for a one (1) year Discovery Period, 100% of the previous annual premium;
(b) for a three (3) year Discovery Period, 150% of the previous annual premium; or
(c) for a six (6) year Discovery Period, 300% of the previous annual premium.

This right of extension shall cease unless written notice is given to the Insurer within sixty (60) days after the termination date, together with full payment of the premium for this extension. The Discovery Period will be part of the immediately preceding "Policy Period" and a single aggregate Limit of Liability will apply to such "Policy Period", including the Discovery Period.

The additional premium for the Discovery Period shall be fully earned at the inception of the Discovery Period. The Discovery Period, once effected, is not cancellable.

SECTION II - DEFINITIONS

As used in this Policy, the following words or expressions shall mean:

1. **"Advertising":** a notice that is broadcast or published to the general public or specific market segments about the "Company's" goods, products or services for the purpose of attracting customers or supporters.

2. **"Business Interruption Loss":** the sum of Actual Loss, and Extra Expense resulting directly from a "Network Outage". The "Business Interruption Loss" will be calculated based on the actual "Business Interruption Loss" the "Company" sustains per hour during the Period of Restoration. If a "Company" could reduce the Actual Loss or Extra Expense resulting from a "Network Outage" by complete or partial resumption of operations, such reductions will be taken into account in arriving at Actual Loss or Extra Expense.

Solely with respect to coverage afforded under Coverage E. Business Interruption Loss:
   (a) Actual Loss is:
      (i) Net Sales less the cost of sales expenses the "Company" would have earned or incurred had there been no "Network Outage"; and
      (ii) continuing normal operating expenses incurred by the "Company", including ordinary payroll expenses, provided such operating expenses must continue during the "Network Outage" and only to the extent that such expenses would have been incurred by the "Company" had no "Network Outage" occurred.
   (b) Extra Expense is necessary or reasonable expenses incurred by the "Company" directly as a result of a "Network Outage", but only to the extent such expense reduces Actual Loss.
   (c) Period of Restoration is the period of time that:
      (i) begins with the date and time that the "Network Outage" first occurs; and
      (ii) ends with the earliest of:
         1) the date and time that the "Network Outage" ends, or would have ended, if the "Insured" had exercised due diligence and dispatch; or
         2) 30 days after the date and time that the "Network Outage" first occurred.
   (d) "Business Interruption Loss" does not include:
      (i) contractual penalties of any nature;
      (ii) cost or expenses incurred to identify or remediate "Computer System" errors or vulnerabilities;
      (iii) cost or expenses incurred to update, restore, replace or otherwise improve any "Computer System" to the level of functionality beyond that which existed prior to the loss event;
      (iv) any other consequential loss or damage;
      (v) legal costs or legal expenses of any nature; and
      (vi) "Loss" arising out of liability to any "Third Party" for whatever reason.

3. **"Claim(s)":**
   (a) any verbal or written demand(s) for monetary or non monetary relief against the "Insured" for a "Wrongful Act";
   (b) a civil proceeding commenced by the issuance of notice of action, statement of claim, writ of summons, complaint or similar proceeding;
   (c) a formal administrative or regulatory proceeding seeking to enforce a statutory mandate requiring notification to customers or credit monitoring as a result of a "Privacy Breach Wrongful Act".

"Claim(s)" does not include criminal proceedings.

4. **"Company":**
   (a) the "Named Insured";
   (b) any entity that the "Named Insured" acquires or forms and which the "Named Insured" either owns or in which the "Named Insured" maintains a fifty-one percent (51%) or more controlling interest provided there is no other insurance available to that entity.

Coverage under this Policy will only apply if:
   (a) the "Named Insured" advised the Insurer within ninety (90) days of the acquisition or formation of such entity and provides the Insurer with reasonable information as it deems necessary to evaluate any material change to the risk; and
   (b) the "Named Insured" agrees to pay any additional premium requested by the Insurer.
   Such acquired or newly formed entity will only be entitled to coverage as a "Company" with respect to a "Claim(s)" for "Wrongful Acts", "Digital Assets Loss", "Business Interruption Loss", or "Credible Threat" occurring after the effective date of acquisition or formation.

5. **"Computer System":** computer hardware, software, firmware, and components thereof, including electronic data stored thereon, which are linked together through a network or two or more computers, including such networks accessible through the Internet, intranets, extranets or virtual private networks.

6. **"Content":** audio, visual, digital or informational material that is disseminated electronically.

7. **"Coverage Territory":** anywhere in the world.

8. **"Credible Threat":** a threat to:
   (a) release, divulge, disseminate, destroy or use a "Company's" "Digital Assets" acquired by "Unauthorized Access" or "Unauthorized Use" of the "Company's" "Computer System";
   (b) introduce "Malicious Code" into the "Company's" "Computer System";
   (c) corrupt, damage or destroy the "Company's" "Computer System";
   (d) electronically communicate with the "Company's" customers and falsely claim to represent the "Company" or acting under the "Company's" direction in order to falsely obtain "Protected Personal Information" of the "Company's" customers; or
   (e) restrict or hinder access to the "Company's" "Computer System", including the threat of criminal or malicious "Denial of Service".

Such threat shall not constitute "Credible Threat" unless prior to surrendering property or other consideration as payment by on or behalf of the "Company":
   (a) the "Company" conducts a reasonable investigation and reasonably determines that such threat is technologically credible;
   (b) the "Company" must report such "Credible Threat", at the Insurer's request, to the RCMP, FBI, CIRCC, CERT, ISAC or any other central reporting or investigative organization that the Insurer may designate.

9. **"Damages":** damages due or awarded in payment for "Claim(s)" including:
   (a) settlements, judgments, and costs awarded pursuant to judgment or appeals;
   (b) punitive or exemplary damages to the extent that such damages are insurable under the law most favourable to the insurability of such damages of any jurisdiction which has a substantial relationship to the "Insured", the Insurer, this Policy or the "Claim"; and
   (c) pre- and post – judgment interest arising from paragraphs (a) or (b) above.

   Damages shall not include:
   (i) fines or penalties (except as provided with respect to punitive or exemplary damages), taxes or the multiple portion of a multiplied damage award;
   (ii) future profits, future royalties, costs of licensing, or other costs of obtaining future use;
   (iii) restitution or disgorgement by any "Insured";
   (iv) the cost of correcting, or re-performing any services provided by the "Insured";
   (v) discounts, coupons, refunds or other incentives offered to the "Insured's" customers or clients;
   (vi) uninsurable under the law pursuant to which this Policy is construed;
   (vii) the return of fees or other compensation paid to the "Insured";
   (viii) "Defence Costs";
   (ix) "Digital Assets";
   (x) "Business Interruption Loss";
   (xi) "Extortion Expense";
   (xii) "Extortion Monies"; and
   (xiii) "Privacy Breach Expense".

10. **"Defence Costs":** legal, investigation and adjusting expenses incurred by the Insurer for the defence of a "Claim(s)" seeking "Damages" payable under this Policy including lawyer's fees and disbursements.

   Defence Costs do not include "Privacy Breach Expenses".

11. **"Denial of Service"**: an attack launched by a person or persons that sends an excessive volume of electronic data to a "Computer System" in order to deplete such "Computer System's" capacity, and prevents those who are authorized to do so from gaining access to such "Computer System" in a manner in which they are legally entitled, provided such depletion of capacity is not caused by a mistake in determining capacity needs.

12. **"Digital Assets":**
   (a) software or electronic data, customer lists and information, financial, credit card or competitive information, and confidential or private information, stored electronically on the "Insured's" "Computer System", which is subject to regular back-up procedures; or
   (b) capacity of the "Insured's" "Computer System", including without limitation, memory, bandwidth, or processor time, use of communication facilities and any other computer-connected equipment.

13. **"Digital Asset Loss":**
   (a) the actual and necessary costs incurred by the "Company" to *Restore* its "Digital Assets" that have been altered, corrupted, destroyed, disrupted, deleted or damaged;
   (b) the actual cost borne by the "Company" to Recollect such "Digital Assets" in the event the "Company" is unable to Restore such "Digital Assets", but is able to Recollect such "Digital Assets";
   (c) in the event the "Company" is not able to *Restore* or *Recollect* such "Digital Assets", the "Digital Asset Loss" will mean only the actual costs incurred by the "Company" to reach this determination.

   "Digital Asset Loss" will not mean, and coverage will not be afforded for:
   (a) loss arising out of any liability to third-parties for whatever reason;
   (b) costs and expenses incurred by the "Insured" to update, upgrade, enhance or replace the "Insured's Digital Assets";
   (c) legal costs or legal expenses;
   (d) loss arising out of any physical damage to or destruction of the computer hardware, firmware or any other property except "Digital Assets";
   (e) that part of any "Digital Asset Loss" for which the proof as to its existence or amount is solely dependent on an inventory computation or comparison; or a profit and loss computation or comparison; provided, however, where the "Insured" establishes wholly apart from such comparison that it has sustained a "Digital Asset Loss", then it may offer its inventory records and actual physical count of inventory in support of the amount of such "Digital Asset Loss" claimed;
   (f) the costs or expenses incurred for researching or developing "Digital Assets";
   (g) the economic or market value of, or the monetary value of lost market share, profits, or royalties related to any "Digital Assets", including without limitation "Trade Secrets";
   (h) costs or expenses incurred to identify and remove software program errors or vulnerabilities; or
   (i) the monetary value of any electronic fund transfers or transactions by the "Insured" or on the "Insured's" behalf, which is lost, diminished or damaged during transfer from, into or between the "Insured's" accounts.

   Recollect: cost of expenses to:
   (a) recollect the information making up the "Digital Asset", including without limitation, information from non-electronic sources; and
   (b) organize and transcribe such information into the same or substantially similar form as the original "Digital Asset".

   Restore: costs or expenses to restore "Digital Assets" from any collection of partially or fully matching electronic data or software, or through electronic data or disaster recovery methods.

14. **"E-Media Wrongful Act":** any actual or alleged negligent act, error or omission by the "Insured" that results in:
   (a) wrongful publication, defamation, slander or libel, product disparagement, trade libel or other tort related disparagement or harm to the reputation of character of any persons or "Company" in the "Company's" "Content" or in the "Company's" "Advertising"; or

(b) misappropriation or misdirection of messages or media of a "Third Party" by the Insured, including metatags, website domains and names, and related "Content".

15. **"E-Media":**
    (a) "Content"; or
    (b) the "Company's" "Content" or "Advertising" that is disseminated on the "Internet", including "Content" disseminated by other means of media transmittal by the "Company" provide that it is a duplication of "Content" already disseminated electronically on the "Company's" Website.

16. **"Employee(s)":** includes any present or former employee, including part-time, seasonal, "Leased Worker", "Temporary Worker" or an "Individual Contracted Worker", but solely while acting on behalf of the "Company".

17. **"Extortion Expense":** the reasonable expense other than "Extortion Monies" incurred by the "Insured" with the Insurer's prior written consent in response to a "Credible Threat". Such consent will not be unreasonably withheld.

18. **"Extortion Monies":** any funds or property paid by the "Insured", with the Insurer's prior written consent, to a person(s) reasonably believed to be responsible for the "Credible Threat" insured under Insuring Agreement G, for the purpose of terminating that threat and all residual effects. Such consent will not be unreasonably withheld.

19. "**Failure Of Security:**" the actual failure or inability:
    (a) of the "Security" of the "Company's" "Computer System" to prevent "Unauthorized Access" or "Unauthorized Use" of the "Company's" "Computer System", receipt or transmission of a "Malicious Code" or attack of the "Company's" "Computer System"; or
    (b) to prevent the physical theft of hardware or firmware controlled by a "Company" on which electronic data is stored, by a person other that an "Insured", from a premises occupied and controlled by a "Company". "Failure Of Security" will also include actual failure and inability above, resulting from the theft of a password or access code by non-electronic means in direct violation of a "Company's" specific written security policies and procedures.

20. **"Fissionable Substance":** any prescribed substances that is, or from which can be obtained a substance capable of releasing atomic energy by nuclear fission.

21. **"First Inception Date":** the date specified on the Declaration Page as the inception date of the first Policy issued by the Insurer that provides the same, or essential the same coverage as this Policy and is continually renewed by the Insurer.

22. "**Identity Theft**": the misappropriation of "Protected Personal Information" of customers or members that is in the "Company's" care, custody and control or stored in the "Company's" "Computer System", which has resulted in, or could reasonably be expected to result in, the wrongful or fraudulent use of such information.

23. **"Individual Contracted Worker":** an individual person hired under contract by the "Company" for a specific task, but only while acting within the scope of their duties for the "Company" and performing duties related to the conduct of the "Company" business under the "Company's" direction.

24. **"Insured(s)":**
    (a) the "Company"; and
    (b) "Insured Person".

25. **"Insured Person":**
    If the "Named Insured" is:
    (a) an individual, the "Named Insured's" spouse is also an "Insured", but only with respect to the conduct of a business of which the "Named Insured" is the sole owner;
    (b) a partnership or joint venture, its members, partners and their spouses are also "Insured(s)", but only with respect to the conduct of the "Named Insured's" partnership or joint venture business;
    (c) a business corporation, its "Employees" are also "Insured(s)" but only with respect to the conduct of the "Named Insured's" business corporation. Its officers and directors are also "Insured" but only with respect to their duties as such shareholders are also "Insured's" but only with respect to their liability as shareholders.

    Any present or past partner, executive officer, director or "Employee(s)" and, in the event of their death, incompetence, insolvency or bankruptcy, their estate or appointed legal representative, while acting within the scope of their duties as such.

26. **"Intellectual Property Wrongful Act":** actual or alleged infringement, breach, violation, wrongful use, misuse, or misappropriation of ideas under implied contract, passing off, plagiarism, piracy or dilution committed by the "Insured" of any: copyright, trade dress, trademark, trade name, service mark, service name, registered or unregistered design, slogan, title, web domain name, database, title, sound, voice, name, likeness, identity, music or other artistic or creative work, including violation of creator's moral or attribution rights, publicity rights, or ideas under implied contract incurring liability for infringement of intellectual property rights.

27. **"Internet":** the worldwide public network of computers which enables the transmission of electronic data and which includes intranets, extranets and virtual private networks.

28. **"Interrelated Wrongful Acts":** "Wrongful Acts" that have a common nexus, fact, circumstance, situation, event, transaction, goal, motive, methodology, or cause or series of causally connected facts, circumstances, situations, events, transactions, goals, motives, methodologies or causes.

29. **"Leased Worker":** a person leased to the "Named Insured(s)" by a labour leasing firm, under an agreement between the "Named Insured(s)" and the labour leasing firm, to perform duties related to the conduct of the "Named Insured's" business. "Leased worker" does not include a "Temporary Worker".

30. **"Loss":** "Damages", "Defence Costs", "Digital Asset Loss" and "Privacy Breach Expenses".

31. **"Malicious Code":** unauthorized corrupting or harmful piece of code, including, but not limited to, computer viruses, Trojan horses, worms, time or logic bombs, spy ware, malware or spider ware.

32. **"Named Insured(s)":** the person(s) or entity(ies) shown in the Declarations Page.

33. **"Network Outage":** the actual and measurable interruption or suspension of the "Insured's Computer System", which is directly caused by a "Failure Of Security".

34. **"Network Security Wrongful Act":** actual or alleged breach of duty, negligent, act, error or omission by the "Insured" that results in a "Failure Of Security". Any failures, interruptions, suspensions and delays of a "Company's Computer System" that results in the same or interrelated "Network Security Wrongful Act" will be considered a single "Wrongful Act", regardless of the number of such failures, interruptions, suspensions or delays or dates when such failures, interruptions, suspensions or delays happened.

35. **"Nuclear Energy Hazard":** the radioactive toxic, explosive or other hazardous properties of radioactive material.

36. **"Nuclear Facility":**
    (a) any apparatus designed or used to sustain nuclear fission in a self-supporting chain reaction or to contain a critical mass of plutonium, thorium and uranium or any one or more of them;
    (b) any equipment or device designed or used for:
        (i) separating the isotopes of plutonium, thorium and uranium or any one or more of them;
        (ii) processing or utilizing spent fuel; or
        (iii) handling, processing or packaging waste;
    (c) any equipment or device used for the processing, fabricating or alloying of plutonium, thorium or uranium enriched in the isotope uranium 233 or in the isotope uranium 235, or any one or more of them if at any time the total amount of such material in the custody of the "Insured(s)" at the premises where such equipment or device is located consists of or contains more than 25 grams of plutonium or uranium 233 or any combination thereof, or more than 250 grams of uranium 235;
    (d) any structure, basin, excavation, premises or place prepared or used for the storage or disposal of waste radioactive material and includes the site on which any of the foregoing is located, together with all operations conducted thereon and all premises used for such operations.

37. **"Miscellaneous Professional Services Wrongful Act":** actual or alleged error, omission, or negligent act, breach of duty, or negligent misstatement committed by the "Insured" solely in the conduct of the "Insured's" "Miscellaneous Professional Services".

38. **"Miscellaneous Professional Services":** services limited to those stated in the Declarations, rendered by the "Insured(s)" to others.

39. **"Policy Period":** the period shown on the Declarations Page. If this Policy is cancelled, the "Policy Period" shall be amended accordingly. If the Discovery Period is exercised in accordance with Section 1, Item 9, it shall be part of the last "Policy Period" and not an additional period.

40. **"Pollutants":** any solid, liquid, gaseous or thermal irritant or contaminant including smoke, odour, vapour, soot, fumes, acid, alkalis, chemicals and waste. Waste includes materials to be recycled, reconditioned or reclaimed.

41. **"Privacy Breach Wrongful Act":** any actual or alleged breach of duty, negligent act, error or omission by the "Insured" that results in:
    (a) the disclosure of "Protected Personal Information"; or
    (b) breach or violation by the "Insured" of any "Privacy Law".

42. **"Privacy Breach Expense":** the following expense where incurred with the Insurer's prior consent in order to comply with any "Privacy Law" or to minimize any "Loss" otherwise covered under this Policy:
    (a) **Notification Expense:** The required amount of necessary expenses incurred by the "Company", or by others on the "Company's" behalf, to minimize any "Loss" otherwise covered under this Policy or to comply with any "Privacy Law" requiring a person or organization storing "Protected Personal Information", either in paper or electronic format, to provide notice to an identified individual of any actual or potential disclosure of "Unauthorized Access" to "Protected Personal Information";
    (b) **Credit Monitoring and Data Recovery Expense:** costs incurred by the "Company" or on the "Company's" behalf:
        (i) to provide credit monitoring expenses to an identified individual to the extent required by "Privacy Law" or to minimize any "Loss" otherwise covered under this Policy; or
        (ii) to recover information which has been accessed without the identified individual's permission where the costs of recovery would minimize any "Loss" otherwise covered under this Policy;
    (c) **Cyber Investigation Expense:** costs incurred by the "Company", or on the "Company's" behalf, with the prior consent of the Insurer, to pay a third party to conduct an investigation of a "Computer System" from which "Protected Personal Information" has been accessed in order to determine the manner in which and the date and time such information was accessed. Such costs do not include compensation, fees, benefits, overhead or the charges or expenses of any "Insured Person"; and
    (d) **Crisis Management Expense:** costs incurred by the "Company", or on the "Company's" behalf, to pay a public relations firm, law firm or crisis management firm, hired with the prior written consent of the Insurer, to perform crisis management services to minimize the potential harm to "Protected Personal Information" which has been wrongfully accessed, but only if in the law enforcement authorities having jurisdiction over the theft of the information have been advised and do not object to such payment. Such costs do not include compensation, fees, benefits, overhead or the charges or expenses of any "Insured Person".

43. **"Privacy Law":**
    (a) the Personal Information Protection and Electronic Documents Act (PIPEDA); or
    (b) other similar federal, provincial, state or local identity theft and privacy protection laws requiring commercial entities that collect personal information to post privacy policies, adopt specific privacy controls, or notify individuals in the event that personal information has potentially been compromised.

44. **"Proposal":** the application for this Policy, together with any other information physically supplied by or on behalf of the "Insured" to the Insurer in connection with underwriting this Policy.

45. **"Protected Personal Information":** a person's first name and/or last name in combination with any one or more of the following:
    (a) social insurance number or social security number;
    (b) medical or healthcare information or data;
    (c) drivers license number; or
    (d) financial account information that would permit access to that individual's financial account.

46. **"Radioactive Material":** uranium, thorium, plutonium, neptunium, their respective derivatives and compounds, radioactive isotopes of other elements and any other substances that the Atomic Energy Control Board may, by regulation, designate as being prescribed substances capable of releasing atomic energy, or as being requisite for the production, use or application of atomic energy.

47. **"Security":** means hardware, software or firmware whose function or purpose is to mitigate loss from or prevent "Unauthorized Access", "Unauthorized Use", receipt or transmission of a "Malicious Code" or "Denial Of Service" attacks of the "Company's" "Computer System". "Security" includes, without limitation, firewalls, filters, computer virus protection software, intrusion detection, the electronic use of passwords or similar identification of authorized users. Also includes specific written policies and procedures intended to directly prevent theft of a password or access code by non-electronic means.

48. **"Technology Professional Services Wrongful Act":** actual or alleged error, omission, negligent act, breach of duty, or negligent misstatement committed by the "Insured" solely in the conduct of the "Insured's" "Technology Professional Services".

49. **"Technology Professional Services":** one or more of the following provided for others for compensation:
    (a) the development, design, assembly, manufacture, sale, leasing, licensing, distribution, installation, modification, integration, servicing, supporting or repairing of computers, computer hardware, firmware and/or software, computerized networks, or similar electronic information systems or telecommunications equipment;
    (b) the provision of computer systems, network related or telecommunication related consulting, analysis, programming, training or support;
    (c) data processing;
    (d) services provider (ASP), domain name registration services, Internet hosting services, Internet service provider (ISP services), web portal services or search engine services; or
    (e) any other related computer services, but will not include "Technology Products".

50. **"Temporary Worker":** a person who is furnished to the "Named Insured(s)" to substitute for a permanent "Employee(s)" on leave or to meet seasonal or short-term workload conditions.

51. **"Technology Products Wrongful Act":** actual or alleged error, omission, negligent act, breach of duty, or negligent misstatement committed by the "Insured" that results in the failure of "Technology Products" to properly perform the function intended.

52. **"Technology Products":** goods, programs, designs, products, services or components which the "Insured" or other trading under the "Insured's" name manufactured, sold, handled or distributed including software updates, service packs and other maintenance releases provided for such products.

53. **"Third Party":** any person or entity which is not an "Insured".

54. **"Trade Secret(s)":** information (including any idea that has been reduced to a written or electronic form, including a formula, compilation, pattern, program, device, method, process, or technique) which:
    (a) derives independent economic value, actual or potential, from not being readily ascertainable through proper means by other person who can obtain economic advantage from its disclosure or use;
    (b) is the subject of reasonable efforts to maintain its secrecy; and
    (c) is used, capable of being used, or intended to be used in commerce.

55. **"Unauthorized Access":** the gaining of access to a "Computer System" by an unauthorized person(s), or by an authorized person(s) in an unauthorized manner.

56. **"Unauthorized Use":** the use of "Computer Systems" by a person unauthorized by the "Insured" or a person authorized by the "Insured" that used the "Computer System" for a purpose not intended by the "Insured".

57. **"Waiting Period":** the number of hours the "Company's" "Computer Systems" experience a "Network Outage" before the Insurer is first obligated to pay "Loss" (other than Extra Expense). The waiting period incepts immediately following the "Network Outage". The "Waiting Period" is specified on the Declarations Page.

58. **"Website":** the software, "Content", and other materials accessible via the "Internet" at a designated Uniform Resource Locator (URL) address owned by the "Company".

59. **"Wrongful Act":** the following, if purchased and a limit is specified on the Declarations Page, when committed by an "Insured" in their capacity as such:
    (a) "Technology Professional Services Wrongful Act";
    (b) "Network Security Wrongful Act";
    (c) "Privacy Breach Wrongful Act";
    (d) "E-Media Wrongful Act";
    (e) "Intellectual Property Wrongful Act";
    (f) "Technology Products Wrongful Act";
    (g) "Miscellaneous Professional Services Wrongful Act".

SECTION III – EXCLUSIONS

COMMON POLICY EXCLUSIONS PART 1

This Policy does not apply to any "Failure Of Security", "Claim" or "Loss" based upon, arising out of or in any way related to:

1. **Dishonest Acts**
    Any actual or alleged dishonest, fraudulent, criminal or malicious act or wilful error or omission committed by any "Insured". This exclusion does not apply to any "Insured" that did not participate in or know about the dishonest act. However, this exclusion will be applied to all "Insureds" if the dishonest act is done with the consent or knowledge of the "Named Insured" or any of the "Named Insured's" directors, partners or executive officers.

COMMON POLICY EXCLUSIONS PART 2

This Policy does not apply to any "Claim(s)" based upon, arising out of or in any way related to:

2. **Asbestos**
    Any actual or alleged liability for any "Claim(s)" in respect of loss, damage, cost or expense directly or indirectly caused by, resulting from or in consequence of, or in any way involving asbestos, or any materials containing asbestos in whatever form or quantity.
    This exclusion applies regardless of any other contributing or aggravating cause or event that contributes concurrently or in any sequence to the loss, damage, cost or expense.

3. **Bodily Injury or Property Damage**
    (a) bodily injury, sickness, mental anguish, disease or death of any person; or
    (b) damage to or destruction of any tangible property including all resulting loss of use of that property. Tangible property does not include data or other information that is in electronic form.
    This exclusion will not apply to a "Claim(s)" for mental injury, mental anguish, or emotional distress resulting directly from a "Privacy Breach Wrongful Act" or an "E-Media Wrongful Act".

4. **Contest and Lotteries**
    Any liability resulting from services provided by or on behalf of the "Insured" or for others that involve contests, games of chance, lotteries, sweepstakes or similar events offering award or other valuable consideration.

5. **Delay, Warranties, Guarantees, Cost Estimates, Fee Disputes**
    (a) delay in the performance of any contract or agreement, unless such delay is due to a "Technology Professional Services Wrongful Act" or a "Miscellaneous Professional Services Wrongful Act";
    (b) express or implied warranty or guarantee;
    (c) cost guarantee or cost estimate; or
    (d) disputes involving the "Insured's" fees or charges.

6. **Discrimination**
    Discrimination of any kind, including, but not limited to, race, creed, religion, age, handicap, sex, marital status or financial condition.

7. **Employment Related Practices**
    Refusal to employ, termination of employment, coercion, demotion, evaluation, reassignment, discipline, harassment, humiliation or any other employment-related practices, policies, acts, errors or omissions.

8. **Fiduciary Duty**
    Breach of fiduciary duty, responsibility or obligation in connection with any employee benefit or pension plan, or arising out of or in consequence of any alleged or actual violation of securities laws, acts or statutes.

9. **Insured versus Insured**
    Any "Claim(s)" that is brought by
    (a) any "Insured"; however, this exclusion will not apply to an otherwise covered "Claim(s)" by an "Employee" alleging a "Privacy Breach Wrongful Act";
    (b) any entity which is owned or controlled by, or is under common ownership or control with, the "Company";
    (c) any person or entity which owns or controls any entity included within the definition of "Insured";
    (d) any "Individual Contracted Worker" of an "Insured"; however this exclusion will not apply to "Claim(s)" arising out of the "Insured's" "Technology Professional Services" and/or "Miscellaneous Professional Services" provided to such "Individual Contracted Worker".

10. **Liability Assumed under Contract**
    The liability of others assumed by the "Insured(s)" under any contract or agreement unless: such liability would have attached to the "Insured(s)" even in the absence of such contract or agreement; or, solely with respect to a "Wrongful Act Respecting Privacy Breach", liability or obligation under a confidentiality or non-disclosure agreement.

11. **Mechanical Failure**
    (a) any electrical or mechanical failures, including power interruption, surge, brownout or blackout; however, this will not apply to electrical or mechanical failures resulting from a "Wrongful Act" relating to the avoidance or minimization of the events above or the resulting consequences;
    (b) fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God, or any other physical event, however caused.

12. **Patents**
    Patent Infringement or theft, copying, misappropriation, display or publication of any "Trade Secret".

13. Pollution
    (a) any "Claim(s)" which arises out of, or would not have occurred, in whole or in part but for the actual, alleged or threatened spill, discharge, emission, disbursal, seepage, leakage, migration, release or escape of "Pollutants" at any time.
    (b) any "Loss", cost or expense arising out of any:
        (i) request, demand or order that any "Insured(s)" or others test for, monitor, cleanup, remove, contain, treat, detoxify or neutralize, or in any way respond to or assess the effects of "pollutants"; or
        (ii) "Claim(s)" or action by or on behalf of a governmental authority for damages because of testing for, monitoring, cleaning up, removing, containing, treating, detoxifying, decontaminating, stabilizing, remediating, neutralizing, or in any way responding to, or assessing the effects of "Pollutants".

14. Prior Acts
Any fact, circumstance or situation indicating the possibility of a "Claim(s)" arising out of any "Wrongful Act" first committed before the Retroactive Date shown in the Declarations Page.

15. Prior Claims
Any fact, circumstance or situation indicating the possibility of a "Claim(s)" and already known to the "Insured(s)", or reported, prior to the effective date of this Policy.

16. Product Recall
The cost or expenses incurred by the Insured or others to withdraw or recall the "Insured's" products or services or any part of such product or services from the marketplace or from use; however, this exclusion will not apply to "Claim(s)" by a "Third Party" for loss of use resulting from the withdrawal, recall, inspection, repair, replacement, adjustment or removal of the "Insured's" products.

17. Nuclear Liability
    (a) liability imposed by or arising under the Nuclear Liability Act;
    (b) any "Claim(s)" with respect to which an "Insured(s)" under this Policy is also Insured under a contract of nuclear energy liability insurance (whether the "Insured(s)" is unnamed in such contract or whether or not it is legally enforceable by the "Insured(s)") issued by the Nuclear Insurance Association of Canada or any other Insurer or group or pool of Insurers or would be an "Insured(s)" under any such Policy but for its termination upon exhaustion of its limit of liability;
    (c) any "Claim(s)" resulting directly or indirectly from the "Nuclear Energy Hazard" arising from:
        (i) the ownership, maintenance, operation or use of a "Nuclear Facility" by or on behalf of an "Insured(s)";
        (ii) the furnishing by an "Insured(s)" of services, materials, parts or equipment in connection with the planning, construction, maintenance, operation or use of any "Nuclear Facility"; and
        (iii) the possession, consumption, use, handling, disposal or transportation of "Fissionable Substances", or of other radioactive material (except radioactive isotopes, away from a "Nuclear Facility", which have reached the final stage of fabrication so as to be usable for any scientific, medical, agricultural, commercial or industrial purpose) used, distributed, handled or sold by any "Insured(s)".

18. Transfer of Funds
The transfer of funds, money and securities; this exclusion will not apply to "Third Party Claim(s)" resulting directly from "Unauthorized Access" to the "Company's Computer System".

19. Violation of Trade Law
Any actual or alleged violation of any law relating to anti-trust, restraint of trade, unfair trade practices, false or deceptive advertising or any other law protecting competition or consumers, other than "Loss" resulting directly from any violation which constitutes a "Wrongful Act Respecting Privacy Breach".

20. Violation of Statues Governing Methods of Sending Material or Information
Any distribution of material that violated or is alleged to violate any statute, ordinance or regulation that prohibits or limits the sending, transmitting, communicating, or distribution of material or information.

21. War
War, invasion, acts of foreign enemies, hostilities (whether war is declared or not), rebellion, revolution, insurrection or military power.

EXCLUSIONS APPLICABLE ONLY TO COVERAGE B – E-MEDIA LIABILITY

This Policy does not apply to any "Claim(s)" based upon, arising out of or in any way related to:
22. INTERNET MEDIA
    (a) disputes over ownership of, licensing or royalty fees associated with, or use of or exercise of rights associated with "E-Media";
    (b) actual or alleged "Failure Of Security" of the "Company's Computer System";
    (c) any "Wrongful Act" or "Interrelated Wrongful Act" in which the first "Wrongful Act" occurs prior to the inception of or subsequent to the termination of the "Policy Period"; or
    (d) display or creation of "E-Media" for or on behalf of others; provided, that this exclusion will not apply to the display of "Advertising" on the "Insured's Internet" site.

EXCLUSIONS APPLICABLE ONLY TO:
COVERAGE C - NETWORK SECURITY AND PRIVACY BREACH LIABILITY
COVERAGE D – PRIVACY BREACH EXPENSE
COVERAGE E – BUSINESS INTERUPTION LOSS
COVERAGE F – DIGITAL ASSETS LOSS
COVERAGE G – CYBER EXTORTION THREAT

This Policy does not apply to any "Failure Of Security", "Claim(s)" or "Loss" based upon, arising out of or in any way related to:

23. TRANSMISSION LINES
Failure of telephone lines, data transmission lines or other infrastructure comprising or supporting the "Internet", unless the lines or infrastructure were under the "Insured's" operational control.

24. FAILURE OF SECURITY
(a) any "Failure Of Security" occurring prior to the "First Inception Date" if the Insured knew or could have reasonably foreseen that this "Failure Of Security" could give rise to a "Claim(s)" or "Loss";
(b) any shortcoming in "Security" that the "Insured" knew about prior to the "Loss";
(c) any failure to ensure the "Insured's" "Computer System" is protected to industry standards by security practices and system maintenance procedures that are equal to or superior to those disclosed in the "Proposal";
(d) the "Insured's" failure to take step to use, design, maintain or upgrade the "Insured's Security"; or
(e)   out of the use, or lack of performance of, software:
(i)   due to expiration, cancellation or withdrawal of the software;
(ii)   that has not yet been released from its developmental state; or
(iii) that has not passed all test runs or proven successful in applicable daily operations.

25. GOVERNMENT AUTHORITY
Any seizure, confiscation, nationalization, or destruction of the "Insured's" "Computer System" or "Digital Assets" by order of any government or public authority.

26. WEAR AND TEAR
Any wear and tear or gradual deterioration of the "Insured's" "Computer System" or "Digital Assets".

SECTION IV – CONDITIONS

1.   ACTION AGAINST THE INSURER
No action or legal proceedings may be initiated against the Insurer unless the "Insured(s)" has fully complied with the requirements of this Policy.

2.   ADJUSTMENT CLAUSE
This Policy is issued and the premium computed on the basis of the information submitted to the Insurer as part of the "Proposal". The Insurer may require premium adjustment, when Premium Adjustment Terms are shown on the Declarations Page, and coverage revision in the event:
(a) the "Named Insured(s)" acquires any other entity; or
(b) the "Named Insured(s)" creates or acquires a subsidiary subsequent to the inception date of this Policy. The "Named Insured(s)" agrees to give notice to the Insurer in writing in ninety (90) days of the happening of either of the foregoing and furnish such information in connection therewith as the Insurer may require.

3.   ALLOCATION
If a "Claim(s)" made again the "Insured" involve both covered and uncovered allegations and/or parties, the "Insured" recognizes that there must be an allocation between insured and uninsured loss. The "Insured" and the Insurer will exert their best efforts to agree upon a fair and property allocation between insured and uninsured loss.

4.   ASSIGNMENT
Assignment of interest under this Policy shall not bind the Insurer unless its consent is endorsed hereon.

5.   ASSISTANCE AND CO-OPERATION
The "Insured(s)" shall co-operate with the Insurer in the investigation and defence of any "Claim(s)" or suit, give to the Insurer such information and written statements as the Insurer may require, and shall attend depositions, hearings and trials and give evidence in connection with the defence of such suit, all without charge to the Insurer. The "Insured(s)" shall not voluntarily make any payment, assume any liability or obligation or incur any expense, unless with the written consent of the Insurer.

6.   AUDIT
The Insurer may examine and audit the "Insured's" books and records at any time during the "Policy Period" and within three (3) years after the end of the "Policy Period', as they relate to the matter of this Policy.

7.   AUTHORIZATION CLAUSE
By acceptance of this Policy, all "Insured's" agree that the "Named Insured(s)" shall act on their behalf with respect to the giving or receiving of any notice provided for in this Policy, the payment of premiums and the receiving of return premiums and the negotiation and acceptance of any endorsement.

8.   BANKRUPTCY
Bankruptcy or insolvency of the "Insured" or of the "Insured's" estate does not relieve the Insurer of its obligations under this Policy.

9.   CANADIAN CURRENCY
All limits of insurance, premiums and other amounts as expressed in this Policy are in Canadian currency.

10. CANCELLATION

This Policy may be cancelled:

(a) by the Insurer giving to the "Named Insured(s)" by registered mail notice of cancellation as follows:

    (i) 15 days' notice of cancellation, if cancellation is due to non-payment of premium;

    (ii) 60 days' notice of cancellation, if cancellation is due to any other reason, such notice to be accompanied by a pro rata return of premium.

(b) by the "Named Insured(s)", giving written notice at any time. Cancellation will take effect on the date of the "Named Insured's" written notice or at a later date if specified therein. The Insurer will refund the unearned premium on a short-rate basis, but in no event shall the short-rate premium for the expired time be deemed to be less than any minimum retained premium specified. This Policy may not be cancelled during the Discovery Period.

11. CHANGES

This Policy contains all the agreements between the "Named Insured(s)" and the Insurer concerning the insurance afforded. The "Named Insured(s)" shown in the Declarations Page is authorized to make changes in the terms of this Policy with the Insurer's consent. The terms of this Policy may be amended or waived only by endorsement issued by the Insurer and made a part of this Policy.

12. NOTICE OF "CLAIM(S)"

A. Liability Coverage's – SECTION I - COVERAGE PARTS (A), (B), and (C)

The "Insured(s)" shall give immediate notice in writing of any "Claim(s)" to the Insurer as soon as practical at the address shown in Section IV, Item 13.

If during the period of this insurance the "Insured(s)" shall first become aware of any occurrence or situation which might reasonably be expected to give rise to a "Claim(s)" against the "Insured(s)" and shall during the period of this insurance give written notice to the Insurer of such occurrence or situation, then any such "Claim(s)" which is subsequently made shall be deemed to have been made on the date that the Insurer was advised of the occurrence or situation. Such notice will include:

1) the name of the potential claimant and a date and description of the specific "Wrongful Act" which form the basis of the potential "Claim(s)";

2) the nature of the potential damages arising from such specific "Wrongful Act"; and

3) the circumstances by which the "Insured" first became aware of the specific "Wrongful Act".

B. Privacy Breach Expense Coverage Notice – SECTION I - COVERAGE PARTS (D)

As a condition precedent to coverage, the "Insured" shall report to the Insurer any "Privacy Breach Wrongful Act" or "Network Security Wrongful Act" for which the "Insured" seeks "Privacy Breach Expense" coverage under this Policy. Such notice must be reported within thirty (30) days of the "Privacy Breach Wrongful Act" or "Network Security Wrongful Act". The "Insured" must obtain written consent from the Insurer prior to incurring such expenses.

C. First Party Coverage - SECTION I - INSURING AGREEMENTS - COVERAGE PARTS (E), (F) AND (G)

As a condition precedent to coverage the "Insured" shall:

(a) give the Insurer immediate written notice of any "Business Interruption Loss", "Digital Assets Loss", or "Credible Threat" which take place or is reasonably likely to take place during the "Policy Period";

(b) provide a written description of the details of the "Network Outage" or "Credible Threat" as soon as practicable;

(c) complete and sign a written, detailed and sworn proof of loss within ninety (90) days after the discovery of a "Business Interruption Loss", "Digital Asset Loss" or "Credible Threat" (unless such period has been extended by the Insurer's written agreement) including a full description of and circumstances surrounding such "Business Interruption Loss", "Digital Assets Loss", or "Credible Threat", including without limitation, the time, place and cause of the " Business Interruption Loss", "Digital Assets Loss", or "Credible Threat", a detailed calculation of any " Business Interruption Loss", the "Insured's" interest and the interest of all others in the property, the sound value thereof and the amount of loss or damage thereto and documents and material of whatever media that reasonably relates to or forms a part of the basis of the claim for such loss;

(d) upon the Insurer's request, submit to an examination under oath;

(e) immediately record the specifics of any "Business Interruption Loss", "Digital Assets Loss", or "Credible Threat" and the date the "Insured" first became aware of such "Business Interruption Loss", "Digital Assets Loss", or "Credible Threat";

(f) at the Insurer's request report such "Credible Threat" to the RCMP, FBI, CIRCC, CERT, ISAC or any other central reporting or investigative organization that the Insurer may designate;

(g) provide the Insurer with any cooperation and assistance that the Insurer may request, including assisting the Insurer in:

    (i) any investigation of a "Failure Of Security", "Loss" or circumstances that may give rise to a "Claim(s);

    (ii) enforcing any legal rights the "Insured" or the Insurer may have against anyone who may be liable to the "Insured";

    (iii) executing any documents that the Insurer deems necessary to secure the Insurer's rights under this Policy; and

    (iv) any inspection or survey conducted by the Insurer.

The costs and expenses of establishing or proving "Business Interruption Loss", "Digital Assets Loss", or "Credible Threat" for this Policy, including those in connection with preparing a proof of loss shall be the obligation of the "Insured" and are not covered under this Policy.

13. NOTIFICATION OF "CLAIM(S)"

All "Claim(s)" notice(s) are to be reported to Charles Taylor Adjusting at:

Local: 416-640-6022

Toll Free: 1-866-547-6022

14. OTHER INSURANCE

If other valid and collectable insurance is available to an "Insured(s)" for any "Loss" that is covered under this Policy, the Insurer under this Policy shall be liable for only the excess, if any, of any "Loss" over the applicable limit of the other insurance covering such "Loss".

This Policy shall not contribute to any "Claim(s)" that is less than or equal to the applicable limit of the other insurance covering such "Claim(s)".

In the event that any part of such other valid and collectible insurance is provided by another Policy of any member company of the Co-operators Group, the Insurer's liability hereon shall be reduced by the amount payable under such other Policy.

15. **REPRESENTATIONS**

By accepting this Policy, the "Named Insured(s)" agrees:

(a) the statements in the Declarations Page are accurate and complete;

(b) those statements are based upon representations the "Named Insured(s)" has made to the Insurer; and

(c) the Insurer has issued this Policy in reliance upon the "Named Insured's" representations, documentation, data and other material the "Named Insured(s)" has furnished to the Insurer.

16. **SEVERABILITY CLAUSE**

This Policy shall be construed as a separate agreement with each "Insured(s)". Nothing in this clause shall increase the Insurer's maximum liability as set forth in Section 1, Item 6 of this Policy.

17. **STATUTORY CONFORMITY**

Terms of this Policy, which are in conflict with the statutes of the province where the "Insured(s)" has its main address, are hereby amended to conform to such statutes.

18. **SUBROGATION**

In the event of any "Claim(s)" under this Policy, the Insurer shall be subrogated to all the "Named Insured's" rights to recovery thereof, and the "Insured(s)" shall execute and deliver instruments and papers and do whatever else is necessary to secure such rights. The "Insured(s)" shall do nothing to prejudice such rights.

IN WITNESS WHEREOF the Insurer has executed and attested these presents, but this Policy shall not be valid unless countersigned on the Declarations Page by a duly authorized representative of the Insurer.

UNLICENSED SOFTWARE EXCLUSION

APPLICABLE TO THE INTELLECT ERRORS AND OMISSIONS LIABILITY FORM

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

It is stated and agreed that **Section III - Exclusions, Common Policy Exclusions Part 2**, is amended to include the following:

Unlicensed Software
Actual or alleged use, duplication, appropriation, downloading, or distribution by any "Insured Person" of any electronic software, data, code, application, file, or program, in breach of any actual or alleged authority, license, terms of use, contract, agreement, copyright, patent, or other intellectual property right, asserted by others over or in connection with such materials.

All other terms and conditions of this Policy remain unchanged.

Except as otherwise provided in this endorsement all terms, provisions and conditions of the Policy shall have full force and effect.