IGS (Infor Government Solutions SaaS) - Terms and Conditions:

These IGS Terms and Conditions only apply to the Software listed in the Order Form to which these terms are attached.

1) INFOR GENERAL OBLIGATIONS & RESPONSIBILITIES.

a) The Software will be provided by Subscription Services utilizing the Amazon Web Services LLC's AWS GovCloud (US) ("AWS GovCloud"), these Subscription Services are referred to as "IGS".

b) Access to Customer Data in IGS by Infor staff will be in accordance with applicable U.S. export controls laws, defined as the Export Administration Regulations, 15 C.F.R. Parts 730-744 ("EAR") and the International Traffic in Arms Regulations, 22 C.F.R. Parts 120-130 ("ITAR") (collectively "U.S. Export Controls Laws").

c) When feasible, Scheduled Maintenance windows will be scheduled to minimize impact on Authorized Users located in continental U.S. time zones.

2) CUSTOMER GENERAL OBLIGATIONS & RESPONSIBILITIES.

a) For Customer Data subject to FedRAMP "Moderate" or "Low" controls, Customer further agrees to be bound by and comply with the Customer Responsibilities Matrix attached hereto and incorporated herein as Exhibit A

b) Customer acknowledges and agrees that Infor is not an exporter of data as contemplated by U.S. Export Controls Laws. Customer also acknowledges and agrees that it is solely responsible for managing its own U.S. Export Controls Laws compliance obligations while uploading, downloading, possessing, accessing, processing, storing, and otherwise maintaining data in IGS. If Customer uploads, downloads, possesses, accesses, processes, stores or otherwise maintains U.S. export-controlled data in IGS then, in addition to any applicable U.S. Export Controls Laws, Customer represents and warrants that:

i) If Customer is a "U.S. Person" under applicable U.S. Export Controls Laws, Customer has and will maintain a valid U.S. export authorization (e.g., license, Technical Assistance Agreement, license exception or exemption) that covers its use of the Software in IGS, including the uploading, downloading, possessing, accessing, processing, storing, and otherwise maintaining of any U.S. export-controlled data in IGS, if required by applicable U.S. Export Controls Laws;

ii) If Customer is a non-U.S. Person (i.e., "Foreign Person") under applicable U.S. Export Controls Laws, Customer is and will continue to be a party (e.g., end user) to a valid U.S. export authorization (e.g., license, Technical Assistance Agreement, license exception or exemption) that covers its use of the Software in IGS, including the uploading, downloading, possessing, accessing, processing, storing, and otherwise maintaining of any U.S. export-controlled data in IGS, if required by applicable U.S. Export Controls Laws;

iii) Customer has and will maintain a valid U.S. Department of State Directorate of Defense Trade Controls annual registration, if applicable and required by the ITAR;

iv) Customer has full export privileges under U.S. Export Controls Laws, and Customer is not a denied or debarred party under U.S. Export Controls Laws or otherwise subject to export-related sanctions, including sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control;

v) There are no overriding data residency requirements with a country of origin restricting Customer from having Customer Data reside in the United States;

vi) Customer understands that it is solely responsible for any U.S.-export controlled data that it and its Authorized Users upload, download, possess, access, process, store, or otherwise maintain in the IGS; and

vii) Customer has and shall maintain its own compliance program for purposes of complying with applicable U.S. Export Controls Laws by Customer and its Authorized Users.

If Customer's export control privileges are revoked, suspended, or terminated, or Customer otherwise becomes subject to sanctions or barred from maintaining export-controlled data, Customer will immediately remove export-controlled data from the Software. Customer will promptly in writing (i) notify Infor that Customer's export control privileges were revoked, suspended, or terminated, or that Customer otherwise became subject to sanctions or barred from maintaining export-controlled data, and (ii) certify that all affected export-controlled data has been removed from the Software.

Customer is responsible for verifying that the Software and Subscription Services are sufficient for Customer's organization, business processes, and any applicable laws or regulations to which Customer is subject, including U.S. Export Controls Laws. Customer is solely responsible for setting, administering, and appropriately restricting access to data, reports, and capabilities within the Software in accordance with U.S. Export Controls Laws and other applicable laws that apply to Customer. Customer acknowledges that if Infor provides any assistance to Customer in connection with such user restrictions, Infor does so at the direction of Customer and subject to Customer's ultimate review. Customer acknowledges and agrees that Customer, not Infor, is providing access by users to data in the IGS.

c) Customer and its Authorized Users will not upload, possess, process, store, or otherwise maintain U.S. government classified information or content that is subject to U.S. governmental regulation or that requires security measures beyond those specified for the Subscription Services or Software, unless Infor has specifically agreed in writing to implement additional security and other measures related to such information or content.

d) Support. When engaging Infor Support for the Software on this Order Form identified as using the AWS GovCloud, Customer shall at the earliest opportunity, disclose that its request pertains to the "GovCloud" or "IGS" environment.

e) Professional Services. Customer acknowledges that these IGS Terms and Conditions do not apply to any professional services provided by Infor. Customer is responsible for establishing any data handling requirements necessary for its Customer Data as part of any such professional services engagement.

f)Customer Responsibility. Customer will be liable for any loss, cost, penalties, fines and expense incurred arising from any breach of Customer's obligations herein, Customer or its Authorized Users' violations of applicable laws, including U.S. Export Controls Laws, and Customer or its Authorized Users' use of U.S. export-controlled data with the Software. Such responsibility for costs and expenses, may include, without limitation, costs and expenses incurred for AWS GovCloud's services arising from Customer's introduction of U.S. government classified information or content into the AWS GovCloud in violation of these IGS Terms and Conditions.

3) LIABILITY.

NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT, EXCEPT IN THE EVENT OF INFOR'S WILLFUL MISCONDUCT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL INFOR, ITS AFFILIATES OR THIRD PARTY LICENSORS BE LIABLE TO CUSTOMER, CUSTOMER AUTHORIZED USERS OR TO ANY THIRD PARTY FOR ANY DAMAGES ARISING IN CONNECTION WITH THE STORAGE OR PROCESSING OF ITAR CONTROLLED DATA IN THE SOFTWARE. THIS DISCLAIMER OF LIABILITY SHALL APPLY REGARDLESS OF THE FORM OF ACTION THAT MAY BE BROUGHT AGAINST INFOR, WHETHER IN CONTRACT OR TORT, INCLUDING WITHOUT LIMITATION ANY ACTION FOR NEGLIGENCE, PRODUCT LIABILITY, FAILURE OF THE SOFTWARE TO CONFORM TO ANY LEGAL OR REGULATORY REQUIREMENT OR CLAIMS ARISING UNDER CONSUMER PROTECTION OR SIMILAR LEGISLATION. IN NO EVENT WILL INFOR, ITS AFFILIATES OR THIRD PARTY LICENSORS BE LIABLE FOR ANY SPECIAL, PUNITIVE, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, AND REGARDLESS OF WHETHER INFOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE. NOTWITHSTANDING ANY OTHER PROVISION IN THE AGREEMENT, ANY PURPORTED LIMITATION ON CUSTOMER'S LIABILITY, AS TO THE TYPE OR AMOUNT OF DAMAGES, SHALL NOT APPLY TO ANY LIABILITY OF CUSTOMER ARISING OUT OF THESE IGS TERMS AND CONDITIONS. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH; (2) FOR GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

4) Infor Government Solutions SaaS (IGS) - External Rules of Behavior.

Customer agrees, as a condition of using the Infor Software and Subscription Services, to require each Authorized User to be bound by the following Rules of Behavior when using the Infor Software and Subscription Services, by executing a written agreement or electronically at first login:

a) Users must conduct only authorized business on the IGS system, including activity that is consistent with behavior expected during consumption of a US Government Information System and compliant with U.S. Export Controls Laws and any other applicable laws.

b) Each Authorized User's level of access to Infor Software, Subscription Services and Customer Data is set by Infor's Customer/Authorized User's employer and limited to ensure Authorized User access is no more than necessary to perform Authorized User's legitimate and authorized tasks or assigned duties. If an Authorized User believes they are

being granted access that they should not have, they must immediately notify Infor's Customer/Authorized User's employer.

c) Authorized Users must maintain the confidentiality of their authentication credentials, including their password. Authorized Users will not reveal authentication credentials to anyone; Infor personnel should never ask Authorized Users for Authorized Users' authentication credentials.

d) Authorized Users must follow proper logon/logoff procedures. Authorized Users must manually logon to their sessions; Authorized Users must not store Authorized User passwords locally or utilize any automated logon capabilities. Authorized Users must promptly logoff when session access is no longer needed. If a logoff function is unavailable, Authorized Users must close their browser. Authorized Users must never leave computers unattended while logged into the system.

e) Authorized Users must report all security incidents or suspected incidents (e.g., improper or suspicious acts) related to Infor Software and Subscription Services to Infor Support.

f) Authorized Users must not establish any unauthorized interfaces between the Infor Software and Subscription Services.

g) Authorized User access to Infor Software and Subscription Services is governed by, and subject to, all federal laws, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the applicable Infor system maintains individual Privacy Act information. Authorized User access to Infor systems constitutes consent to the retrieval and disclosure of the information within the scope of Authorized User's authorized access, subject to the Privacy Act, and applicable state and federal laws.

h) Each Authorized User must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.

Authorized Users must not upload, process, store, or otherwise maintain information in the Software or Subscription Services that is classified more stringently than the data classification level of Controlled Unclassified Information (CUI) currently associated with Infor's FedRAMP authorization and attestation for compliance; unless expressly permitted in writing by Infor.

i) Authorized Users must not browse, search, or reveal information hosted by the Infor Software and Subscription Services, except in accordance with that which is required to perform your legitimate and authorized tasks or assigned duties.

j) Authorized Users must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.

k) Authorized Users understand that any person who obtains information from a computer connected to the Internet in violation of her/his employer's computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

l) Authorized Users agree to contact Infor Support if they do not understand any of these rules.

In addition, Customer must ensure the following for Authorized Users' web browser(s):

m) that Web browsers use Secure Socket Layer (SSL) version 3.0 (or higher) and Transport Layer Security (TLS) 1.2 (or higher). SSL and TLS must use a minimum of 128-bit, encryption.

n) that web browser is configured to warn about invalid site certificates.

o) that web browser checks for a publisher's certificate revocation.

p) that web browser checks for server certificate revocation.

q) that proper anti-virus/malware technology is applied to check for any malicious code upon download.

By its signature to this Order Form, Customer confirms it has read the above Rules of Behavior for Infor Software and Subscription Services. By its signature, Customer acknowledges and agrees that Customer and its Authorized Users' access to all Infor Software and Subscription Services is covered by, and subject to, such Rules of Behavior and applicable laws, including U.S. Export Controls Laws. Further, Customer acknowledges and accepts that any violation by Customer or any of its Authorized Users of these Rules of Behavior or applicable laws, including U.S. Export Controls Laws, may subject Customer or its Authorized Users to civil and/or criminal actions by the U.S. government. Customer also acknowledges and accepts that Infor retains the right, at its sole discretion, to terminate, cancel or suspend Customer and any of its Authorized Users access rights to the Infor Software and/or Subscription Services at any time, without notice, if Customer or any of it Authorized Users violate the Rules of Behavior, or if Customer o or any of its Authorized Users actions or inactions creates a security risk, or negatively impacts the availability of the system. When the End User is an instrumentality of the U.S., recourse against the United States for

any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act).

Exhibit A

Infor Government Solutions Customer Responsibility Matrix

for Data Subject to FedRAMP "Low" or "Moderate" Controls

Ref #	Customer Responsibility	Controls Reference
1	As Infor relies upon Customer's Identity Provider (IdP), it's the Customer's responsibility to identify and select the "boot strap" admin needed to account management of the tenant. Customer or the privileged user for Customer will establish conditions and role membership for the tenant as well as specify any authorized users of the group and role membership, access authorizations/privileges and any other attribute (as required) for each account. Customer is responsible for identifying and determining the personnel and the roles necessary as well as the processes to approve, enable, modify, disable and/or remove user accounts (privileged or non-privileged). Customer is responsible for monitoring the use of their accounts and also for identifying personnel and/or processes in additions to roles that will provide notification to boot strap admins/privileged users when accounts are no longer required, the user is terminated or transferred, or when a usage or need-to-know changes. Customer is responsible for authorizing access to the tenant based on valid access authorization, intended usage, and other attributes as required by Customer or their customer's mission or business needs. Customer is responsible for reviewing the accounts for compliance, annually. Customer is also responsible for establishing a process to reissue shared/group account credentials (if deployed) when individuals are removed from the group.	AC-2
2	Customer has the responsibility to apply the principles of least privilege to the development, implementation and operations as it relates to Customer implementation or configuration settings affecting the Customer's assets on premise or hosted under the purview of the Customer. Specifically, Customer will only allow authorized access for users (or processes acting on behalf of users) which are critical to accomplish assigned tasks in accordance with Customer or their customer's missions and business functions.	AC-6
3	Customer application access is controlled by SAML tokens and CACs, implemented as part of Customer authentication solutions. It is a Customer responsibility to handle unsuccessful login attempts.	AC-07
4	Application access will use accounts on Customer identity management solutions, auditing successful and unsuccessful logon events and account management events is a Customer responsibility for customer identity management solutions. Infor will audit users accessing the system with SAML tokens and assignment of Infor roles to Customer accounts including addition of roles to an account, changes of roles to an account and removal of roles from an account. Customer is also responsible for all Customer application data, including the people, places, things, business rules, and events in relation to Customer's business goals/mission. This data is provided to Customer from within the application for their review and analysis. The distinction between Infor Security Related Data and Customer Application Data has been made to clarify what audit information is required. Customer Application Data is not necessary to support after-the-fact investigations of security incidents and will not be captured for this function. Auditable events regarding Customer Application Data will be captured and will be made accessible to customers through the application or by request, if not available through the application.	AU-02
5	Customer's Authorizing Official will determine risk acceptance for any web calls, PIs or other data flows (ingress/egress) that might impact the confidentiality, integrity and/or availability. Infor is responsible for documenting the data flows and updating the documentation of the security attributes as necessary.	CA-3
6	Customer accounts maintained on customer identity management systems will be used for application access. Infor will accept SAML tokens from Customer Active Directory or LDAP implementations. It is a Customer responsibility to provide access	IA-02

	control and multifactor authentication for accounts that reside in customer identity management implementations that provide access to Infor. These users would connect to Infor using HTTPS with TLS sessions utilizing Customer provided credentials including multifactor authentication verified against customer identity management systems. Typically this would include a user ID, password or PIN and a Personal Identity Verification (PIV) card or Common Access Card (CAC). It is also a Customer responsibility to manage additional user types, if they determine they are needed within their SaaS instance. These user types provide limited access for specific functions outside of the general use case. They are implemented, configured, and managed from within the IGS application by a privileged customer user. IGS user types, how they are to be used, the justification for their inclusion, and the mitigating controls are detailed below. IA controls are not applied to customer service accounts. These accounts have limited access through the ION API Gateway to specific functions, based on Customer need. Access to back end systems are not permitted.	
7	It is a Customer responsibility to provide multifactor authentication as part of their identity management implementation that will be used with Infor.	IA-02(1) and IA-02(2)
8	It is a Customer responsibility to provide replay-resistant multifactor authentication as part of their identity management implementation that will be used with Infor.	IA-2(8)
9	It is a Customer responsibility to provide multifactor authentication requiring a separate device, such as a PIV card or CAC, as part of their identity management implementation that will be used with Infor.	IA-2(11)
10	It is a Customer responsibility to authorize access for their organization's users of the Infor system before granting access. The application access path includes customer authentication via SAML assertions from customer identity management solutions. It is a Customer responsibility to select identifiers for application access by their users. It is a Customer responsibility to provision and manage the administration of InforOS Service Accounts that are created and enabled from within the Customer interface within the Infor environment. These Service Accounts perform specific actions with limited scope on behalf of the Customer to support Infor applications within its cloud suites.	IA-4
11	Infor utilizes SAML assertions from customer identity management solutions to control access to the system. It is a Customer responsibility to implement all aspects of authenticator management for their users.	IA-5
12	Infor utilizes SAML assertions from customer identity management solutions to control access to the system. It is a Customer responsibility to implement all aspects of authenticator complexity, lifetime, reuse and protection on their identity management systems.	IA-5(1)
13	It is a Customer responsibility to distribute PIV Cards or CACs or any other hardware or biometric multifactor authenticators that may be used in the Customer's authentication solution in person before a Customer registration authority with authorization by Customer account authorizers.	IA-5(3)
14	It is a Customer responsibility to define the token quality requirements for hardware token-based authentication for use with their identity management solution.	IA-5(11)
15	It is a Customer responsibility to configure customer identity management systems to obscure feedback of all authenticators.	IA-6
16	Customer users authenticate to their own agencies' identity management solutions and access Infor with a SAML token presented by the customer identity management solution. Customer requirements are detailed throughout the IA controls	IA-8
17	Verification of PIV credentials is a Customer responsibility and will be carried out by customer identity management systems. After successful authentication SAML assertions will be transmitted from the customer identity management systems to INFOR.	IA-8(1)

18	All verification of third party credentials will be carried out by customer identity management systems. It is a Customer responsibility to configure their identity management systems to accept only FICAM-approved third-party credentials.	IA-8(2)
19	All verification of third party credentials will be carried out by customer identity management systems. It is a Customer responsibility to employ only FICAM-approved information system components in their identity management system to accept third-party credentials.	IA-8(3)
20	It is a Customer responsibility to implement identity management systems that conform to FICAM-issued profiles.	IA-8(4)
21	Roles within Infor are highly customizable and new roles can be defined by the Customer. It is a Customer responsibility to limit management functionality to appropriate roles and users within their organization.	SC-2
22	It is the responsibility of Customer to install, configure, system harden and conduct routine risk management of any SFTP server from which Infor services will securely transfer files to/from our authorized boundary. Customers are required to setup authentication and provide account management. All traffic traversing the internet must be supported to encrypt end-to-end using an IPSec tunnel and the latest FISMA/FedRAMP encryption standards (i.e - FIPS 140-2 validated module)	AU-2, CM-6, RA-5, IA-7, IA-8
23	Customer has a responsibility to scan for vulnerabilities related to Customer implementation or configuration settings affecting the Customer's assets on premise or hosted under the purview of the Customer, monthly for OS, dB and web applications; ad-hoc when new vulnerabilities potentially affecting the system/applications are identified and reported; and annually by an American Association for Laboratory Accreditation (A2LA) accredited Third Party Assessment Organization (3PAO) to scan OS, dB and web application. Customer is responsible for employing scanning tools leveraging standards for enumerating platforms, software flaws, and improper configurations formatting checklists and test procedures and measuring vulnerability impact against the Common Vulnerability Scoring System (CVSS). Customer is responsible for the monthly interpretation of the vulnerability scan reports as well as analysis of any security control assessments performed on the Customer's assets on premise or hosted under the purview of the Customer. Customer is responsible for remediating any legitimate vulnerabilities within 30 days for high CVSS findings, 90 days for moderate CVSS findings, 180 for low CVSS findings from the date of discovery. For Federal customer's or customer's supporting Federal customers: it's their responsibility to share with their Risk Executive, IGS' System Owner, and the FedRAMP JAB information obtained from the annual vulnerability scanning process and security control assessments conducted by the 3PAO and monthly for any overdue high findings to IGS' System Owner and FedRAMP JAB related to customer implementation or configuration settings affecting customer's assets on premise or hosted under the purview of customer. For all other customers, it's their responsibility to share with their Risk Executive and/or the Risk Executive of their customer as well as IGS' System Owner information obtained from the annual vulnerability scanning process and security control assessments conducted by the 3PAO and monthly for any overdue high findings to IGS' System Owner and FedRAMP JAB related to customer implementation or configuration settings affecting the customer's assets on premise or hosted under the purview of the customer.	RA-5
	Customer has a responsibility as part of their configuration management process to identify, report and correct any flaws or vulnerabilities that are a result of Customer implementation and/or configuration settings. Customer also has a responsibility to install security relevant or vendor dependent software and firmware updates within 30 days of the release of the updates. As part of Customer's release process, Customer's responsibilities include testing software and firmware updates related to the flaw remediation or any other security relevant vendor dependencies before production deployment for any system breaks	SI-2