Infor Government Solutions

Cybersecurity Maturity Model Certification (CMMC) & International Traffic in Arms Regulations (ITAR) & Access Controls

Frequently Asked Questions

CMMC Compliance

Is your ERP system designed to meet CMMC requirements?
Yes, both Infor CloudSuite Aerospace and Defense & CloudSuite Industrial are deployed in the AWS Gov Cloud and Infor hires a 3rd party independent audit firm to identify any vulnerabilities to NIST Controls.

Can you provide documentation or evidence of CMMC compliance for your product? Can you provide an SOC 2 Type 2 Report?
Yes, we annually receive a letter of attestation for NIST 800-171 and can provide both an example of this and SOC Type 2 report.

What CMMC level(s) does your product support?
Compliant with CMMC v2 level 2

How does your ERP system handle Controlled Unclassified Information (CUI)?
Infor's Information Security Office (ISO) has established an Information Security Management System (ISMS), inclusive of security policies that provide guidelines towards the people, processes and technology necessary to protect the confidentiality, integrity and availability of data.

The Infor Cloud Environments have multiple layers of security, designed to help protect against both targeted attacks and general information gathering attacks. Infor monitors its network using a set of tools (like firewall group networks, DDoS protection, recurring vulnerability scans) , specifically configured to manage logs from multiple resources and alerts in real time (SIEM) to identify hacking or other intrusion attempts. Additionally SaaS systems also have Host-based intrusion detection and prevention systems (IDS/IPS) to deter infiltration attempts.

Infor SaaS solutions use industry standard encryption methods while transmitting or storing Licensee data; (1) In Transit the data is encrypted with TLS 1.2 and (2) while data at rest within SaaS the storage is encrypted with AES 256 bit.

How is our data protected in transit and when stored at rest? Specifically, is it FIPS 140-2 level Encrypted?
Infor SaaS solutions use industry standard encryption methods while transmitting or storing Licensee data; (1) In Transit the data is encrypted with TLS 1.2 and (2) while data at rest within SaaS the storage is encrypted with AES 256 bit. Amazon's Key Management Service (KMS) is used to manage encryption within Infor SaaS deployments.

Encryption keys are securely protected against unauthorized access, separation of duties exists between the key managers and the hosting organization

KMS Service is well described in the following link:
https://docs.aws.amazon.com/kms/latest/cryptographic-details/kms-crypto-details.pdf

To enable effective encryption for encryption at rest, Infor relies upon AWS EBS Encryption which is fully explained here: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Can employees of your company access our data without our approval? Can we bring our own Encryption Keys?

No. Application-level access is controlled via the customer's existing authentication infrastructure via ADFS/SAML 2.0 integration. Customer identity provider (IdP) should be SAML 2.0 complaint. For Users, Infor offers a multitude of profiles for our customers. Administration accounts are set up by Infor for the benefit of customers' users to perform functions necessary, with the appropriate role access.

Access to the data by company's employee will always be controlled by the company. They will have the ability to assign roles and responsibilities to each of your users. The creation of each user account is designed with a "least privileged" starting point. Meaning that the company will have the ability to assign access and privileges on a user-by-user basis.

Infor manages all cryptographic keys used to encrypt/secure our customer's data. We leverage Amazon Web Services' Key Management Service (KMS) to create and manage encryption keys. Encryption keys are securely protected against unauthorized access, and separation of duties exists between the key managers and the Cloud Operations team with systems access.

Please visit https://aws.amazon.com/kms for more information on AWS KMS Service.

What security measures are in place to prevent unauthorized access to sensitive data?

Infor SaaS application provides defined security roles and responsibilities, that enables Licensee to establish security constraints from the most generic to the most specific for their users, enabling them to control the amount of access the user has to the application's data. Infor's product documentation provides detailed information on how to define User, Group and Role security.

The Infor Cloud Environments have multiple layers of security, designed to help protect against both targeted attacks and general information gathering attacks. Infor monitors its network using a set of tools (like firewall group networks, DDoS protection, recurring vulnerability scans) , specifically configured to manage logs from multiple resources and alerts in real time (SIEM) to identify hacking or other intrusion attempts. Additionally SaaS systems also have Host-based intrusion detection and prevention systems (IDS/IPS) to deter infiltration attempts.

Infor SaaS solutions use industry standard encryption methods while transmitting or storing Licensee data; (1) In Transit the data is encrypted with TLS 1.2 and (2) while data at rest within SaaS the storage is encrypted with AES 256 bit.

Do you regularly undergo CMMC assessments or audits?

An audit is performed annually by an independent 3rd party audit firm. Infor SaaS applications undergo SSAE18-based assessment and third-party generated audit reports are published (SOC Reports). These are available to our prospect customers upon signing a Non-Disclosure Agreement. More details can be located on www.trust.infor.com.

ITAR Compliance

Is your ERP software designed to support ITAR regulations for export-controlled data?
When deployed in the AWS Gov Cloud, Infor CloudSuite Aerospace and Defense and CloudSuite Industrial can only be accessed by US Persons by AWS and Infor and the customer holds a shared responsibility model when granting access.

Is your ERP System FedRamp Authorized?
Yes, and we are listed on the FedRAMP marketplace.
https://marketplace.fedramp.gov/products/FR1710033970

How does your ERP system ensure the protection of ITAR-restricted information?
By insuring access only to US Persons

Are there specific features or modules in your ERP system that address ITAR compliance?
Yes, we have fields and tables protected by role or user.

Can you provide references of customers who use your ERP system for ITAR compliance?
Yes, we be happy to provide references as our partnership matures.

Do you have a documented ITAR compliance strategy and program in place?
We have best business practices in the IPC to assist with ITAR controls.

Access Controls

Do you support multi-factor authentication (MFA) to enhance security?

Yes. Authentication is achieved through your identity provider whereby MFA can be configured.

Infor leverages Federation/SAML 2.0 services to integrate with the customer's existing authentication infrastructure. If the customer's current authentication infrastructure provide multi-factor authentication, then Infor can incorporate that solution into the authentication process. Infor does not provide a multi-factor authentication solution on its own.

Enabling multi-factor authentication for users is an implementation decision. Support for multi-factor authentication is a standard feature of the proposed solution.

Customers may choose to enable multi-factor authentication through their selected Identity Management solution, either:

- a customer-managed, SAML 2.0-compliant or OIDC-compliant solution (most common), or
- Infor's provided Infor Federated Services (IFS) solution – see user privileges below

Can your ERP system enforce role-based access controls (RBAC) to restrict access to sensitive data?

Infor SaaS application provides defined security roles and responsibilities, that enables Licensee to establish security constraints from the most generic to the most specific for their users, enabling them to control the amount of access the user has to the application's data. Infor's product documentation provides detailed information on how to define User, Group and Role security.

How are user privileges managed and monitored?

User privileges are managed in the Infor OS IFS component. User assignment to roles to managed in this tool. A SCIM interface allows for automation from your IDP/IAM tool. For monitoring, change records are accessible within the tool. As any change is made to the user or role, events are sent to the integration component in order to provide integration possibilities within other applications or tools.

Infor provides integration to the customer's existing authentication infrastructure via ADFS / SAML 2.0. Access to the system is restricted by individual user access IDs and passwords; each user has a unique login/password combination.

Application access (authentication and authorization) is managed by customer security officers. Applications are configured to leverage the customer's corporate directory server, and all password policies in place for that server (password complexity, maximum and minimum age, etc.) are honored by the application. Administration accounts are set up by Infor for the use of client users to perform functions necessary, with the appropriate role access. Infor's system administrators are the only ones that will use remote access. All access requires two-factor authentication and is logged and monitored.

The customer is responsible for user accounts modification, new accounts, existing accounts deletion.

Infor offers a multitude of profiles for our customers. It is the responsibility of the customer to designate privileges.

Is there a feature for tracking user activities and generating audit logs?
Yes. User activities such as login, logout, timeout, etc are captured in the IFS component and can be captured in the Infor Data Lake also.

Basic Application level logging can be captured if the auditing feature in the application is enabled. Application related logs are within the application and remain within the application DB, such logs are related to Licensee's activities. These are available to Licensee admin at all times and is not stored outside of the tenants allocated to Licensee.

For infrastructure related logs hosting the tenants, Infor has implemented a centralized Security Information and Event Management (SIEM) solution which copies all system logs to an immutable location for analysis and reporting. The level of logs includes access to systems and database and records of the activities that were performed. These are only shared with Licensee to support any relevant active security incident investigation. Type of logs selected to be retained is as per Infor discretion.