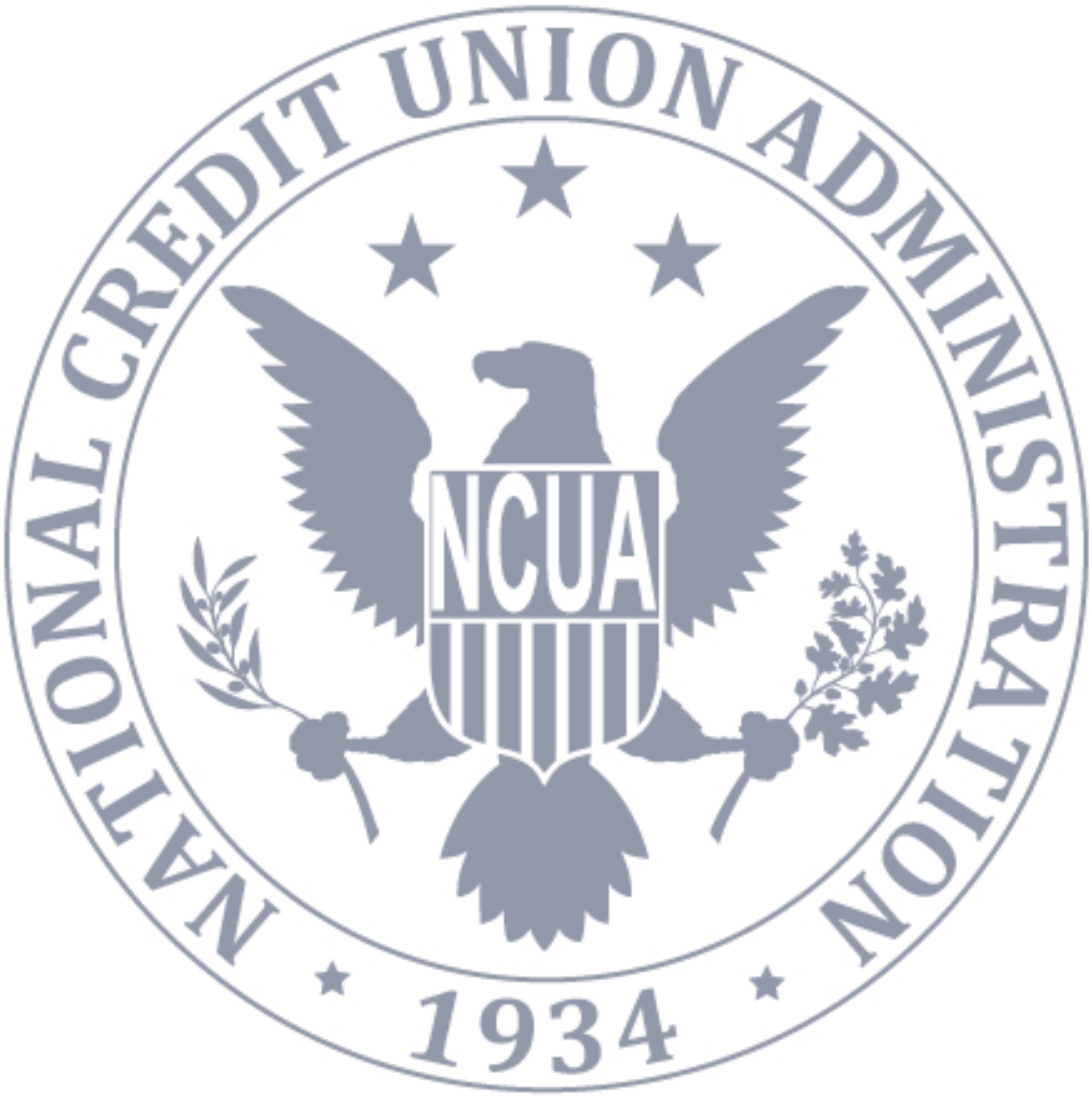
NCUA
National Credit Union Administration

Privacy Impact Assessment for Concur Technologies, Inc.

Fiscal Year 2018

[This page intentionally left blank]



PIA for Concur Technologies, Inc. • FY2018

Table of Contents

About this Document

A Privacy Impact Assessment (PIA) is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

Program offices and system owners are required to complete a PIA whenever they develop, procure, or use information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[1] Completion of a PIA is a precondition for the issuance of an authorization to operate.[2]

A PIA form (and an automatic workflow and streamlined review and approval process) has been developed for consistency and ease of use. The form, and additional guidance about PIAs, is available for NCUA staff on the Privacy team's intranet site.

The Privacy team is responsible for reviewing and approving PIAs, preparing approved PIAs for publication, and otherwise managing the PIA process.

Basic Information about the System

System Name: Concur Technologies, Inc.

NCUA Office Owner: OCFO

System Manager: [redacted]

[1] 44 U.S.C. § 3501, note; Pub. L. 107–347, § 208(b).
[2] OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).

Authority

NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII if it has authority to do so, and such authority should be identified in the appropriate notice.

Authority for the System

5 U.S.C. §§ 5701—5709, 5 U.S.C. §§ 5721—5739

Purpose Specification and Use Limitation

NCUA should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Purpose of the System

- Provide users with a mean to create travel requests and/or book travels (flight, hotels, car rentals…) easily with the capability of communicating and/or enforcing a travel policy
- Provide users with means to collect and centralize travel-related information
- Provide users with a mean to create expense reports easily with the capability of communicating and/or enforcing an expense policy
- Provide the organization with a mean to control, audit, approve, reject, and archive, bookings, and expense reports

Intended Use of the PII Collected

NCUA uses Concur as a secure End-to-End Travel Expense Management System via a secure Web portal environment. Concur is used to track and manage travel expenses.

Sharing of the PII

Concur transmits traveler profile and itinerary information to Global Distribution System providers (Sabre Travel Network) in connection with any travel that is booked on behalf of a customer employee.

Minimization

NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.

Types of PII Collected

Concur collects only the minimum necessary PII and uses it only for agreed upon purposes. Concur receives the following information from NCUA via Concur/CHRIS (HR system) interface and also from NCUA employees:

- Employee name
- User ID
- Password (optional, depends on the plan chosen for account provisioning)
- Password hint (if provided by end user) Corporate credit card number (optional, depends on the plan chosen for account provisioning)
- Bank account number (optional, depends on methods used for out-of-pocket reimbursement)
- Corporate credit card number and expiration date
- Passport number
- Frequent flyer / traveler membership numbers / traveler preferences
- Contact information (address, telephone, email, emergency contact)

Individual Participation

NCUA should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

Opportunity for Consent

Individuals consent to their personally identifiable information being stored in this system.

Procedures to Address Individuals' Privacy Related Complaints and Inquiries

The Privacy team knows that complaints, concerns, and questions from individuals can be a valuable source of input that improves operational models, uses of technology, data collection practices, and privacy safeguards. To facilitate this type of feedback, the Privacy team has established the Privacy Complaint Process to receive and respond to complaints, concerns, and questions from individuals about NCUA's privacy practices. The process is described on NCUA's privacy website. The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.

Quality and Integrity

NCUA should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

Source of the PII

Agency and its employees. Concur receives the following information from NCUA via Concur/CHRIS (HR system) interface and also from NCUA employees:

- Employee name (NCUA)
- User ID (NCUA)
- Password (optional, depends on the plan chosen for account provisioning) (Employee)
- Password hint (if provided by end user) (Employee)
- Bank account number (optional, depends on methods used for out-of-pocket reimbursement) (Employee)
- Corporate credit card number and expiration date (Employee)
- Passport number (Employee)
- Frequent flyer / traveler membership numbers / traveler preferences (Employee)
- Contact information (address, telephone, email, emergency contact) (Employee)

Security

NCUA should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

Safeguards

Concur protects sensitive information in Concur services so that it is accessible to authorized persons only as needed. Customer data is not stored in web servers or application servers, but only in back end database servers. Concur minimizes exposure of PII data by ensuring that such data is only present on any mid-tier server for just the duration of the transaction. User state is stored at the RDBMS level, and no data remains at the mid-tier servers after the completion of the transaction.
Concur has implemented the following safeguards related to Personally Identifiable Information (PII):

- Encrypted when transmitted over public networks
- Encrypted when stored in databases and flat files
- Encryption of e-mail messages sent from Concur Premium to customers
- Accessible only by vetted, authorized personnel
- Storage of PII prohibited on Concur workstations, mobile devices, and portable storage devices
- Published privacy policies
- Security Audits

Concur undertakes several external security audits each year, many of which are directly related to the security controls described in the previous section. These security audits include:

- PCI DSS performed by a Qualified Security Assessor (QSA)
- SOC 1 (SSAE16 / ISAE3402) performed by a U.S. public accounting firm
- ISO 27001 and ISO 20000 performed by an organization accredited to certify organizations to these and other standards
- SOX (Sarbanes Oxley) performed by a U.S. public accounting firm

Transparency

NCUA should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

Applicable SORN

This system is covered by NCUA-4.

Availability of Privacy Notices

The SORN and PIA for the Concur Technologies, Inc. are publicly available on the privacy page of NCUA's website.

Accountability

> *NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. NCUA should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.*

Compliance with the Fair Information Privacy Principles

As evidenced by this PIA (and the other information publicly available on the privacy page of NCUA's website), NCUA is committed to achieving and maintaining compliance with the Fair Information Privacy Principles.

Roles and Responsibilities of NCUA Staff

As detailed in the NCUA Computer Security Rules of Behavior, all NCUA staff are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Staff must protect all PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.

To protect PII, staff must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what they need to complete their job duties, and must not disclose PII to unauthorized parties. Managers are also responsible for providing their subordinates with context-specific practical guidance about protecting PII.

All NCUA staff are required to review and acknowledge receipt and acceptance of the Rules of Behavior upon gaining access to NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.[3]

Training

Together with the Office of Human Resources, the Privacy team ensures that new employees complete mandatory privacy training, and all existing employees and contractor employees complete privacy refresher training once every fiscal year. NCUA staff electronically certify acceptance of their privacy responsibilities as a part of annual privacy refresher training. The Privacy team keeps auditable records of completion of all mandatory trainings.

Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy on 9/28/17.

[3] 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.