ORACLE
Cloud

Product/Service Feature Guidance – Oracle Aconex Cloud Service (including Aconex add-on modules)

SEPTEMBER 2020

Disclaimer

The purpose of this document is to outline some of the product features currently available or under consideration for the Oracle service offering referenced above, with a focus on privacy and security related controls. Customers should refer to the available on-line product documentation for a more complete description of available product features and functionality.

The information contained in this document is for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, functionality, or certification or compliance status, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle. All information is provided "AS-IS", without warranty, is subject to change, and is confidential information under your agreement with Oracle.

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation, including through the use of any vendor's products or services.

Privacy Features	Description	Oracle Documentation
Data Minimization	Granular Access: Configured Job Roles are provided but not configurable by customers. Purging: No specific functionality provided by the product/service.	Manage Roles and Permissions https://help.aconex.com/aconex/our-main-application/aconex-admin-kit/admin-kit-org-admins/manage-user-roles-permissions
Data Deletion at Contract Term or Termination	Aconex Contracts - Data may be deleted 1 year after the termination of the services. Oracle Contracts - Data is deleted 180 days after the termination of the services. Data deletion can be performed at any time with a Support Desk request by authorized customer representatives with required approvals other customers on the project.	Oracle GBU Pillar Policy https://www.oracle.com/corporate/contracts/cloud-services/
Data Portability	The application currently supports bulk export of project/user data functionality via the UI and via APIs Aconex also supports an option to have a Local Copy Archive of ALL the Project Data. Customers can currently export a subset of their data in machine readable formats.	Data Export Instructions https://help.aconex.com/search?search_api_views_fulltext=export https://help.aconex.com/search?search_api_views_fulltext=export+excel
End-user Access and Other Requests	Customer end users must request access from the Customer Administrator to originally provision and subsequent access changes. All customer data is accessible via the UI and reporting interface to the customer.	Mail and Document Access https://help.aconex.com/aconex/our-main-application/aconex-essentials/mail-essentials/who-can-see-mail-documents

Right to Erasure and/or Right to be Forgotten	Users can correct/edit selected user profile data e.g. update contact details. Changes to the user profiled directly update the Global Directory. Personal Information can be amended in the user profile and deleted by a user at any time except for an email ID. A user can request to be deleted via their Admin to Oracle: User account will be disabled (no longer accessible). Also, a User can be removed from the Global Directory on request or after a period of inactivity and the account no longer being associated with a contracted project, it will be rendered unrecoverable. Correction or removal of non-user editable data/documents can only be done on authorized written request to the Aconex Service Desk. Not all data is editable/removable e.g. uploaded contracts documents, logs etc.	Updating User Contact Details https://help.aconex.com/aconex/our-main-application/using-aconex/aconex-account/personal-settings/update-contact-details
Notice and Consent	In general, specific functionality is not provided by this product/service for the customer to push out consent notices. Global Directory does have Opt-In and Opt-Out functionality.	
Availability	Aconex provides daily and incremental backups for all customer data and also continuous replication of the database to the secondary Disaster Recovery site.	

Tracking Technologies	The service only uses functional (no tracking) non-persistent cookies for maintaining the login session and no third-party cookies. The cookies, if not set, would have a detrimental impact on the user experience, as they maintain the logged in session identifier. The cookies are set based on the end user successfully logging into the system; and are removed when the session expires or the browser is closed.	
Security Features	**Description**	**Oracle Documentation**
Multi-factor authentication	Aconex supports SSO and two-factor authentication functionality.	Manage Roles and Permissions Manage 2-Step Verification and Single Sign On https://help.aconex.com/aconex/our-main-application/aconex-admin-kit/admin-kit-org-admins/manage-user-roles-permissions
IP white-listing	No specific functionality provided by this product/service.	
Separation of duties	The service supports a Role Based Access Control (RBAC) model to set up authorization policies for users. These policies control the functionality available to users.	Default User Role Settings https://help.aconex.com/aconex/our-main-application/aconex-admin-kit/admin-kit-org-admins/manage-user-roles-permissions/default-user-role-settings

Flagging Special Categories of Data	Aconex allows the use of restricted fields in Mail for input of structured notes that only a specific organization can see. Confidentiality of Documents features allow users to restrict the visibility of documents and the data to a list of individuals specifically granted the right to view the document. Confidentiality of Mails: For sensitive mail that only certain users should have access to, they can be marked as confidential before sending it.	Restricted fields https://help.aconex.com/aconex/our-main-application/aconex-admin-kit/project-admin-kit/project-setup-guide/prepare-use-mail-forms-restricted-fields-project Confidentiality of Documents https://help.aconex.com/aconex/our-main-application/using-aconex/working-documents/advanced-tasks-documents/make-document-register-confidential Confidentiality of Mail https://help.aconex.com/aconex/our-main-application/using-aconex/using-project-mail/create-send-mail/sending-confidential-mail
Separate auditing and "detective control" privileges	No specific functionality provided by this product/service.	
Features Limiting Oracle's access to customer data	Oracle users must be granted permission to the Aconex system by the Customer Administrator. The service supports a Role Based Access Control (RBAC) model to set up authorization policies for users. These policies control the functionality available to users. Users are provided role based permissions based on the function they are performing on behalf of the customer within Aconex.	Oracle Hosting and Delivery Policy – System and Data Access https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html

Encryption	Data In-Transit: Aconex uses signed 2048-bit SSL keys for all HTTPS traffic to ensure all information is encrypted across the public internet while in-transit. Data At Rest: Client data can be protected at select primary sites by an encryption-at-rest solution in select primary sites for an additional cost.	
Anonymization	No specific functionality provided by this product/service.	
Pseudonymization	No specific functionality provided by this product/service.	
Data Masking	No specific functionality provided by this product/service.	
Truncation	No specific functionality provided by this product/service.	
Tokenization	No specific functionality provided by this product/service.	
Logging	Aconex application event logs are retained but not accessible from the application and are currently purged every three months. Logging is not configurable by the customer. The sending of event logs to external destinations (including write-once storage) is not supported.	