



John Huges
 #440, Ridge Dr
 A/C # 0012380
 SSN 550-55-5500



John Doe
 #XXX, *%#@e
 A/C %XX*XX%
 SSN XXX-XX-XXXX

Automated Data Masking Pack in Non-Production With Solix EDMS KnowledgeBase for Oracle E-Business Suite

Privacy Needs Active Protection

Ensuring data privacy is the law in many regulated industries; however protecting sensitive data is good business practice. Leaking confidential customer, financial and employee data can lead to significant financial, legal and reputational losses. While data protection is strongly enforced in production systems, the same rigor is often not applied to non-production test and development systems.

Regulations are on the Rise

Oracle E-Business Suite has thousands of implementations storing sensitive information for millions of end users and businesses worldwide. These systems are constantly under the scrutiny of auditors looking for the potential risk for privacy weaknesses. This new scrutiny is forcing organizations to take personal information security and data privacy more seriously than in the past. Since November 2007, over 100 data breaches have been reported to the U.K. data protection authorities alone. In the EU, the European Data Protection Directive (Directive95/46/EC) states that Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life. The provision also assigns liability to companies who misuse data and allows that any person who has suffered damage as a result of an unlawful data processing operation to receive compensation from the violating party.

The United States is not far behind the EU with privacy legislation of its own. The Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and the Fair Right to Financial Privacy Act are just a few of the Federal privacy laws being enacted and many states are enacting their own state privacy regulations

Oracle E-Business Suite Testing Challenges

Privacy directives often state that data cannot be used for purposes other than for what it was collected and that the data must be accurate and processed securely. The issue for Oracle E-Business Suite administrators is that live data from their own production systems is the best set of data to use in their test and development environments. But it is this use of application data in non-production that potentially exposes organization to wide scale data theft. Database Administrators (DBA) tasked with making full clones of live production databases with sensitive data are able to do so bypassing the usual production level security measures. With this data being copied many times over, the security risks are obvious. Test and Development clones are a necessary part of any application environment but data masking or encryption techniques need to be applied to ensure that data is not leaked outside the organization.



Solix EDMS KnowledgeBase and Oracle Data Masking Pack

Pre-Configured Masking

Ships with pre-configured algorithms to ensure data privacy for popular Oracle E-Business Suite modules that contain highly sensitive data.

Obscures Actual Data

Data obfuscation ensures test and development users are unable to determine the actual or original values through one way data scrambling, masking and/or random data generation.

Supports Encryption and Decryption

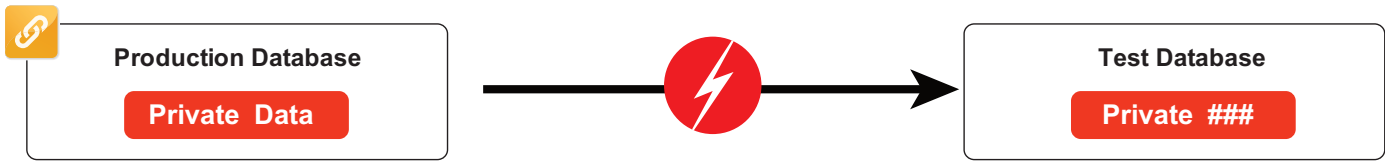
The ability to support encryption/decryption is important when the application server incorporates encryption during reads and writes.

Maintains Transaction Relational Integrity

When sensitive data is a Primary/Foreign Key or maintains a columnar reference, transactional relational integrity is required.

Easy to Use and to Set up Policies

Through a separate policy manager, those who define the policies are different than those who execute them ensuring segregation of duties.



Customer Jane Moore	Credit Card 4145 1230 0000 6012	Shuffling	Mary 23456	Customer #\$%^	Credit Card 4531 0000 %\$#! 6012
Name Joe	Phone 555 2320	Masking	xxx999999999	Customer XXX	Phone 999-999-9999
Name Davie	Address 32 Elm St	Substitution	Mfdy64528798	Customer Mary	Address 65 FrEds
Name Sue	SSN 654599876	Encryption/Decryption	@#%fah^&*AS%^345	Customer Jane Moore	SSN @#%-&*-1111
Name Mary	Zip Code 26453	Nulling	#####	Customer #####	Employer #####
Name Mary	CCN 555526453...	Custom	Custom Custom Algorithm	Customer	CCN

Data Privacy and Oracle E-Business Suite

Oracle E-Business Suite contains organizations’ transactional and historical records. Oracle Human Resources Management System and Oracle Financials contain salary, employee social security (national identifiers) and employee numbers, commission compensation, health records, HR actions and more. It is a smorgasbord of private information that is subject to company and governmental privacy regulations.

Organizations that are outsourcing their testing operations overseas must also comply with data transfer rules that prohibit data outside of the host country unless there are provisions to handle the data as if it were in the home country. While offshore testing is allowed, the liability for breach of data security and privacy still lies in the organization’s home country.

Managing Risk and Privacy

To protect organizations against unauthorized access to sensitive data that can result in regulatory sanctions and impact corporate reputations, IT organizations need to focus on risk avoidance, awareness and mitigation. Using scrambled, encrypted or otherwise masked data on sensitive fields can avoid the risk of compromising personal data. Sensitive personal data is loosely defined as data that can identify an individual; masking names, addresses, phone and social security numbers eliminate the personal nature of the data in test and development environments.

CIO’s and senior IT management need to better understand the rules and regulations governing data privacy and implement active security policies that ensure data is secure by masking data wherever possible.

When masking is not an option, documentation and a complete auditing system is required to prove compliance.

Solix EDMS KnowledgeBase for Oracle E-Business Suite

Oracle Data Masking Pack for Enterprise Manager and Solix EDMS KnowledgeBase(KB) for Oracle E-Business Suite effectively scrambles, encrypts, or masks sensitive data from Oracle E-Business Suite to depersonalize the data while ensuring the data format remains valid for testing purposes. For example, data relational integrity and formats are accurate to account for proper vacation accrual or pension benefits calculations and credit card formatting is consistent with the Visa or Mastercard system identifiers. The Solix EDMS KB pre-packages the specific algorithms to handle the formats required for creating a valid test environment for Oracle E-Business Suite while ensuring privacy.

Companies that are storing employee, consumer, or company information should have concerns about the privacy controls in their organizations and take steps to secure it. The integrated solution of Oracle Data Masking and Solix Data Privacy Pack for Oracle E-Business Suite is a low cost, rapidly deployable solution for ensuring privacy in your test and development environment.

Complete Application LifeCycle Management

The integration of Solix EDMS with Oracle Enterprise Manager is to ensure non-production databases are not the source of data leaks. It ensures an end-to-end monitoring of data obfuscation, system provisioning, system testing and diagnostics and tuning.