|  |
| --- |
| QARMS  MySQL Encryption  Version 1.1 |

|  |  |
| --- | --- |
| Document Type | Information Security – Personal Data Protection |
| Prepared By | Ravi M |
| Prepared On | 22-Mar-2021 |

**Glossary**

| Version | Change Description |
| --- | --- |
| GDPR | Global Data Protection Regulation |
| BI | Business Intelligence |
| TBD | To Be Done / Discussed |

**VERSION CONTROL**

| Version | Change Description | Updated By | Date | | Reviewed By |
| --- | --- | --- | --- | --- | --- |
| 1.0 | Initial version for review | Ravi M | 22-Mar-2021 | Lokesh | |
| 1.1 | Done the alignment changes based  on the feedback given by Lokesh | Ravi M | 22-Mar-2021 | Lokesh | |

# Change Details

|  | Details |
| --- | --- |
| Type | Enhancement |
| Description | Information Security – Personal Data Protection |
| Impact | Medium |
| Raised by & On | IT Infra on 18-Feb-2021 |
| Impact Application(s) | QARMS |

# Current Behaviour

There is no current behavior.

# Expected Behaviour

The objective of this CR is to encrypt the VAS Partnered Personal Data Tables in QARMS.

# What is InnoDB Tablespace Encryption?

* InnoDB tablespace encryption is designed to provide customers with the ability to transparently apply encryption within the database without impacting existing applications.
* Returning data in encrypted format would break most existing applications.

# Why InnoDB Tablespace Encryption ?

* This encryption supports the Advanced Encryption Standard (AES256) block-based encryption algorithm.
* It uses Electronic Codebook (ECB) block encryption mode for tablespace key encryption and Cipher Block Chaining
* (CBC) block encryption mode for data encryption.

# How to Encrypt ?

* To encrypt data in an InnoDB tablespace, run ALTER TABLE tbl\_name ENCRYPTION='Y'. InnoDB tablespace encryption is only supported with file-per-table tablespaces.

# Pros

* InnoDB tablespace encryption provides the benefit of encryption without the overhead associated with traditional database encryption solutions, which would typically require expensive and substantial changes to applications, database triggers, and views.

# Limitations

* The InnoDB tablespace encryption feature in non-enterprise editions of MySQL use the keyring file plugin for encryption key management, which is not intended as a regulatory compliance solution. Security standards such as PCI, FIPS, and others require use of key management systems to secure, manage, and protect encryption keys in key vaults or hardware security modules (HSMs).

# 1. Implementation Steps

**Step 1:** Ensure the Current MySQL Version greater than **5.7**

# Why MySQL Upgradation?

MySQL v5.6 does not support the InnoDB tablespace encryption feature.The v5.6 documentation does not include the encryption option.

**Step 2:** Add the following highlighted line in my.cnf file under mysqld "early-plugin-load=keyring\_file.so"

**Step 3:** Check the plugin isntalled status using following query

SELECT PLUGIN\_NAME, PLUGIN\_STATUS

FROM INFORMATION\_SCHEMA.PLUGINS

WHERE PLUGIN\_NAME LIKE 'keyring%';

**Step 4:** Encrypt table using following query

ALTER TABLE arms\_cfg\_agent ENCRYPTION='Y';

ALTER TABLE customer ENCRYPTION='Y';

ALTER TABLE qarms\_cfg\_ops\_sftp\_configuration ENCRYPTION='Y';

ALTER TABLE qarms\_cfg\_qic\_configurations ENCRYPTION='Y';

ALTER TABLE qarms\_cfg\_shipment\_sftp\_configuration ENCRYPTION='Y';

ALTER TABLE qarms\_cfg\_vfone\_sftp\_configuration ENCRYPTION='Y';

ALTER TABLE qarms\_mas\_cbq\_voucher ENCRYPTION='Y';

ALTER TABLE qarms\_mas\_sim\_shipping\_inventory ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_cbq\_details ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_cbq\_update\_ibanno ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_gibl\_details ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_gibl\_update\_accno ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_mybook\_details ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_service\_telecom\_details ENCRYPTION='Y';

ALTER TABLE qarms\_trn\_vodafone\_api\_tracking ENCRYPTION='Y';

ALTER TABLE user ENCRYPTION='Y';

**Step 5:** Execute the following query to check the encrypted tables

SELECT TABLE\_SCHEMA, TABLE\_NAME, CREATE\_OPTIONS FROM INFORMATION\_SCHEMA.TABLES WHERE CREATE\_OPTIONS LIKE '%ENCRYPTION="Y"%';

# 2. Implementation Plan - UAT

* Backing up the current QARMS UAT MySQL Dump;
* Do the encryptions for the required tables;
* Ask them to share results once implemented;
* Targeted to Implement in UAT 26-Mar-21;

# 3. Implementation Plan - Live

* TBD based on Implementation in UAT

# 4.Business Requirement section

* To comply with the revised EU Data Protection regulation (GDPR), all personal and sensitive data of the applicants shall be encrypted and saved in the QARMS DB for security reasons. At the QARMS front end, the user shall be able to see these data in the decrypted form.
* Reference Section