DATA ENCRYPTION SECURITY POLICY

PURPOSE:

The purpose of this document is to provide the RCMS organization with the information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure Legally/Contractually Restricted Information (Sensitive Data) (refer to RCMS – Data Access Policy).

In Worldwide any data can be protected at three different stages which can be at, **Data at rest** which includes the data residing on a wide variety of computer storage and electronic devices, such as network shares, backup storage, hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, smart phones and others, secondly **Data in motion** refers mainly to the data moving through the network and finally when the **Data in use** which includes the data on a computer which is being analyzed or worked on, including creation, retrieval, modification, deletion, saving and printing.

And in our Organization we have chosen the responsibility to protect the **Data at rest** in order to avoid information leakage in primary stage.

SCOPE:

This information assurance policy applies to all our organization's workforce members who have contact or potentially may have contact with this organization's data, applications, and computing resources.

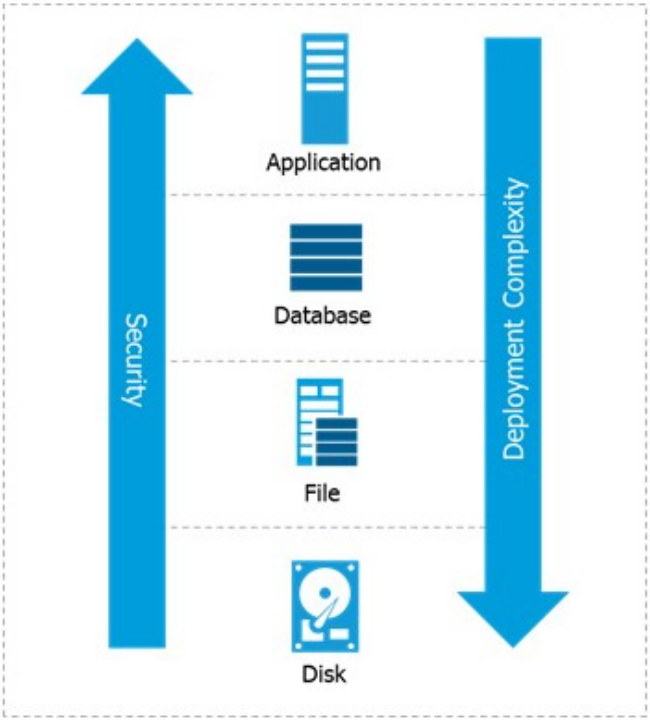
Yubikey:

Data encryption at rest is a mandatory step toward data privacy, compliance, and data sovereignty. We use yubikey as the Encryption product to encrypt and decrypt the data which we protect. The yubikey is managed by our Chief Executive Officer as he is the concerned person who has the key used in a storage encryption solution are secured and managed properly to support the security of the solution.

This process flow is been approved by our CEO and the same is been in effect from 2nd of November, 2018 and after several affirmation and validation the same will be documented and included in our IS policy on 31st of March, 2019 as per our review policy of IS policy is bi-annual, with the fulfillment and acceptance of our entire higher and superior officials and also to employees

connecting to any RCMS workforce members and network domain to clear any snags found in-between of the process.

LOGIC DIAGRAM:



Extensive key management is planned and followed which includes secure key generation, use and storage. Initially yubikey. will be vaulted and the key for that vault will be in control of the CEO. If a third party want to access our hard disc then he must follow the steps stated below for accessing our data:

Initially the Security/Linux admin must register his name and details in ledger before approaching the yubikey.

Later the security/Linux admin needs to get the key for the vault where the yubikey is been vaulted, by unlocking the vault he can able to access the yubikey where 2 key's will be available, both serves the same role one is kept as backup key for the other.

Once after the insertion of the yubikey into the system, it asks for 128 bit password to handle the hard disc, this 128 digit password is split up into 2 segments as 64 digits. This first part of 64 digits password is been controlled by Linux Admin and the second 64 digits is handled by security admin.

After successful enrollment of this 128 segment the third party can access the hard disc without any further delay.

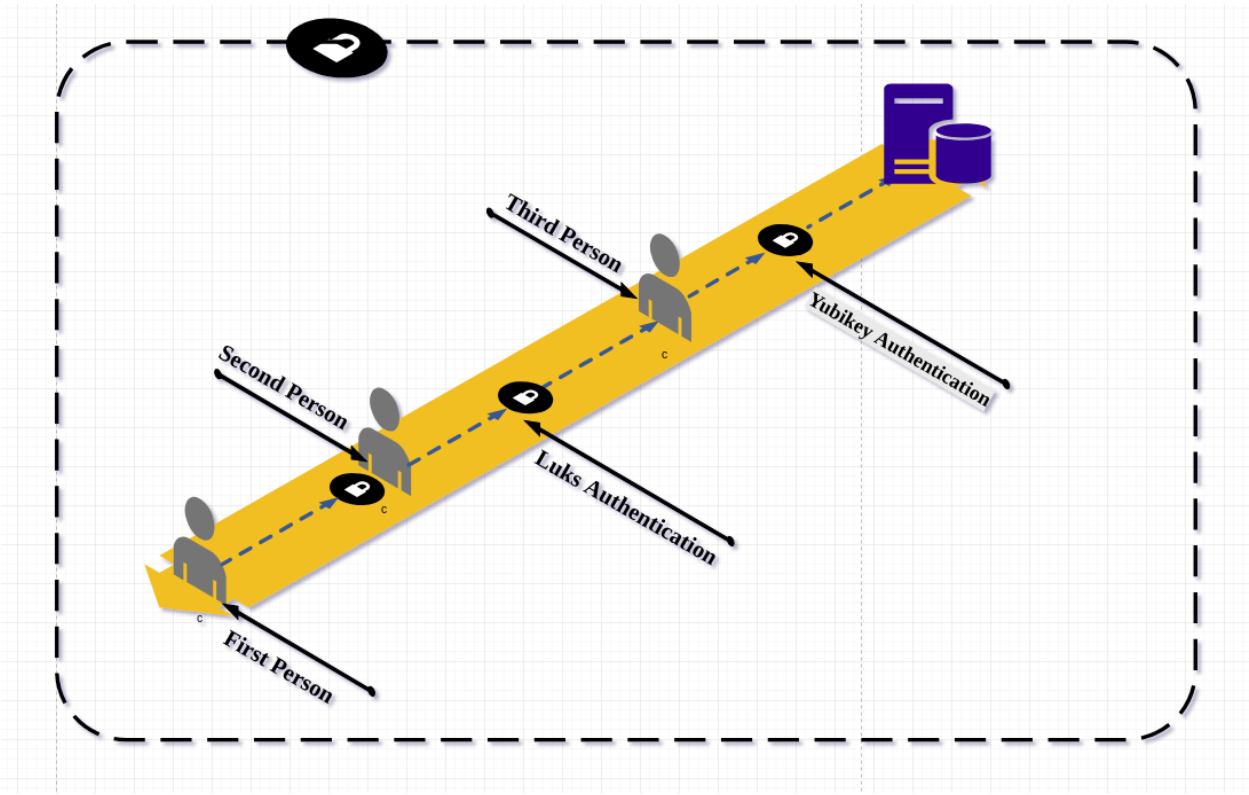


Fig: Structure representing hard disc access

After completion of the authentication process, the yubikey is returned to the CEO and the network/Linux admin should enroll the IN time of the yubikey back to the vault in the ledger.

Network/Security department will ensure that access to encryption keys is properly restricted. Authentication for each process is followed in order to gain access to keys (passwords, tokens, etc.).

PROCESS FLOW:

In order to access the Hard disc, we are using 2 levels of authentication and they are

1. LUKS **- Primary authentication**

2. YUBIKEY **- Secondary authentication**

LUKS - Primary authentication:

To encrypt the server we utilize Luks authentication and in order to access this we need 128 char to finish first level of authentication. This 128 char is splitted into 2 segments and first 64 segments is handled by Linux admin and the second 64 segments is handled by security admin

YUBIKEY - Secondary authentication:

This yubikey will be kept and handled by manager level authority. We need to finish the yubikey level of authentication to enable server login.

PROCEDURES FOLLOWED:

Once Luks is installed it will automatically deduct for LUKS password in order to Login as it encrypts entire block devices and is therefore well-suited for protecting the contents of mobile devices such as removable storage media or laptop disk drives. The underlying contents of the encrypted block device are arbitrary. This makes it useful for encrypting swap devices. This can also be useful with certain databases that use specially formatted block devices for data storage.

Administrative:

The Chief Executive Officer of this organization has the responsibility for the overall administration of this policy. Establishment of the administrative procedures for the compliance with Corporate Policies is the responsibility of the officers and the managers of this organization and all the business units.