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).
The focus of our Data Encryption Practice Standard is to set minimum encryption standards for the transmission of confidential data via the Internet, to establish rules for transmitting confidential data and to identify the roles and responsibilities of the End-User, Management and Information Services.

Scope:

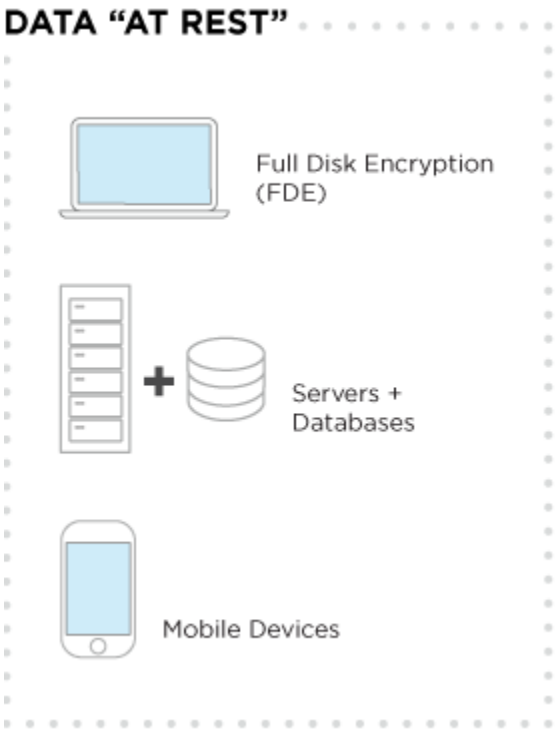
This information assurance policy applies to our organization's workforce members who have contact or potentially may have contact with this organization's data, applications, and computing resources.

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 are 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.

LOGIC DIAGRAM:



Extensive key management is planned and followed which includes secure key generation, use, storage and destruction. Considerations are made as to how these key management practices can support the recovery of encrypted data if a key is inadvertently disclosed, destroyed or becomes unavailable. Specific technical options are tied to this product which is in use in our organization.

Departments 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.). The keys themselves should be physically secured with at least two upper-level trustee's assigned access

In order to access the Server, we are using 2 levels of authentication and they are (i) LUKS (ii) YUBIKEY **i.e.., LUKS-Primary authentication and 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.

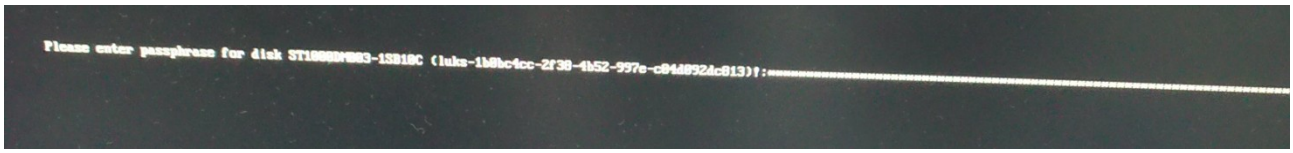
This 128 char is splitted into 2 segments and first 64 segments is handled by LINUX ADMIN and the second 64 segments is handled by SECURITY ADMIN

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:

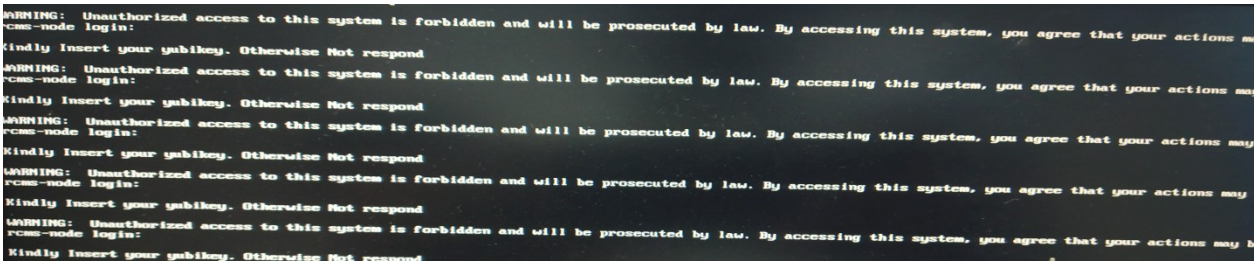
Once LUKS is installed it will automatically deduct for LUKS password in order to Login as it encrypts entire block devices and is therefore well-suited for protecting the contents of mobile devices such as removable storage media or laptop disk drives. The underlying contents of the encrypted block 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.

Below is the evidence for Luks encryption screen shot

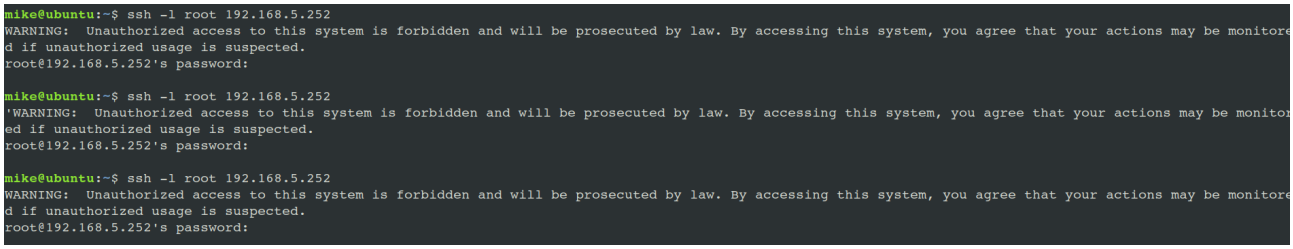


Luks password → 128 characteristics {Linux admin have 64 characteristics + security admin have 64 characteristics)

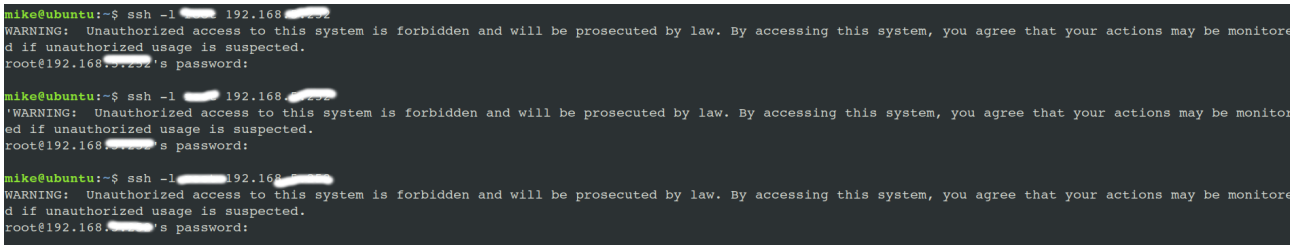
2. The below image represents the after logging in to LUKS and Waiting for Yubikey Access.



3. Yubikey Access for ssh with Password



4. If we don’t own YUBI KEY ssh will not get accessed.



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 its business units.