POLICY AND PRODCEDURE

Policy Name: Encryption Key	**Effective Date: 07/04/2016**
Policy Number: 4006	**Revision Date: 07/05/2017**
Department: IT	**Author: Daniel Mos**

PURPOSE: UnifyHR uses encryption keys to protect sensitive data. Each encryption key has a public and private key. This policy pertains to the protection of the private keys. Keeping the private keys protected is necessary to protect sensitive data.

POLICY:

Access to Private Keys (UnifyHR Application)

Access to UnifyHR's private encryption keys are limited to members of the Senior Management Group. The keys may never be distributed to anyone outside of this group.

Storage (UnifyHR Application)

The private encryption keys are stored in the production application environment, as well as one protected location outside of the production environment. The keys shall never be removed from the locations. When keys are stored inside the production environment, they should be stored in a separate layer than the data they are decrypting whenever possible, preferably separated by a firewall. The password for the key may not be stored in the same location as the key. The storage mediums must have redundancy.

Employee Keys

Employees may use individually created key pairs to exchange data with clients, upon client request. These keys may be stored on a local computer, but the password should not be stored on the same machine or location as the private key. The private key may not be distributed, and the password may not be shared with others.

PROCEDURES:

Key Generation:

Upon generation of a key pair, the private key must be moved to a protected location if the generation takes place in a location separate from the storage area, and the private key must be completely removed from the creation location. Reasonably complex passwords should be used.

Compliance

Compliance is handled by the IT team. Compliance may be performed by internal audits and review of equipment email. Exceptions to this policy must be approved by IT leadership.

Breaches

If a private key becomes compromised, a new private key must be created using the key creation policy aforementioned. All clients affected are notified, and a new public key will be distributed.

This policy shall be reviewed for language and application on an annual basis following its last revision and shall be reviewed every year thereafter.

Revision History

Version	Date	Author	Summary of Changes
1.0	12/15/2015	Daniel Mos	Original
1.1	07/05/2017	Daniel Mos	Updates for Improvements/Changes in Process
1.1	07/27/2018	Daniel Mos	Reviewed – No Changes
1.1	08/01/2019	Daniel Mos	Reviewed – No Changes

Approvals

Version	Date	Approver	Summary of Changes
1.0	07/04/2016	Chris Heinefield Craig Firestone	Original
1.1	07/05/2017	Chris Heinefield Allen Gehrki	Updates for Improvements/Changes in Process
1.1	07/27/2018	Chris Heinefield	Reviewed – No Changes
1.1	08/01/2019	Daniel Mos	Reviewed – No Changes