POLICY AND PROCEDURE

Policy Name: Access Control Policy	**Effective Date: 07/04/2016**
Policy Number: 1009	**Revision Date: 10/24/2018**
Department: Administration	**Author: Daniel Mos**

PURPOSE: All servers, applications or network devices that contain, transmit or process UnifyHR Protected Data are considered "High Security Systems". This policy outlines the access controls that apply to UnifyHR employees and vendors that connect to UnifyHR High Security Systems.

POLICY:

Access to High Security Systems will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor, with a valid business justification. Access controls to High Security Systems are implemented via an automated control system. Account creation, deletion, and modification as well as access to protected data and network resources is completed by IT.

On a regular recurring basis, IT will audit all user and administrative access to High Security Systems. Discrepancies in access will be reported to the appropriate supervisor in the responsible unit and remediated accordingly.

User Access

All users of High Security Systems will abide by the following set of rules:

- Users with access to High Security Systems will utilize a separate unique account, different from their normal account. This account will conform to the following standards:
    - The password will conform, at a minimum, to the published Password Standards.
    - Inactive accounts will be disabled after 60 days of inactivity.
    - Access will be enabled only during the time period needed and disabled when not in use.
    - Access will be monitored when account is in use.
    - Repeated access attempts will be limited by locking out the user ID after not more than 5 attempts.
    - Lockout duration must be set to a minimum of 15 minutes or until an administrator enables the user ID.
    - If a session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.
- Users will not login using generic, shared or service accounts.

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
1.0	07/05/2017	Daniel Mos	Reviewed – No Changes
1.0	07/27/2018	Daniel Mos	Reviewed – No Changes
1.1	10/24/2018	Jennifer Shaub	Added Purpose Statement
1.1	08/19/2019	Daniel Mos	Reviewed – No Changes

Approvals

Version	Date	Approver	Summary of Changes
1.0	07/04/2016	Chris Heinefield Craig Firestone	Original
1.0	07/05/2017	Chris Heinefield Allen Gehrki	Reviewed – No Changes
1.0	07/27/2018	Chris Heinefield	Reviewed – No Changes
1.1	10/24/2018	Daniel Mos	Added Purpose Statement
1.1	08/19/2019	Daniel Mos	Reviewed – No Changes