POLICY AND PROCEDURE

Policy Name: Security and Privacy Policy	**Effective Date: 07/04/2016**
Policy Number: 1005	**Revision Date: 09/04/2018**
Department: Administration	**Author: Daniel Mos**

PURPOSE: The Security and Privacy policy addresses the safeguards and guidelines used by UnifyHR to protect customer data including individually identifiable information.

POLICY:

Individually Identifiable Information

UnifyHR recognizes that the growth of online services has created many privacy concerns, particularly for consumers. These concerns focus on protecting "individually identifiable" information that an individual or customer reasonably expects to be kept private. As the term suggests, individually identifiable information is information that can be associated with a specific individual or entity, such as name, address, telephone number, e-mail address and/or information about online activities directly linked to them.

It is common practice and often a necessity for companies, governments or other organizations to collect individually identifiable information to conduct business and offer services. For example, a telecommunications provider may collect individually identifiable information during billing and providing telephone service to a customer.

UnifyHR Privacy Policy

UnifyHR has developed the following privacy policy to protect individually identifiable information. This policy covers UnifyHR and its subsidiaries and applies to all individually identifiable information that UnifyHR receives during performing its services.

Disclosure: UnifyHR will not sell, trade or disclose to third parties any individually identifiable information derived from the completion of its services (except as required by subpoena, search warrant or other legal process or in the case of imminent physical harm to the customer or others). When UnifyHR uses other agents, contractors or companies to perform services on its behalf, UnifyHR will ensure that the company protects your individually identifiable information consistent with this policy. The results of our services, along with the substantiating evidence, may be provided to the benefit plan sponsor, or designated business associate during, or at the completion of service.

Collection and Use: UnifyHR will collect and use individually identifiable information for the services UnifyHR has contracted to perform for its clients.

Security: UnifyHR has implemented technology and security features and strict policy guidelines to safeguard the privacy of your individually identifiable information from unauthorized access or improper use, and we will continue to enhance our security

@Copyright 2018 UnifyHR. All Rights Reserved.

procedures as new technology becomes available. These policies include, but are not limited to; document access logs, secured physical storage facility with multiple lock access requirements, secured server facility, employee background checks, and advanced encryption techniques

UnifyHR Information Security

UnifyHR maintains an in-depth security policy that describes all necessary procedures to maintain a high level of ongoing security. The policy discusses password policies, security log procedures, classification of vital information and how it is to be encrypted and transferred as well as defines network security administrators who review and approve all of the above information.

UnifyHR encrypts all passwords. Minimum password length and complexity is enforced. UnifyHR utilizes roles-based security to ensure data confidentiality and security. Application users are only provided access to data on an as-needed basis to perform the functions related to their position. User authentication takes place via a backend process that validates user, client access, and password information. Generic accounts are not allowed for login. Generic accounts will be deactivated when possible. In the production environment, an IDS system will be in place to send alerts when a generic account is used for login.

UnifyHR performs periodic recurring documented review of data access logs to ensure data access is being performed by appropriate parties with a current need of access.

All customer data the system utilizes shall be encrypted while in transit and at rest. Data will only be decrypted as needed and temporarily. Prior to deletion, data will be ensured to be in an encrypted state. Customer data will never reside in a non-production environment (including test and development environments.)

Production system uses a multi-tier structure with firewalls between each tier ensure utmost security. Long term data storage never takes place in an internet facing tier.

UnifyHR takes system security, privacy, and reliability very seriously. The UnifyHR electronic delivery mechanisms are a key differentiator in the industry, and UnifyHR seeks to ensure high levels of availability of these systems. The UnifyHR strategy is to anticipate potential problems and resolve them in advance.

Security

UnifyHR has policies and procedures in place to address all recommended security incidents. We have alarms configured to notify us when any unauthorized network intrusions or other network security related events occur. We also have assigned personnel who check security logs daily for violations and anomalies. Clients would be immediately contacted and informed of the security violation, and UnifyHR would take all necessary steps to contain the problem. ID logs and other security transaction logs are used to identify invalid access attempts and other security related incidents, and to help us track down and resolve security related problems as required. Log monitoring occurs daily with all vital data storage servers. Multiple contacts are notified immediately, and emergency action procedures go into effect when an error is detected. Logs are backed up and stored in a geographically distinct location for future need as required.

We use multiple enterprise level products to manage and protect our data and users from malicious infections. We use an industry grade anti-virus server and software products to perform on demand and daily monitoring of worms and viruses. Software automatically updates virus definition files daily, and UnifyHR performs full weekly scans of all files and e-mails. Exception reports notify network administrators of any virus issues for immediate research and action. We also use industry recommended spy ware products to protect our web users from the influx of spam and spy ware.

UnifyHR also utilizes enterprise level intrusion detection software. This software automatically notifies UnifyHR personnel when suspicious behavior has occurred.

UnifyHR engages a 3rd party security company, Qualys, to perform vulnerability testing and malware scanning on our software and equipment. Vulnerability testing is performed after every software release and on a regularly recurring basis. Any risks that are identified are corrected and the corrections are verified with another vulnerability scan. Qualys also performs automated malware scans on our software and equipment on a recurring basis, and they send reports on their findings. Any new hardware or software added to the environment would be subject to the vulnerability testing and malware scanning.

Data Transmission

Data transmission is secured using unique, individual FTPS/ SFTP sites per client along with file encryption. A public PGP encryption key is delivered to each client to encrypt the data file prior to transmission. The file is delivered to a password protected site in UnifyHR's secure data center. An automated process moves the file off the site to a secure location immediately after it is received, ensuring a minimal amount of time the encrypted file remains on the site.

Data transmission from UnifyHR to our clients can be performed in two different ways. First, data can be pulled directly from our web application which uses HTTPS to encrypt the data. This transmission may be scheduled or on demand at the client's discretion. Second, data can be pulled from our secure site. Both the methods utilize unique user names, passwords, and data expiration using client specified timeframes.

UnifyHR also uses secure email and opportunistic TLS for client email communications.

Digital Data

Upon completion of services UnifyHR will have collected significant amounts of information about the client's employees and employees' dependents. This information will exist in both electronic data interface (EDI) files as well as database records within the UnifyHR proprietary platform.

For each of these types of records the client may choose to have nothing done and UnifyHR will continue to house and protect the data until which time UnifyHR. All data will continue to be stored encrypted using the same standards outlined previously.

The client may also opt for UnifyHR to perform an encryption of relevant data at a database field level. This encryption will be performed using a public/private encryption scheme. It will be the client's responsibility to provide UnifyHR with the public key to be used to perform the encryption. The encryption will also be applied to all EDI files containing personal demographic information. These fields include (but are not limited to) first name, last name, address (excluding state and zip code), social security number, member number, employee identification number, etc. Once the data is encrypted the contents of these fields will be inaccessible to anyone, including UnifyHR staff.

At the clients request the data may be decrypted, upon presentation of the private key to the UnifyHR staff. Clients must recognize that loss of the private key will make decryption impossible and the individual results will no longer be available for review. Clients must also recognize that encrypting and decrypting data is a labor and time intensive process. Beyond the initial encryption clients will be charged an administrative hourly fee equal to the current UnifyHR custom data conversion rate.

Security Training

Security, privacy and related policies and procedures are the subject of formal training presented by UnifyHR Security Privacy Officers. All employees must complete the Security training annually and new employees within two weeks from the hire date. After the training, the employee is required to pass the Security test. In the event of a change to the policy and procedures, training may be scheduled earlier.

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

@Copyright 2018 UnifyHR. All Rights Reserved.

Revision History

Version	Date	Author	Summary of Changes
1.0	12/15/2015	Daniel Mos	Original
1.1	07/05/2017	Danny Mos	Updates for improvements/changes in process
1.2	08/17/2018	Jennifer Shaub	Added language for generic accounts, data access log reviews, security training
1.2	07/30/2019	Jennifer Shaub	Reviewed – No Changes
1.3	08/19/2019	Daniel Mos	Updated Security section regarding scans on software and equipment

Approvals

Version	Date	Approver(s)	Summary of Changes
1.0	07/04/2016	Craig Firestone Daniel Mos Chris Heinefield	Original
1.1	07/05/2017	Danny Mos Chris Heinefield Allen Gehrki	Updates for improvements/changes in process
1.2	09/04/2018	Danny Mos Chris Heinefield Allen Gehrki	Added language for generic accounts, data access log reviews, security training
1.2	07/30/2019	Allen Gehrki Chris Heinefield	Reviewed – No Changes
1.3	08/19/2019	Daniel Mos	Updated Security section regarding scans on software and equipment