CONFIDENTIALITY POLICY AND PROCEDURE

Policy Name: Confidentiality	**Effective Date: 04/01/2016**
Policy Number: 1002	**Revision Date: 07/30/2019**
Department: Administration	**Author: Craig Firestone**

POLICY: This policy applies to all UnifyHR facilities, employees, contractors, consultants and any other permitted visitors who have access to UnifyHR facilities.

PURPOSE: Our company Confidentiality Policy addresses limits and prohibitions on the disclosure of important information that the company holds. During the course of everyday business, employees will unavoidably receive and handle personal and private information about clients, partners and the company. This policy is designed to set the rules that serve to ensure the confidentiality of this information.

PROCEDURES:

Information that the company considers confidential and proprietary is undisclosed, valuable, expensive and/or easily replicated. More specifically, information that is classified as confidential includes, but is not limited to:

- Customer lists (existing and prospective)
- Data of Customers/Partners/Vendors
- Trade secrets
- Private deals
- Unpublished financial information
- Processes, methods and know-how
- Patents, formulas or new technologies
- Pricing/marketing and other undisclosed strategies or tactics
- Unpublished goals, forecasts or initiatives that are marked as confidential
- Data entrusted to the company by external parties
- Documents, processes or other elements explicitly marked as confidential
- Any other knowledge acquired by employees during their employment

All these types of information must be protected for different reasons – some may be legally binding (e.g. sensitive data) and some constitute assets of UnifyHR representing a competitive advantage (e.g. business processes). The disclosure of some kinds of information may expose the company to increased risk such as specific trade secrets, while for others the result could be the loss of important partners or diminished reputation.

In the course of their employment, employees will have various levels of authorized access to confidential information so as to conduct their business and perform their job duties. When they do so, the following rules strictly apply:

- No amount of information will be disseminated to anyone outside of the organization
- The disclosure of information inside the organization will be limited to those with authorized access and legitimate reason to require that information
- The information will not be used for the personal benefit or profit of the employee or any other except the company
- The employee will have access only to the amount and type of information required for the completion of their job responsibilities and no more
- Employees must limit to a minimum the occasions when they take confidential information out of the office
- When perusing or sharing information through electronic means, all precautionary safety measures must be in effect
- Confidential information must not be left unattended or unlocked
- Unauthorized replication of information is prohibited
- All copies of confidential documents must be shredded when no longer needed
- Upon separation of employment all confidential information must be returned or deleted from the employee's electronic devices

The company has established measures to ensure that confidential information is well protected. Those measures include, but are not limited to:

- Electronic information which includes customer or customer employee data must be encrypted
- Databases will be protected with all available security measures
- Paper documents will be safely stored (including shredding receptacles) and locked
- Authorization of access will be carefully controlled by senior management
- Employees, contractors and certain visitors must sign non-compete and/or non-disclosure agreements

Confidential information as described above may occasionally have to be disclosed for legitimate reasons, e.g. upon request of a regulatory body or for business purposes. In such cases, a strict procedure must be followed that includes; i) the explicit consent of parties involved (unless the employee is legally required to make such disclosure) and, ii) the disclosure of only relevant information and no more.

Administrative

Consistent Compliance Essential - The interconnected nature of Confidential Information, electronic communication(s), related technologies, and information systems requires that all workers observe an abundance of caution regarding Information Assets. This document defines the minimum level of due care for all workers.

Violations - The Company will take appropriate action against any employee, contractor, vendor or customer whose actions are found to violate this policy. Disciplinary actions may include, at the Company's sole discretion, oral or written reprimand, suspension or immediate termination of employment or business relationship, or any other disciplinary action or combination of disciplinary actions as deemed appropriate to the circumstances. A record of the disciplinary action will be retained in employee personnel files.

UnifyHR reserves the right to notify the appropriate law enforcement authorities of any suspected or alleged unlawful activity and to cooperate in any investigation of such activity.

Any employee who is requested to undertake an activity which he or she believes is in violation of this policy, must immediately provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department.

Risk Acceptance - In rare cases, a business case for non-compliance can be established. In all such cases, the non-compliant situation must be approved in advance through the CEO. Instances of risk acceptance will be periodically reviewed by the CEO and CIO, or Information Technology Department leadership.

Definitions

Confidential Information (Sensitive Information) – Confidential Information is any UnifyHR information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by UnifyHR from a third party, whether or not under a non-disclosure agreement, and explicitly includes customer employee data. For additional information, please refer to the Confidentiality and Non-Disclosure Agreement which you signed when you joined the company for a complete description of information considered confidential.

Information Asset – Any UnifyHR data in any form, and the equipment used to manage, process, or store UnifyHR data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Partner – Any non-employee of UnifyHR who is contractually bound to UnifyHR or to whom UnifyHR is contractually bound.

User - Any UnifyHR employee or partner who has been authorized to access any UnifyHR electronic information resource.

Visitor - Any person who does not normally work in a UnifyHR facility or who does not perform regular business functions requiring access to or entry into a UnifyHR facility.

References

None

Related Documents

UnifyHR Information Security Policy
UnifyHR Employee Handbook
- Confidentiality and Non-Disclosure of Company Information
- Confidentiality and Non-Disclosure Agreement
- Code of Business Conduct and Ethics

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	04/01/16	Craig Firestone	Original
1.0	09/05/17	Allen Gehrki	Reviewed – No Changes
1.0	09/05/17	Daniel Mos	Reviewed – No Changes
1.1	08/10/18	Jennifer Shaub	Changed Confidential Information and Invention Assignment Agreement to Confidential and Non-Disclosure Agreement
1.2	07/30/2019	Jennifer Shaub	Updated Format

Approvals

Version	Date	Author	Summary of Changes
1.0	4/01/2016	Craig Firestone	Original
1.0	09/05/2017	Allen Gehrki	Reviewed – No Content Changes
1.1	08/14/2018	Allen Gehrki	Changed Confidential Information and Invention Assignment Agreement to Confidential and Non-Disclosure Agreement
1.2	07/30/2019	Allen Gehrki Chris Heinefield	Updated Format