United for Respect / WorkIt - Privacy Statement

We are United for Respect (“UFR”, “WorkIt”, “we”, “us” and “our”). We provide an online platform for workers in the retail sector of the economy (the “Services”), including:
Our parent site at United4Respect.org (“WorkIt Site”).
Mobile application on user devices (“WorkIt App”).

Each person or entity who uses our Services is referred to as a “user” or “you” or “your”. If you subscribe to any of our Services, we will refer to you as a “registered user”. If you don’t register with us, we will refer to you as an “anonymous user”. This Privacy Statement and the Terms of Service (“Terms”) apply to each user.

This document is our statement of our privacy practices (“Privacy Statement”). Among other things, it explains how we and some of the companies we work with collect, use, share and protect personally-identifiable information, including without limitation personal

health information, personal financial information, and other sensitive information (collectively, “Personal Information”) while using our Services, and your choices about the collection, storage and use of your Personal Information.

By using our Services you understand and agree that we are providing a platform for you to receive and post information and Content, including comments and other materials (collectively, “Content”) to the Services and to share Content through the Services and through other means. This means that other users may see, use, or share any of your Content that you make publicly available through our Services.

When using our Services you consent to the collection, transfer, analysis, transformation, storage, disclosure and other uses of your information, including your Personal Information, as described in this Privacy Statement.

---

1. Information We Collect

Information you provide us directly

Registration information. When you create or modify an account or subscribe to any of our Services, you provide Personal Information to us, such as your user name, password, postal address, email address, phone number, and store affiliation.

Profile information. You may provide us with additional profile information to make public, such as your birthday, a short description of yourself, your website or a picture. You may also provide information to customize your account, such as a cell/mobile phone number for the delivery of short message system (“SMS”) or text messages. We may use your contact information to send you information about our Services or to market to you.

You may use your account settings to customize notifications from us. If you email us, we may keep your message, email address and contact information to respond to your request.

Location Information. We may ask for your geographic location information. When you post Content to our website or to social media, you may provide your location information, including global positioning system ("GPS") data or other location information embedded in or accompanying the Content (e.g., in tags or captions).

Communications between you and UFR: We may send you emails, SMS or text messages, and other electronic communications for account verification, notices of changes/updates to features of the Services, technical and security notices, and for other purposes. We may collect and store these communications.

Information we gather from your use of our Services

Emails. We collect and may save private emails sent to us by users, and we may share your emails with any third party or other user. Any public post on the Services may be viewed by any user and is public to anyone who visits the Services. You may elect to disclose certain Personal Information and information that is not Personal Information ("Non-Personal Information"). The information you submit in any public forum is not confidential or private, and UFR does not protect it. All information you choose to provide publicly, including information that identifies you or others, can be read, collected, or used by other users and by other third parties, and could be used to send you unsolicited messages and for other purposes.

Social Media. In addition to media that we control, such as the WorkIt Site and the WorkIt App, you may post comments, photographs, drawings and other Content on third-party social media, such as Facebook, Instagram and Twitter, each of which enforces its own terms of use and privacy policy for its

service. As noted in the Terms of Service, we may use and copy the Content you post. More to the point, your Content may contain Personal Information about you and other people in the form of names, email addresses and location information. You should also be aware that a photograph or drawing of a person may be Personal Information to the extent the person may be recognized in and identified by the photograph or drawing. We may collect and use Content and the Personal Information contained in the Content to market our Services.

Analytics. We use third-party analytics tools to help us measure traffic and usage trends and other Non-Personal Information for the Services. These tools collect information sent by your device or our Services, including the web pages you visit, add-ons, and other information that assists us in improving our Services. We collect and combine this analytics information with analytics information from other users so that it cannot be used to identify any particular individual user.

Metadata. Metadata is usually technical data that is associated with other data, including Content. For example, metadata can describe how, when and by whom an item of Content was collected and how that Content is formatted. WorkIt may collect and store metadata, including about each user's public posts on the Services.

Links. WorkIt may keep track of how you interact with links across our Services, including our email notifications and third-party Services by redirecting clicks or through other means. We do this to help improve our Services, to provide more relevant local data, and to be able to share aggregate click statistics such as how many times a particular link was clicked on.

Device Identifiers. We may access, collect, monitor, store on your device, or remotely store one or more "device identifiers." Device identifiers are small

data files or similar data structures stored on or associated with your computer, phone or other device, which uniquely identifies your device. A device identifier may be data stored in connection with the device hardware, data stored in connection with the device's operating system or other software, or data sent to the device by WorkIt. A device identifier may deliver information to us or to a third-party partner about how you browse and use the Services and may help us or others provide reports or personalized Content and ads. Some features of the Services may not function properly if use or availability of device identifiers is impaired or disabled.

Log Data. Our servers automatically record information ("log data") created by your use of the Services. Log Data may include information such as your Internet Protocol ("IP") address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information. We receive log data when you interact with our Services, for example, when you visit our website, sign into our Services or interact with our email notifications. WorkIt uses log data to review how we provide our Services and to measure, customize, and improve the Services.

---

2. How We Store Your Information

● We provide the Services from within the United States, and we store all Personal Information that we currently collect and retain on servers inside the United States.

● In the future, we may store Personal Information on servers located outside the United States.

● Certain types of Content you submit to us might reveal your gender, ethnic origin, nationality, age, religion, sexual orientation, or other Personal Information about you or others.

● By using our Services, or by submitting your personal Information to us, you consent to the collection, storage, processing and onward transfer of your personal Information as stated in the current version of this Privacy Statement and the current version of the Terms of Service.

---

3. How We Use Your Information

We share and use your Personal Information in the following circumstances:

Opt-in with Your Consent. We may ask for your permission to share your Personal Information with other people and organizations outside of UFR, including to help conduct studies or provide you with other services. As with any opt-in procedure, you are under no duty to agree to a request that you opt-in.

Affiliates of UFR We may share your Personal Information with our UFR affiliates (meaning entities controlled by, controlling or under common control with UFR) as necessary to provide the Services.

To Avert a Serious Threat to Health or Safety. We may use or disclose your health information when necessary to prevent a serious threat to your or your family members' health and safety or the health and safety of the public or another person.

Cookies: Cookies are unique identifiers that we transfer to your device to enable our systems to recognize your device and to provide features and remember your personalization choices. We use cookies to make it easier to access and use our Services. The help feature on most browsers will tell you

how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the website of its manufacturer. Because cookies allow you to take advantage of some of the Service's essential features, we recommend that you leave them turned on. Cookies are also used to display particular Content and to set session identifiers for visitors who voluntarily join membership areas.

Third Party Advertisers. We do not work with any third party advertisers or advertising networks and will not provide your address, email address or mobile phone number to third parties.

Opt-out Email or Postal Address. If you supply us with your postal or email address you may receive periodic mailings from us with information on new products and services or upcoming events. If you do not want to receive such mailings, please let us know by sending an email to us at the "opt-out" address in the email footer. We will be sure your name is removed from the list we use internally. Opting-out of these emails does not mean we remove your email from our system entirely, because we still retain it for login and password reset purposes.

Opt-out Telephone Numbers. Users and registered users who supply us with their mobile telephone numbers do so predominantly as a mechanism to reset forgotten passwords, however they may receive telephone calls, texts and other communications from us with information regarding new products and services or upcoming events. If you do not want to receive such telephone communication, please let us know by sending email to us at the "Contact Us" email address or writing to us at the "Contact Us" postal address. Please provide us with your exact name, company name, address and phone number. We collect the mobile phone numbers of those who

voluntarily provide them to us. Although any mobile communication from us incurs no mobile data fee levied by UFR, standard messaging and data fees may apply. Check your mobile plan for more details.

Service Providers. We employ third party companies and individuals to facilitate our Services (e.g., payment processing, maintenance, analysis, audit, marketing and development). These third parties may have limited access to your Personal Information only to perform these tasks on our behalf and are obligated to UFR not to disclose or use your Personal Information for other purposes.

Required by Law. We may access, preserve and share your Personal Information in response to a legal request (like a search warrant, court order or subpoena). We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm. Information we receive about you may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm.

National Security and Intelligence Activities. We may release your Personal Information to authorized federal officials for intelligence, counterintelligence and other national security activities when authorized by law. For example, under current law in the United States, certain federal officials may require that we provide particular information in response to a national security or related request, demand or order, and we would be required not to tell you that we complied with that request, demand or order.

Change of Control. If we sell or otherwise transfer part or the whole of UFR or our assets to another organization (e.g., a merger, acquisition, or

reorganization), your Personal Information such as user name and email address, Content and any other information collected through the Services may be among the items sold or transferred. You will continue to own your Content, but the license you granted in the Terms may be transferred to others.

Non-Personal Information. We may share aggregated information that is not personally-identifiable information ("Non-Personal Information") publicly and with publishers, researchers or connected sites. For example, we may share Non-Personal Information publicly to show trends about the general use of our Services. Non-Personal Information includes collective information about multiple users that does not reflect or reference an individually-identifiable user.

Other. In addition to some of the specific uses of information we describe in this Privacy Statement above, we may use Personal Information that we receive to:

- help you efficiently access your information after you sign in.

- remember information so you will not have to re-enter it during your visit or the next time you visit the Services.

- provide personalized Content and information to you and others, which, in the future, could include online ads or other forms of marketing.

- provide, improve, test, and monitor the effectiveness of our Services.

- develop and test new products and features.

- monitor metrics such as total number of visitors, traffic, and demographic patterns.

- diagnose or fix technology problems.

4. Your Right to Review, Request Changes, and Disclose Personal Information

Subject to applicable laws and regulations, each user and family member may inspect and receive a copy of his or her Personal Information as stored in the Services. In rare circumstances, we may deny a request along with an explanation. If we deny your request, you may request a review by another professional, who will be chosen by UFR, and we will comply with the outcome of the review.

Subject to applicable laws and regulations, the Personal Information you provide to us remains completely under your control, although each family member has his or her own rights. If you believe the Personal Information we have is incorrect or incomplete, you or the family member may in writing request an amendment to that person's Personal Information. UFR will approve or deny each request, and notify the maker of the request of our decision. If approved, UFR will amend the Personal Information. We will also make a reasonable effort to notify people to whom the Personal Information was released. In the case of a denial, UFR will provide the reason for the denial and instructions on how to appeal.

Any information or Content that you voluntarily disclose for use of the Services, such as your user name, your Personal Information or your Content, may become available to the public if you release it to other users or to the general public. Once you have shared your Personal Information or your Content with other people, or otherwise made it public, that Personal Information and your Content may be re-shared by others.

---

5. Children

Our Services are not yet directed to persons under age 18. If you are the parent or guardian of a person under 18, and you become aware that your young person has provided us with Personal Information or Content without your express consent, please contact us at info@United4Respect.org and we will remove such information or Content, and we will terminate the young person's account and any subscriptions.

---

6. Changes to this Privacy Statement

We may modify our Privacy Statement from time to time on prior written notice sent to the email address we have for you. For any user who has not provided us with an email address, the revised Privacy Statement will become effective no less than thirty (30) days after posting on the WorkIt website at www.United4Respect.org. We will also keep prior versions of this Privacy Statement in an archive for your review.

---

7. Different Locations, Different Laws

The laws and regulations that address privacy rights and responsibilities (collectively, "Laws") are different from one to another. Indeed, some of the Laws do or do not apply depending on different factors, including:

- Location or residence of the user.

- Location or residence of the individual that is the subject of the Personal Information ("Data Subject").

- Location or residence of the person or organization that employs or contracts with the Data Subject.

- Location of each server or other machine where the Personal Information is received, stored, processed or forwarded to.

- Location of the relevant office of UFR

Several of the Laws that concern anonymous users, registered users, family members and UFR are discussed in this Section, but these are not all of the Laws that may apply.

7.1 United States Federal Laws

Several of the federal Laws in the United States may apply to the Personal Information collected by WorkIt.

Currently, all Personal Information of users and registered users resident in the United States is stored on servers and other machines physically located within the United States.

7.1.1 Health Insurance Portability and Accountability Act (“HIPAA”)

Currently, HIPAA does not apply to the Services as UFR is neither a covered entity nor a business associate (as those terms are used in HIPAA).

7.1.2 Children’s Online Privacy Protection Act (“COPPA”)

Currently, COPPA does not apply to the Services provided by UFR Each registered user and other user must be 18 years of age or older. As noted in this Privacy Statement, if we learn of any registered user or user is under the age of 18, or if any parent or guardian contacts us, we will close that person's account and remove all information provided by the individual from our Services.

7.2 State Laws in the United States

Individual states in the United States have passed and enforce information privacy and security laws.

7.2.1 Your California Privacy Rights

If you are a California resident, California Civil Code Section 1798.83 permits you to request information regarding the disclosure of your Personal Information by UFR to third parties for the third parties' direct marketing purposes. To make such a request, please send an email to info@United4Respect.org, or send us postal mail at:

Attn: Privacy, Organization United for Respect, , 3758 Grand Avenue, PO Box 14, Oakland, CA 94610.

Pursuant to California Civil Code Section 1798.83(c)(2), UFR does not share users' Personal Information with affiliate companies or others outside UFR for those parties' direct marketing use unless a user elects that we do so.

If you are a California resident under the age of 18, and a subscriber of any site where this Privacy Statement is posted, California Business and Professions Code Section 22581 permits you to request and obtain removal

of content or information you have publicly posted. To make such a request, please send an email with a detailed description of the specific content or information to info@United4Respect.org. Please be aware that such a request does not ensure complete or comprehensive removal of the content or information you have posted and that there may be circumstances in which the law does not require or allow removal, even if requested.

7.3 Countries and Regions Other than the United States

Currently, UFR does not attract users from any country, region or jurisdiction other than the United States of America, but may do so in the future. Any individual who provides Personal Information to us from outside the United States consents to the storing, processing and use of that person's Personal Information in accordance with United States privacy and security law, which may be less protective than the laws of other countries or regions.

---

8. Use of Email Addresses and Other Contact Information

We collect the email addresses of those who voluntarily provide them to us, including users and registered users. You may receive subscription, editorial and other messages from any WorkIt Services. If you do not want to receive email from us in the future, please let us know at http://remove.United4Respect.org.

Please note that we do not provide your email addresses to others for unrelated third-party email offers.

9. Contact Us

If you have questions or concerns about this Privacy Statement, please contact us online at info@United4Respect.org, or by postal mail addressed to:

Attn: Privacy, Organization United for Respect, 3758 Grand Avenue, PO Box 14, Oakland, CA 94610.

---

10. Revision Date and History

These Terms were last revised: August 22, 2017.

Prior versions of this Privacy Statement are listed below:

● November 10, 2016.

● September 16, 2016.

Organization United for Respect – Written Information Security Policy (WISP)

We are Organization United for Respect (“UFR”, “we”, “us” and “our”). We are an online community for works in the retail sector of the (the “Services”).

The objectives of this comprehensive written information security program ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards UFR has selected to protect the personal and sensitive information (“Personal Information”) it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the Massachusetts Data Security Regulation and other similar laws.

In the event of a conflict between this WISP and any legal obligation or other UFR policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3 of this WISP).

---

1. Purpose.

The purpose of this WISP is to:

1.1 Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information UFR collects, creates, uses, and maintains.

1.2 Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

1.3 Protect against unauthorized access to or use of UFR-maintained personal and other sensitive information that could result in substantial harm or inconvenience to any customer or employee.

1.4 Define an information security program that is appropriate to UFR's size, scope, and business; its available resources; and the amount of personal and other sensitive information that UFR owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

2. Scope.

This WISP applies to all employees, contractors, officers, and directors of UFR. It applies to any records that contain personal and other sensitive information (“Personal Information”) in any format and on any media, whether in electronic or paper form.

2.1 For purposes of this WISP, "Personal Information" includes without limitation an individual’s first and last name, or first initial and last name, in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

2.1.1 Social Security number, driver's license number, or other government-issued identification numbers, including any passport number, or tribal identification number.

2.1.2 Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial accounts.

2.1.3 Any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information, where “personally identifiable financial information” includes any information:

2.1.3.1 A consumer provides UFR to obtain a financial product or service.

2.1.3.2 About a consumer resulting from any transaction involving a financial product or service with UFR.

2.1.3.3 Information UFR otherwise obtains about a consumer in connection with providing a financial product or service.

2.1.4 Health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional created or received by UFR. “Health information” includes any information which identifies or for which there is a reasonable basis to believe the information can be used to identify the individual and which relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual.

2.1.5 Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer.

2.1.6 Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris.

2.1.7 Electronic mail (“email”) or other communications address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

2.1.8 UFR considers to be highly confidential information that, if accessed by or disclosed to unauthorized parties, could cause significant or material harm to UFR, its customers, or its business partners.

---

3. Information Security Coordinator.

3.1 UFR has designated a Chief Privacy Officer to implement, coordinate, and maintain this WISP, and who will also either serve as or supervise the "Information Security Coordinator".

3.2 The Information Security Coordinator shall be responsible for initial implementation of this WISP, including:

3.2.1 Assessing internal and external risks to Personal Information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4).

3.2.2 Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5).

3.2.3 Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal [and other sensitive] information (see Section 6).

3.2.4 Ensuring that the safeguards are implemented and maintained to protect Personal Information throughout UFR, where applicable (see Section 6).

3.2.5 Overseeing service providers that access or maintain Personal Information on behalf of UFR (see Section 7).

3.2.6 Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8).

3.2.7 Defining and managing incident response procedures (see Section 9).

3.2.8 Establishing and managing enforcement policies and procedures for this WISP, in collaboration with UFR human resources and management (see Section 10).

3.3 The Information Security Coordinator will also be responsible for employee, contractor, and (as applicable) stakeholder training, including:

3.3.1 Providing periodic training regarding this WISP, UFR's safeguards, and relevant information security policies and procedures for all employees,

contractors, and (as applicable) stakeholders who have or may have access to Personal Information;

3.3.2 Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through written acknowledgement forms.

3.3.3 Retaining training and acknowledgment records.

3.4 Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in UFR's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing Personal Information (see Section 11).

3.5 Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or UFR's information security policies and procedures.

3.6 Periodically reporting to UFR management regarding the status of the information security program and UFR's safeguards to protect Personal Information.

---

4. Risk Assessment.

4.1 As a part of developing and implementing this WISP, UFR will conduct a documented risk assessment periodically or whenever there is a material change in UFR's business practices that may implicate the security, confidentiality, integrity, or availability of records containing Personal Information.

4.2 The risk assessment shall:

4.2.1 Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing Personal Information.

4.2.2 Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the Personal Information.

4.2.3 Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

4.2.3.1 Employee, contractor, and (as applicable) stakeholder training and management.

4.2.3.2 Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures.

4.2.3.3 Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal.

4.2.3.4 UFR's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

4.3 Following each risk assessment, UFR will:

4.3.1 Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

4.3.2 Reasonably and appropriately address any identified gaps.

4.3.3 Regularly monitor the effectiveness of UFR's safeguards, as specified in this WISP (see Section 8).

---

5. Information Security Policies and Procedures.

5.1 As part of this WISP, UFR will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders.

5.2 UFR will establish policies regarding:

5.2.1 Information classification.

5.2.2 Information handling practices for Personal Information, including the storage, access, disposal, and external transfer or transportation of Personal Information.

5.2.3 User access management, including identification and authentication (using passwords or other appropriate means).

5.2.4 Encryption.

5.2.5 Computer and network security.

5.2.6 Physical security.

5.2.7 Incident reporting and response.

5.2.8 Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD).

5.2.9 Information systems acquisition, development, operations, and maintenance.

5.3 UFR will detail the implementation and maintenance of UFR's administrative, technical, and physical safeguards (see Section 6).

6. Safeguards.

6.1 UFR will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of Personal Information that UFR owns or maintains on behalf of others.

6.2 Safeguards shall be appropriate to UFR's size, scope, and business; its available resources; and the amount of Personal Information that UFR owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

6.3 UFR shall document its administrative, technical, and physical safeguards in UFR's information security policies and procedures (see Section 5).

6.4 UFR's administrative safeguards shall include, at a minimum:

6.4.1 Designating one or more employees to coordinate the information security program (see Section 3).

6.4.2 Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4).

6.4.3 Training employees in security program practices and procedures, with management oversight (see Section 3).

6.4.4 Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7).

6.4.5 Adjusting the information security program in light of business changes or new circumstances (see Section 11).

6.5 UFR's technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports secure user authentication protocols, including:

6.5.1 Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices.

6.5.2 Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records.

6.5.3 Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

6.6 UFR’s technical safeguards shall also include secure access control measures, including:

6.6.1 Restricting access to records and files containing Personal Information to those with a need to know to perform their duties.

6.6.2 Assigning unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) to each individual with computer or network access that are reasonably designed to maintain security.

6.6.3 Encryption of all Personal Information traveling wirelessly or across public networks.

6.6.4 Encryption of all Personal Information stored on laptops or other portable or mobile devices [, and to the extent technically feasible, Personal Information stored on any other device or media (data-at-rest)].

6.6.5 Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to Personal Information or other attacks or system failures.

6.6.6 Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) Personal Information.

6.6.7 Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

6.7 UFR's physical safeguards shall, at a minimum, provide for:

6.7.1 Defining and implementing reasonable physical security measures to protect areas where Personal Information may be accessed, including reasonably restricting physical access and storing records containing Personal Information in locked facilities, areas, or containers.

6.7.2 Preventing, detecting, and responding to intrusions or unauthorized access to Personal Information, including during or after data collection, transportation, or disposal.

6.7.3 Secure disposal or destruction of Personal Information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

---

7. Service Provider Oversight.

UFR will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain Personal Information on its behalf by:

7.1 Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and UFR's obligations.

7.2 Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and UFR's obligations.

7.3 Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and UFR's obligations.

---

8. Monitoring.

UFR will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of Personal Information. UFR shall reasonably and appropriately address any identified gaps.

---

9. Incident Response.

UFR will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

9.1 Documenting the response to any security incident or event that involves a breach of security.

9.2 Performing a post-incident review of events and actions taken; and

9.3 Reasonably and appropriately addressing any identified gaps.

---

10. Enforcement.

Violations of this WISP will result in disciplinary action, in accordance with UFR's information security policies and procedures and human resources policies.

---

11. Program Review.

UFR will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in UFR's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing Personal Information. UFR shall retain documentation regarding any such program review, including any identified gaps and action plans.

---

12. Effective Date and Revision History.

This WISP is effective as of September 16, 2016.

Prior versions of this WISP are listed below:

- None