CANDIDATE DATA PROTECTION STANDARDS

I. OBJECTIVE

The aim of these Candidate Data Protection Standards ("Standards") is to provide adequate and consistent safeguards for the handling of candidate data by Genworth entities.
The identifiable information about yourself that you provide to a Genworth entity as a job seeker for a position with a Genworth entity (the "Candidate Data" or "Data") will be used for recruitment purposes, and the Candidate Data will be protected in accordance with Genworth's Standards outlined below and all applicable laws.
By submitting your Candidate Data, you confirm and agree that:

- you have reviewed Genworth's Standards
- Genworth may process the Candidate Data according to the recruitment purposes set out in the Standards; and
- the Candidate Data may be transferred worldwide consistent with Genworth's Standards.

Your consent is required in order to complete the submittal process. If you do not agree, click cancel and the submittal process will discontinue.
These Standards, unless noted otherwise, do not form part of any contract of employment, where applicable, offered to successful hires.

II. SCOPE

These Standards apply to all Genworth entities that process Candidate Data.
Processing refers to any action that is performed on Candidate Data, whether in whole or in part by automated means, such as collecting, recording, organizing, storing, modifying, using, disclosing, or deleting such data.
Candidate Data are defined as any identifiable information about you that you or someone else provides (on your or Genworth's behalf) in the context of applying for a position with a Genworth entity.
These Standards do not cover data rendered anonymous or where pseudonyms are used. Data are rendered *anonymous* if individual persons are no longer identifiable or are identifiable only with a disproportionately large expense in time, cost, or labor. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either impossible or at least rendered considerably more difficult. If Data rendered anonymous become no longer anonymous (i.e., individual persons are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then these Standards will again apply.

III. APPLICATION OF LOCAL LAWS

These Standards are designed to provide a uniform minimum compliant standard for every Genworth entity with respect to its protection of Candidate Data worldwide. Genworth recognizes that certain laws may require stricter standards than those described in these Standards. Genworth entities will handle Candidate Data in accordance with local law applicable at the place where the Candidate Data are processed. Where applicable local law provides a lower level of protection of Candidate Data than that established by these Standards, then the requirements of the Standards shall apply.

IV. PRINCIPLES FOR PROCESSING CANDIDATE DATA

GENWORTH respects the privacy rights and interests of each individual. Genworth entities will observe the following principles when processing Candidate Data:

- Data will be processed fairly and lawfully.
- Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes.
- Data will be relevant to and not excessive for the purposes for which they are collected and used. For example, Data may be rendered anonymous when feasible and appropriate, depending on the nature of the Data and the risks associated with the intended uses.

- Data will be accurate and, where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Candidate Data that is inaccurate or incomplete.
- Data will be kept only as long as it is necessary for the purposes for which it was collected and processed.
- Data will be processed in accordance with the individual's legal rights (as described in these Standards or as provided by law).
- Appropriate technical, physical, and organizational measures will be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to Data.

V. DATA COLLECTION

You may use various methods to submit your Candidate Data to Genworth. These methods may include: (a) e-mail or paper submission to Genworth personnel; (b) online submittal of Candidate Data processed by a third party service provider into an electronic database based in the U.S. accessible by Genworth authorized personnel; or (c) via a Genworth employment application.
Genworth may periodically collect further information with your consent or in accordance with applicable laws. For example, Genworth may collect your feedback and opinions (e.g., surveys) for business purposes, such as improving processes. You may respond to these surveys voluntarily or may elect not to respond and will not suffer reprisals for your decision. These Standards will be applicable to any further information collected including any responses to such surveys.

VI. PURPOSES AND ACCESS FOR CANDIDATE DATA PROCESSING

Genworth and Genworth entities process Candidate Data for legitimate human resources purposes. Such processing will be conducted within such purpose limitations and in accordance with applicable law. These principal purposes include:
Human Resources Purposes Include: Identifying and/or evaluating candidates for Genworth positions; making a decision about whether the individual should be hired; maintaining appropriate record-keeping related to hiring practices; analyzing the hiring process and outcomes; and conducting background investigations, where permitted by law (the "Purposes").
If a Genworth entity processes your Candidate Data for purposes that go beyond the Purposes described above, the Genworth entity responsible for the new purpose will ensure that you are informed of the new purposes for which your Candidate Data are to be used, and the categories of recipients of your Candidate Data.
Your Data will be accessed and processed by individuals who are involved in the hiring process for Genworth and who have a legitimate need to access and process your Data for the Purposes.

VII. TYPES OF CANDIDATE DATA

Candidate Data that is processed includes:

- Candidate status
- Work history/job data
- Education
- Compensation
- Employer feedback
- Online questionnaire results
- Candidate contact information
- Previous addresses or names of the Candidate
- Additional information provided by the Candidate (e.g., a cover letter)
- Driver's license number, as needed for certain positions
- References
- Criminal history, where permitted by law

VIII. SPECIAL CATEGORIES OF DATA

To the limited extent a Genworth entity needs to collect any Special Data (such as data containing personal information about racial or ethnic origin, political opinions, religious or political beliefs, trade-union membership, health or medical records, or criminal records), the Genworth entity will ensure that the individual is informed of such collection and processing. Where required by law, the person's explicit consent to the processing and particularly to the transfer of such data to non- Genworth entities will be obtained. Appropriate security and protection measures (e.g., physical security devices, encryption, and access restrictions) will be provided depending on the nature of these categories of data and the risks associated with the intended uses.

IX. SECURITY AND CONFIDENTIALITY

Genworth entities are committed to taking appropriate technical, physical, and organizational measures to protect Candidate Data against unauthorized access, unlawful processing, accidental loss or damage, and unauthorized destruction.

Equipment and Information Security

To safeguard against unauthorized access to Candidate Data by third parties outside Genworth, all electronic Candidate Data held by Genworth entities are maintained on systems that are protected by secure network architectures that contain firewalls and intrusion detection devices. The servers holding Candidate Data are "backed up" (i.e., the data are recorded on separate media) on a regular basis to avoid the consequences of any inadvertent erasure or destruction of data. The servers are stored in facilities with comprehensive security and fire detection and response systems.

Access Security

Genworth entities limit access to internal systems that hold Candidate Data to a select group of authorized users who are given access to such systems through the use of a unique identifier and password. Access to Candidate Data is limited to and provided to individuals for the purpose of performing their job duties (e.g., a human resources manager may need access to a Candidate's contact information for the purposes of setting up an interview). Compliance with these provisions will be required of third-party administrators who may access certain Candidate Data, as described in SECTION XI. *TRANSFERRING DATA.*

Training

Genworth will conduct training regarding the lawful and intended purposes of processing Candidate Data, the need to protect and keep information accurate and up-to-date, and the need to maintain the confidentiality of the Data to which employees have access. Authorized users will comply with these Standards, and Genworth entities will take appropriate disciplinary actions, in accordance with applicable law, if Candidate Data are accessed, processed, or used in any way that is inconsistent with the requirements of these Standards.

X. RIGHTS OF DATA SUBJECTS

Any person may inquire as to the nature of the Candidate Data stored or processed about him or her by any Genworth entity. You will be provided access to Candidate Data as is required by law in your home country, regardless of the location of the data processing and storage. A Genworth entity processing such data will cooperate in providing such access either directly or through another Genworth entity. All such requests for access may be made by sending a request in writing to:

Human Resources – Staffing Center
6620 W. Broad Street
Building 4
Richmond, VA 23230

Candidate Data will be available for access for a reasonable period of time, and Genworth will allow you to view your Candidate Data upon reasonable notice and at reasonable times.

You may also contact the Staffing Center to ask questions regarding these Standards or your Candidate Data or withdraw your consent. Any letters sent to the Administrator for any other purpose other than the above will not be responded to and will be discarded.

If access or rectification is denied, the reason for the denial will be communicated and a written record will be made of the request and reason for denial.

If you demonstrate that the purpose for which the data is being processed is no longer legal or appropriate, the data will be deleted, unless the law requires otherwise.

If any Candidate Data is inaccurate or incomplete, you may request that the data be amended by submitting a new resume/CV with the updated information (e.g., new home address or change of name).

In addition, you may send an email to EmploymentDataPrivacy@genworth.com to withdraw your consent.

XI. TRANSFERRING DATA

Transfers to other Genworth entities:

Genworth strives to ensure a consistent and adequate level of protection for Candidate Data that are processed and/or transferred between Genworth entities. A transfer of Candidate Data to another Genworth entity is considered a transfer between two different entities, which means that even in such "intra-group" cases, a data transfer shall be carried out only if applicable legal requirements are met and if:

- The transfer is based on a clear business need;
- The receiving entity provides appropriate security for the data; and
- The receiving entity ensures compliance with these Standards for the transfer and any subsequent processing.

Transfers to non-GENWORTH entities:

- **Selected Third Parties:** At times, Genworth entities may be required to transfer Candidate Data to selected external third parties that they have hired to perform certain employment-related services on their behalf. These third parties may process the data in accordance with the Genworth entity's instructions or make decisions regarding the data as part of the delivery of their services. In either instance, Genworth entities will select reliable suppliers who undertake, by contract or other legally binding and permissible means, to put in place appropriate security measures to ensure an adequate level of protection. Genworth entities will require external third-party suppliers to comply with these Standards or to guarantee the same levels of protection as Genworth when handling Candidate Data. Such selected third parties will have access to Candidate Data solely for the purposes of performing the services specified in the applicable service contract. If a Genworth entity concludes that a supplier is not complying with these obligations, it will promptly take appropriate actions.
- **Other Third Parties:** Genworth entities may be required to disclose certain Candidate Data to other third parties (1) as a matter of law (e.g., to tax and social security authorities); (2) to protect Genworth's legal rights (e.g., to defend a litigation suit); or (3) in an emergency where the health or security of a Candidate is endangered (e.g., a fire).

XII. DIRECT MARKETING

Genworth entities will not disclose Candidate Data outside Genworth to offer any products or services to a Candidate for personal or familial consumption ("direct marketing") without his or her prior consent.
The restrictions in this section apply only to contact data obtained in the context of applying for a position with Genworth. They do not apply to contact data obtained in the context of a consumer or customer relationship.

XIII. AUTOMATED DECISIONS

Some countries regulate the making of Automated Decisions, which are decisions about individuals that are based solely on the automated processing of data and that produce legal effects that significantly affect the individuals involved.
In some circumstances, job seekers will be asked to complete a questionnaire where automated decisions will be made based on the Candidate's responses.
Except in limited circumstances (e.g., the screening via computer or telephone for some open positions in Genworth), Genworth entities do not make Automated Decisions to evaluate individuals or for other purposes. If Automated Decisions are made, affected persons will be given an opportunity to express their views on the Automated Decision in question by contacting the Human Resources Data Protection Administrator.

XIV. ENFORCEMENT RIGHTS AND MECHANISMS

All Genworth entities will ensure that these Standards are observed. All persons who have access to Candidate Data must comply with these Standards. In some countries, violations of data protection regulations may lead to penalties and/or claims for damages.
If at any time, a person believes that Candidate Data relating to him or her has been processed in violation of these Standards, he or she may report the concern to the Human Resources Data Protection Administrator.
If the concern relates to an alleged violation of these Standards by a Genworth entity located in a country other than that of the person or the exporting Genworth entity, he or she may request the assistance of the exporting entity. That Genworth entity will assist him or her in investigating the circumstances of the alleged violation. If the violation is confirmed, the exporting and importing entities will work together with any other relevant parties to resolve the matter in a satisfactory manner, consistent with the provisions of these Standards.
If the Staffing Center or the local Genworth entity does not resolve the concern, it may be escalated to Genworth's Global Privacy Council. The Global Privacy Council, chaired by Genworth's Data Privacy Officer, is composed of a group of Genworth employees who have oversight responsibility for all aspects of compliance with these Standards and for the resolution of all concerns and issues that arise with respect to Genworth's handling of Candidate Data under these Standards. The Global Privacy Council may be contacted by email at EmploymentDataPrivacy@genworth.com. The Global Privacy Council will communicate its decision and any associated remedy to the relevant persons.
The processes described in these Standards supplement any other remedies and dispute resolution processes provided by Genworth and/or available under applicable law.

XV. AUDIT PROCEDURES

To further ensure enforcement of these Standards, Genworth's Privacy Officer, along with Genworth's Global Privacy Council, which is composed of senior privacy officials from each of Genworth's major businesses, will identify Candidate and employment Data procedures that should be audited. For this purpose, Genworth will engage its Corporate Audit Staff, who are independent of the business lines of management. Members of the Audit Staff report to Genworth's Vice President,

Corporate Audit Staff, who has an independent line of communication to the Audit Committee of Genworth's Board of Directors. Reports of the Audit Staff's findings will be submitted to Genworth's Global Privacy Council for review and response. The Council will require an action plan to ensure compliance with these Standards. To the extent such matters cannot be adequately handled with Genworth's own resources, Genworth agrees to appoint an independent third party to conduct an investigation/audit of any procedures or issues involving Candidate or employment Data under the Standards.

XVI. COMMUNICATION ABOUT THE STANDARDS

In addition to the training on these Standards, Genworth will communicate these Standards to current and new employees by posting them on selected internal Genworth websites and by providing a link to the Standards on information technology applications where Candidate Data are collected or processed.

XVII. MODIFICATIONS TO THE STANDARDS

Genworth reserves the right to modify these Standards as needed, for example, to comply with changes in laws, regulations, Genworth practices and procedures, or requirements imposed by data protection authorities. Genworth's Data Privacy Officer, or his/her designee, must approve all changes to the Standards for them to become effective. If Genworth makes changes to the Standards, Genworth will submit the Standards for renewed approval where required by law. Genworth will inform Genworth employees and other persons (e.g., persons accessing Genworth websites to enter Candidate Data such as job application information) of any material changes in the Standards. Genworth will post all changes to the Standards on relevant internal and external websites.
Effective with the implementation of these Standards, all existing intra-group agreements and applicable company privacy guidelines relating to the processing of Candidate Data will be superseded by the terms of these Standards. All parties to any such agreements will be notified of the effective date of implementation of the Standards.

XVIII. OBLIGATIONS TOWARD DATA PROTECTION AUTHORITIES

Genworth will respond diligently and appropriately to requests from data protection authorities about these Standards or compliance with applicable data protection and privacy laws and regulations. Genworth employees who receive such requests should contact their local Human Resources manager or business legal counsel. Genworth will, upon request, provide data protection authorities with names and contact details of relevant contact persons. With regard to transfers of Candidate Data between Genworth entities, the importing and exporting Genworth entities will (i) co-operate with inquiries from the data protection authority responsible for the entity exporting the data, and (ii) respect its decisions, consistent with applicable law and due process rights.

ADDENDUM

Rights and Obligations with Respect to Candidate Data Collected Within the EU/EEA and Processed Elsewhere
In addition to any rights and obligations that are set forth in Genworth's Candidate Data Protection Standards ("Standards") or that otherwise exist, the following principles established in light of Directive 95/46/EC ("European Data Protection Directive") will apply to Candidate Data collected by GENWORTH entities in the European Union/European Economic Area and processed elsewhere. In jurisdictions where this Addendum applies, the enforcement rights and mechanisms mentioned in the Standards also apply to the provisions of this Addendum. The following are not intended to grant employees further rights or establish further obligations beyond those already provided under the European Data Protection Directive:

1. Job seekers may object to the processing of Candidate Data about them on compelling legitimate grounds relating to their particular situation. This might occur, for instance, if the job seeker's life or health is at risk due to the processing of the data. This provision shall not apply if the processing is (i) required by law, (ii) based on the job seeker's individual consent, or (iii) necessary to fulfill a contractual obligation between the job seeker and Genworth.
2. After exhausting appropriate internal dispute resolution processes, job seekers may seek compensatory damages from a Genworth entity for loss or damage to them caused by a violation of the Standards (including the provisions of this Addendum) by the GENWORTH entity. The Genworth entity shall not be liable for damages if it has observed the standard of care appropriate in the circumstances.
3. If any of the terms or definitions used in the Standards are ambiguous, the definitions established under applicable local law within the relevant EU/EEA member state shall apply or where there are no such definitions under applicable local law, the definitions of the European Data Protection Directive shall apply.