



## Data Use Agreement

Pursuant to 105 KAR 1:140 \_\_\_\_\_ (“Employer”) is required to submit certain reports electronically to Kentucky Retirement Systems (“KRS”) using the secure Kentucky Retirement Systems' Employer Self Service website ("Website") implemented through the Strategic Technology Advancements for the Retirement of Tomorrow ("START") project, or through the KRS Secure Email Portal ("Portal").

Employer will be submitting certain Personal Information through the Website or Portal that is required to be transmitted securely in order to protect the privacy and security of the Personal Information. Such Personal Information must only be transmitted through the Website or Portal in accordance with this Agreement and Applicable Law.

KRS and Employer intend to protect the privacy and provide for the security of Personal Information transmitted to KRS pursuant to this Agreement and Applicable Law.

Section 2(2)(i) of 105 KAR 1:140 requires that the Employer enter into this Data Use Agreement to protect the privacy and provide for the security of Personal Information transmitted to KRS.

### Article I - Definitions

**NOW, THEREFORE,** Employer agrees as follows:

1.1. Meaning of Terms. The following terms shall have the meaning ascribed to them in this Section:

- (a) **Applicable Law** shall mean all applicable federal, state, and local statutes, regulations, standards and policy requirements that apply to KRS or Employer, as applicable. Applicable Law shall also include, without limitation, any regulations or sub-regulatory guidance issued by KRS related to the START program, the Website, or the Portal.
- (b) **Breach** shall mean:
  - (1) the submission by an Employer of Unsecured Personal Information about one or more Individuals to KRS;
  - (2) the submission of Personal Information by an Employer regarding an Individual intended to be submitted to KRS to another person or entity by hand-delivery, mail, fax, or in an electronic format; or
  - (3) the unauthorized acquisition, access, use, or disclosure of Personal Information that compromises the security or privacy of such information.
- (c) **Electronic Personal Information** means Personal Information that is transmitted or maintained by or in electronic media.

- (d) **Reporting Official** shall mean the individual designated by Employer and whose duties are described in this Agreement, including, without limitation, Section 3.5.
- (e) **HIPAA** shall mean the Health Insurance Portability and Accountability Act of 1996, as amended or modified by HITECH or other Applicable Laws or regulations.
- (f) **HITECH** shall mean the Health Information Technology for Economic and Clinical Health Act of 2009, as amended.
- (g) **Individual** shall mean an employee of an Employer or such employee's beneficiaries or dependents.
- (h) **Personal Information** means an Individual's first name or first initial and last name in combination with the Individual's:
  - (1) social security number;
  - (2) driver's license number;
  - (3) personal identification number permitting access to the Individual's account; or
  - (4) medical information.
- (i) **Portal** means the KRS Secure Email Portal.
- (j) **Privacy Rule** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, as amended or modified by HITECH or other Applicable Laws or regulations.
- (k) **Security Rule** shall mean the Security Standards for Protecting Electronic Personal Information at 45 C.F.R. Parts 160 and 164, as amended or modified by HITECH or other Applicable Laws or regulations.
- (l) **Unsecured Personal Information ("Unsecured Personal Information")** shall mean Personal Information that is not secured through the use of technologies and methodologies that render such Personal Information unusable, unreadable, or indecipherable to unauthorized individuals.
- (m) **Website** means the Kentucky Retirement Systems' Employer Self Service Website.

## Article II - General Terms

2.1. Interpretation of Provisions. In the event of an inconsistency between the provisions of this Agreement and the mandatory terms of 105 KAR 1:140 (as amended), 105

KAR 1:140, shall prevail. The provisions of 105 KAR 1:140 are incorporated herein by reference.

2.2. Provisions Permitted by Privacy Rule or Security Rule. Where provisions of this Agreement are different from those mandated by 105 KAR 1:140, but are nonetheless permitted by 105 KAR 1:140, the provisions of the Agreement shall control.

### **Article III - Obligations and Activities of Employer**

3.1. Reports. Employer shall submit the reports required under KRS 61.675 and KRS 78.625 electronically using the Website by:

- (a) The Enter Report Details Module; or
- (b) Uploading an electronic file in the format specified in the Employer Contribution Record Layout.

3.2. Method of Reporting. Employer shall submit the contributions required by KRS 61.675 and KRS 78.625:

- (a) Electronically using the Website;
- (b) By mailing or hand delivering a check;
- (c) By the eMARS system maintained by the Finance and Administration Cabinet; or
- (d) By wire transfer.

3.3. Reporting of Creditable Compensation. Employer shall report all creditable compensation paid during a month by the tenth day of the following month.

- (a) Employer shall designate the month to which the creditable compensation should be applied if it is not the month for which the employer is reporting if the month the creditable compensation was earned is the month in which the employee:
  - (1) Became eligible to participate in one of the systems administered by KRS;
  - (2) Was transferred to hazardous coverage from nonhazardous participation;
  - (3) Was transferred from hazardous coverage to nonhazardous participation;
  - (4) Terminated from employment; or
  - (5) Became ineligible to participate in one (1) of the systems administered by KRS.

- (b) Reporting of Lump-Sum or Nonrecurring Payment. If the employee is paid creditable compensation in a lump-sum or nonrecurring payment, Employer shall designate the reason for the lump-sum or nonrecurring payment.
- (1) If the lump-sum or nonrecurring payment was earned during a specific time period, the employer shall designate the time period during which the lump-sum or nonrecurring payment was earned.
  - (2) If Employer fails to designate a specific time period during which the lump-sum or non-recurring payment was earned, the payment shall be considered a lump-sum bonus pursuant to KRS 16.505(8), 61.510(13), or 78.510(13).

3.4. Inapplicability to Kentucky Personnel Cabinet. The provisions of Section 3.1 of this Article shall not apply to the Kentucky Personnel Cabinet or agencies that are reported by the Kentucky Personnel Cabinet.

3.5. Reporting of Regular Full-Time Employees. Employer shall report employees who are regular full-time employees as defined by KRS 61.510(21) and 78.510(21) and shall remit employer and employee contributions for those employees.

3.6. Reporting of Non Regular Full-Time Employees. Employer shall report employees who are not regular full-time employees as defined by KRS 61.510(21) and 78.510(21), but shall not remit employer or employee contributions for those employees unless required to do so pursuant to KRS 61.680(6).

3.7. Submission of Electronic Mail. Employer shall submit electronic mail to KRS by logging on to the KRS secure electronic mail server.

3.8. Interest Rates. Employer shall pay interest at the rate adopted by the board for any creditable compensation paid as a result of an order of a court of competent jurisdiction, the Personnel Board, or the Human Rights Commission or for any creditable compensation paid in anticipation or settlement of an action before a court of competent jurisdiction, the Personnel Board, or the Human Rights Commission including notices of violations of state or federal wage and hour statutes or violations of state or federal discrimination statutes. The interest shall be assessed from the time period for which the creditable compensation has been reinstated.

3.9. Effect of Refusal to Provide Required Information. If Employer refuses to provide the retirement systems access to records or information requested in accordance with KRS 61.685 or does not respond to a request for information or records by the retirement systems, KRS may, if appropriate:

- (a) Hold all payments of any funds due to Employer;
- (b) Hold payments of refunds or initial retirement allowances to any employee or former employee of Employer whose refund or retirement may be affected by the records or information requested by KRS; and

- (c) Use any other legal remedy available to KRS to enforce this agreement and the statutes and administrative regulations governing KRS.

3.10. Submission of Personal Information. If Employer submits Personal Information about its employees to the retirement systems in an unsecure electronic format or submits personal information regarding its employees intended to be submitted to the retirement systems to another person or entity by hand delivery, mail, fax, or in an electronic format, the employer shall notify affected employees in writing of the disclosure of personal information and provide information regarding obtaining credit reports.

3.11. Safeguards. Employer agrees to use reasonable and appropriate administrative, physical and technological safeguards to: (i) prevent use or disclosure of the Personal Information other than as provided for by this Agreement or Applicable Law, and (ii) to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Personal Information that it creates, receives, maintains or transmits to KRS. Employer represents and warrants that it has implemented, and during the term of this Agreement shall maintain, comprehensive written privacy and security policies and procedures and the necessary administrative, technical and physical safeguards appropriate to the size and complexity of Employer's operations and the nature and scope of its activities. When transmitting any Personal Information that includes medical information, Employer will comply with HIPAA, including, without limitation, the Security Rule requirements set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316, all of which are hereby incorporated into the Agreement. Employer will comply with such requirements regardless of whether Employer or KRS is considered to be a "covered entity" as defined by HIPAA at 45 C.F.R. § 160.103.

3.12. Mitigation of Harm. Employer agrees to mitigate, to the extent practicable, any harmful effect that is known to Employer of a use or disclosure of Personal Information by Employer, or any agent or subcontractor of Employer, in violation of the requirements of this Agreement or Applicable Law.

3.13. Report of Breach or Improper Use or Disclosure of Personal Information.

- (a) If Employer knows of a Breach of Personal Information, it shall immediately notify KRS. Such report shall be in writing and shall be reported to KRS as soon as practicable after Employer becomes aware of such Breach, but in no event more than 48 hours following such date. A Breach shall be treated as discovered by Employer as of the first day on which such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of Employer. Employer's notification shall be in writing and shall include identification of each Individual whose Personal Information has been, or is reasonably believed by Employer to have been subject to the Breach. Employer shall include the following information in its notification of Breach to KRS:

- (1) A description of the Breach, including the date of the Breach and the date of the discovery of the Breach, if known;

- (2) A description of the types of Personal Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, credit card numbers, diagnosis, disability code or other types of Personal Information were involved);
- (3) Any steps that Individuals should take to protect themselves from potential harm resulting from the Breach;
- (4) A description of what Employer is doing to investigate the Breach, to mitigate the harm to Individuals and to protect against further Breaches; and
- (5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, Web site or postal address.

In the event that some of the above listed information is not known by Employer at the time of notification of KRS of the Breach, Employer shall provide such information to KRS as soon as it becomes available to Employer, but in no event later than 30 days after Employer discovers such Breach. Employer shall also provide such assistance and further information with regard to the Breach to KRS as reasonably requested by KRS.

- (b) If KRS becomes aware of a Breach of Personal Information, it shall notify the affected Employer.
- (c) After any notices required by subsections (a) or (b) have occurred, Employer shall notify affected Individuals in writing of the Breach of their Personal Information and provide information regarding obtaining their credit reports. Prior to providing any such notices, Employer shall submit a draft of the notice to KRS for its approval. Upon KRS' approval, Employer shall provide the written notices to the affected Individuals and shall provide KRS with copies of all such notices after they have been provided to the affected Individuals.
- (d) If KRS is required by Applicable Law to provide notification to Individuals about a Breach of Personal Information by Employer, or if KRS determines that it should provide notification to affected Individuals because of the nature or magnitude of Employer's Breach of Personal Information, Employer shall reimburse KRS for its costs incurred in making any such notifications. Such costs may include, without limitation, costs related to: notifying affected Individuals and any relevant governmental agencies or any other persons or entities under Applicable Law; any remediation necessitated by the Breach; any fines or penalties arising out of the Breach; and any other actions required to be taken pursuant to Applicable Law.

3.14. Access to Personal Information By Employers' Personnel.

- (a) Employer shall designate an Employer Administrator who shall determine the authorized users under Employer's control who use, disclose, and transmit Personal Information for the purposes in this Agreement and under Applicable Law.
- (b) To designate the Employer Administrator, Employer must complete the Form 7071, Employer Self Service Reporting Official Account Creation Request. Employer may designate up to two users with an Administrator role in Employer Self Service. A Form 7071 will be required for each user designated as an Employer Administrator.
- (c) The Employer Administrator will be responsible for maintaining user accounts at an agency for the Website and the Portal. This includes setting up and assigning roles to additional users and managing credentials. The Employer Administrator may reset passwords and Employer PINs as well as disabling credentials for users who are no longer employed. The Employer Administrator shall immediately notify KRS in the event that a user name or password has been disclosed or otherwise made known to any person not authorized to have knowledge of that user name or password.

3.15. Employer's Responsibility for Authorized Users. Employer shall be solely responsible, as allowed by federal or state law, for all acts and omissions of the Employer and/or the Employer's authorized users, and all other individuals who access the Website, the Portal, or Personal Information either through the Employer or by use of any password, identifier or log-on received obtained, directly or indirectly, lawfully or unlawfully, from Employer or any of Employer's authorized users, and all such acts and omissions shall be deemed to be the acts and omissions of the Employer. Each Employer shall certify:

- (a) That its authorized users have received training regarding the confidentiality of Personal Information under Applicable Law and agree to protect the Personal Information in compliance with Applicable Law and this Agreement;
- (b) That its authorized users shall only access the Website and the Portal and use, disclose, and transmit Personal Information for purposes that are consistent with this Agreement and Applicable Law;
- (c) That its authorized users have agreed to hold any passwords, or other means for accessing the Website, the Portal, and Personal Information, in a confidential manner and to release them to no other individual;
- (d) That its authorized users agree and understand that their failure to comply with this Agreement and Applicable Law may result in their inability to access the Website, the Portal, and Personal Information, and may constitute cause for disciplinary action by the Employer; and
- (e) That it has restricted access to the Website, the Portal, and Personal Information only to the authorized users that Employer has identified pursuant to this Agreement.

3.16. Agents and Subcontractors. Employer agrees to ensure that any agent, including a subcontractor, to whom it provides Personal Information received from, or created or received by Employer on behalf of, KRS, agrees in writing to the same restrictions and conditions that apply through this Agreement to Employer with respect to Personal Information. Such written agreement shall also require the agent or subcontractor to implement reasonable and appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Personal Information that it creates, receives, maintains or transmits on behalf of KRS.

3.17. Availability of Internal Practices, Books and Records. Employer shall make internal practices, books, and records relating to the use and disclosure of Personal Information received from, or received by Employer on behalf of, KRS available to KRS, in a time and manner designated by KRS, for purposes of determining Employer's compliance with 105 KRS 1:140, this Agreement, and Applicable Law.

3.18. Training. Employer shall provide appropriate training to its workforce in security, privacy, and confidentiality issues and regulations relating to Personal Information under this Agreement and Applicable Law.

3.19. Response to Subpoena. Employer shall notify KRS within forty-eight (48) hours if it receives a subpoena or other legal process seeking the disclosure of Personal Information. Such notification shall be provided in a timeframe that allows KRS a reasonable amount of time to respond to the subpoena, object to the subpoena, or to otherwise intervene in the action to which the subpoena pertains.

3.20. Notification of Claims. Employer shall notify KRS within forty-eight (48) hours upon notification or receipt of any civil or criminal claims, demands, causes of action, lawsuits, or governmental enforcement actions arising out of or related to this Agreement or the Personal Information, regardless of whether KRS and/or Employer are named as parties in such claims, demands, causes of action, lawsuits, or enforcement actions.

3.21. Assistance in Litigation or Administrative Proceedings. Employer shall make itself and any subcontractors, employees or agents assisting Employer in the performance of its obligations under this Agreement, available to KRS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against KRS, its trustees, officers, or employees based upon a claimed violation of Applicable Law, except where Employer or its subcontractor, employee, or agent is named as an adverse party.

#### **Article IV - Reimbursement for Claims**

4.1. In addition to the obligations set forth in Section 3.13(d), Employer shall reimburse KRS for, any expenses, losses, damages, legal fees, or costs arising out of or related to any civil or criminal claims, demands, causes of action, lawsuits, or governmental enforcement actions, whether brought by a third party or asserted by Employer, arising out of or related to Employer's actual or alleged acts and omissions (or those of its agents or subcontractors) associated with Employer's or its agents' or subcontractors' obligations under this Agreement or



their use or disclosure of Personal Information. Such reimbursement shall include, but not be limited to, the payment of all reasonable attorney fees associated with any claim, demand, action, cause of action, or lawsuit arising out of or related to such acts or omissions.

**Article V - KRS Duties Pursuant to 105 KAR 1:140**

5.1. Notice to Employer. KRS shall notify Employer of the web address of the Website and shall notify Employer if the web address changes.

5.2. Invoices. KRS shall submit an invoice to Employer for any payments owed to KRS, which were not paid through the normal monthly reports. KRS may offset funds owed by the employer to the retirement systems with funds owed to Employer by the retirement systems.

5.3. Change or Revocation of Permission. KRS shall provide Employer with any changes in, or revocation of, permission by an Individual to use or disclose Personal Information, if such changes affect Employer's permitted or required uses and disclosures. Employer shall comply with any such changes or revocations.

**Employer**

Name of Employer: \_\_\_\_\_

Agency Head or Reporting Official: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_